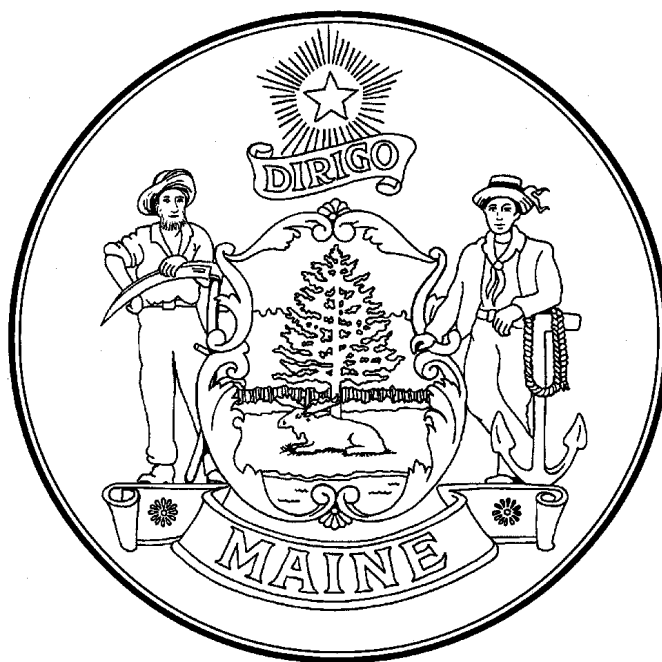


# MAINE STATE LEGISLATURE

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)

May 5, 2025

Senator Anne Carney, Chair  
Committee on Judiciary  
100 State House Station  
Augusta, ME 04333

Representative Amy Kuhn, Chair  
Committee on Judiciary  
100 State House Station  
Augusta, ME 0433

**RE: LD 1822 – An Act to Enact the Maine Online Data Privacy Act**

Chair Carney, Chair Kuhn, and Members of the Committee,

AdvaMed, the MedTech Association, is the largest medical technology association, representing the innovators and manufacturers transforming health care through earlier disease detection, less invasive procedures, and more effective treatments. Our more than 600 members range from small, emerging companies to large multinationals and include traditional device, diagnostic, and digital health technology companies.

We appreciate Chair Kuhn's efforts to tackle this complex issue and engage on LD 1822 and her willingness to support the overall effort to provide confidence to Mainers that their data privacy is secured. LD 1822 would provide the residents of Maine with transparency and control over their personal data and provide new privacy protections.

We support this legislation and its goal to further clarify how healthcare now, and in the future, will be safeguarded for patients and their health care. Though this legislation does contain nearly all the language advancing these objectives, it is missing two key provisions that will help safeguard patient data by avoiding ambiguity while ensuring access to lifesaving and life-enhancing devices and other advanced medical technologies in the most appropriate settings.

**Unique Nature of Medtech Health Data:**

- **Clinician-Oriented:** Unlike consumer devices, medical devices are often chosen and used by clinicians, not by the patients themselves.
- **HIPAA and non-HIPAA health care providers:** Medtech companies often support health care providers (providers), and not all of those providers are HIPAA covered entities because of the structure of the HIPAA rules. To be safe, medtech companies apply HIPAA protections to all data received from provider-managed devices.
- **No Direct Patient Interface:** Many medical devices are designed to be operated solely by clinicians, with no direct interface for patients. Without a patient interface,



there is no direct means of obtaining and recording consent for data collected from non-HIPAA covered providers

We request adding the following language to Section §9604. 2. Exempt Data:

- Q. Information treated in the same manner as Protected Health Information that is maintained by a Covered Entity or Business Associate;
- R. Information included in a Limited Data Set as described at 45 CFR 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified at 45 CFR 164.514(e);

### **Information Treated like HIPAA**

The inclusion of this language is essential to avoid a negative impact on patient care and research and development in Maine. This language has been incorporated into privacy laws in CA, CO, CT, FL, IN, IA, KY, MD, MN, MT, NV, NH, OR, TN, TX, UT, VA, and WA. It will prevent unintended negative impacts on patient care and avoid unnecessary liability for disclosures of patient data that are enabled under HIPAA and critical to a functioning healthcare system.

A **real-world example** for why this amendment is crucial to enabling seamless patient care is described below.

A heart monitor manufacturer can be liable for sharing ECG recordings with a consulting healthcare provider (with instruction from the ordering provider) without the patient's explicit consent just because the ordering provider is not a HIPAA covered entity. In other words, because LD 1822 exempts only HIPAA covered entities but not non-covered providers, a medtech company will be held liable for treating any patient data gathered by their devices as HIPAA data, as if it originated from a provider who takes insurance. Since medtech companies often responsible for this sharing won't have direct interaction with the patient necessary to obtain this consent, they err on the side of caution and treat all data they receive as HIPAA data.

Here's how that could look:

*The physician ordering the cardiac monitor is an ob-gyn physician who does not accept insurance, so they are not a covered entity and the data collected by that cardiac monitor falls outside of HIPAA. The ordering physician seeks a consult from a physician outside of her institution and logs into the medtech company's cloud platform to grant access to the consulting physician, which notifies the consulting physician by email to create an account or login if she already has an account to access the ECG recordings for this patient. The information collected by the cardiac monitor is technically not protected health information under HIPAA since the ordering physician does not accept insurance, so exemption I. would not apply and the medtech company would be liable for not obtaining affirmative express consent to disclose the ECG recording to the consulting provider. The heart monitor device only has a single button to mark events when a patient feels dizzy or has palpitations and does not have an interface to seek and record consent to share information.*



Importantly, this amendment helps avoid any ambiguity on how patient data is treated. It does not enable a healthcare institution or provider that does not take insurance from sharing patient data with any outside entity, nor does omitting this amendment prevent them from doing so unless Maine state law explicitly prevents this.

### **Limited Data Sets Diversify and Strengthen R&D**

This exemption enables the sharing of protected health information for crucial purposes without compromising patient privacy. Limited data sets may be used for research, public health activities, and health care operations purposes. The recipient need not be a covered entity or business associate but must nonetheless enter into a data use agreement requiring them to protect the information.

Allowing for the use of these critical data sets diversifies and expands the breadth of knowledge that goes into medical research and development, leading to more innovative and better researched medical devices and technology.

### **Conclusion**

Unlike other industries, health care is already subject to extensive regulation at the federal level. Our goal for this bill – and similar legislation around the country – is focused on avoiding conflict between state and federal laws and ensuring both the continued delivery of high-quality patient care and ensuring essential health research is not disrupted.

AdvaMed has taken a leadership role throughout the country in ensuring that state-level data privacy legislation in 19 states recognizes the existing federal framework governing health data and medical device and technology products. We encourage the committee to follow suit and ensure that there continues to be alignment across the country.

Thank you for your consideration and we look forward to working with you and the committee on these amendments.

Sincerely,



Roxolana Kozycky  
Senior Director, State Government and Regional Affairs  
AdvaMed



5/5/25  
LD1822  
Findhelp

Good afternoon, Chair Kuhn and honorable members of this committee and thank you for the opportunity to speak today.

My name is Toby Landau, and I am here on behalf of Findhelp, a social care data company that has proudly connected the citizens of Maine to a network of over 4,000 free and reduced cost services for more than a decade. We are speaking in strong support of An Act to Enact the Maine Online Data Privacy Act (LD1822), and we deeply appreciate the committee's leadership in moving this critical legislation forward.

As technology continues to shape every aspect of our lives—from the way we work, interact with our families, to how we access essential services—data privacy has never been more important. In this landscape, **LD 1822 stands as a vital safeguard** for the privacy of Maine residents, ensuring that individuals are protected from the misuse, exploitation and inappropriate sale of their personal information.

Findhelp's mission is to connect people in need to the programs that serve them with dignity and ease. Our platform serves over 292,000 users across Maine, helping people access essential social care services—everything from housing and food stability to transportation and employment. We proudly partner with Maine Health, Maine 211, Northern Light, Mainely Teeth and several other organizations that serve Mainers.

As the nation's largest social care network and closed-loop referral system, we handle significant amounts of extraordinarily sensitive data. This includes **social care data**—information that ranges from housing status to food insecurity to transportation needs.

Since our founding in 2010, we have **committed to never selling data**. Our network is built on a consumer-directed privacy model where individuals opt in to share their information for each referral, and access to referral history is permission-based. **Our industry moves at the speed of trust**; and our users trust us with their most personal information because we protect it.

To quote one of our customers, Ayla Burke, with Mainely Teeth, many of the people they “serve have come from dangerous situations. If we don't protect their information and privacy, we're risking their lives in ways that we don't even understand.”

That's why we strongly support the Maine Online Data Privacy Act. This bill represents a step toward ensuring that all personal data is protected. The bill's provisions on **data minimization, consumer rights, and the protection of sensitive data** are essential, as they ensure that data is only collected when necessary and that individuals have the right to access, correct, and delete their data.

We believe the bill can be strengthened to define social care data and explicitly include it among the most sensitized data and banning the sale or monetization of data collected in systems like Findhelp. **We encourage the committee to review similar Data Privacy bills**

5/5/25

LD1822

Findhelp

**being considered in the Massachusetts Legislature, HD3628 and SD2264, respectively sponsored by Representative Giannino and Senator Mark.**

In a world where data brokers and privacy violations are common, **LD1822 represents the kind of forward-thinking legislation we need to safeguard the privacy of our citizens.** By setting clear standards for how companies collect, process, and store personal data, Maine will lead the way in protecting its residents in the digital age. As technology continues to evolve, it's critical that our laws evolve with it to protect the fundamental rights of Maine residents. This bill is an essential step toward that goal, and we at Findhelp strongly support its passage.

Thank you for your time and consideration.



Testimony of Brian Langley

Before the Joint Standing Committee on Judiciary  
May 5, 2025

**In Support of LD 1224, “An Act to Comprehensively Protect Consumer Privacy”  
In Opposition to 1822, “An Act to Enact the Maine Online Data Privacy Act”**

Senator Carney, Representative Kuhn, and distinguished members of the Joint Standing Committee on Judiciary, my name is Brian Langley, and I am a resident of my hometown of Ellsworth. I’ve owned and operated the Union River Lobster Pot restaurant right here in Ellsworth for nearly thirty years. I’m here today to support Representative Roberts’ bipartisan bill, LD 1224, and I’d like to tell you why this matters to me as a small business owner and someone who cares deeply about Maine’s future.

After four decades in the restaurant industry, I can tell you it has never been harder to run a business than it is today. Costs are up, staffing remains a challenge, and we’re heading into a season filled with more questions than answers. I talk to my colleagues across the hospitality and tourism industry, and what I hear over and over again is uncertainty—about travel patterns, about spending habits, and yes, about what new policies might be coming out of Augusta.

Maine is a small business state, and for many of us, that means being the HR department, the maintenance crew, the marketers, and the bookkeeper, usually all before lunch. But too often, legislation is crafted in silos, without recognizing the cumulative toll it takes on small operators like us. One new rule or law might seem manageable in isolation, but pile enough of them on, and it becomes a barrier to even staying open. Many of us are one or two payrolls away from closing for good.

In the middle of all that, we can’t afford to be experimenting with sweeping new policies that haven’t been tested. LD 1224 gives us something that’s thoughtful and workable. It

protects consumer privacy, which we all care about, but it also gives businesses like mine the ability to keep up with how the world works now, especially online.

There was a time when the Yellow Pages was the only game in town. You paid for a listing and hoped someone saw it. Now, it's a completely different world. Digital tools help us reach people in real time. They're cost-effective, and they let us turn on a dime. Here's a classic Maine example. I look outside and see it's raining? I snap a photo of a steaming bowl of lobster stew and post it online. The sun comes out in the afternoon two hours later? We pivot from lobster stew to microbrews and sunset dining. That kind of agility keeps us connected with customers, not just selling a meal but sharing a moment.

That's "marketing by the minute". And these tools aren't a luxury. They're a necessity for small businesses, especially in tourism. Someone in Bangor picks up their phone and searches "restaurants with outdoor seating near me." If we're not showing up because new laws make it harder or riskier to use those tools, we have lost that customer. She's not flipping through a phone book. She's relying on search results.

Now, I've heard people say, "Don't worry—we'll carve small businesses out." But if I can't use the same digital marketing tools as a restaurant in New Hampshire or Rhode Island, that's not a carve-out—that's a carve-off. That puts me at a real disadvantage. We support strong consumer protections, but we also need clear, consistent policies that won't box us in or leave us behind. Take those tools away, or make them too confusing or risky to use, and you're pulling the rug out from under us. "What's even worse is a large corporate company, like the Yellow Pages will come in for an exorbitant price, stating that they "comply with all the regs" will take care of advertising for us. It's *Déjà vu*.

LD 1224 strikes a balance. It's modeled after 17 other states, including several New England neighbors. It gives businesses time to comply and avoids conflicting regulation across state lines. That's not just smart policy, it's also practical and fair.

Restaurants, inns, and other small businesses like mine are more than just places to eat or stay. We are ambassadors for the state of Maine. We're in the business of creating memories—of the sea coast, the food, the people, and the feeling of being here. But we can't do that if we're buried in red tape or boxed out of the very tools we need to survive and compete with the corporates.

LD 1224 gives us a path forward that works for both consumers and small businesses. I urge you to support it. Thank you for your time, and I'd be happy to answer any questions.

May 3, 2025

Judiciary Committee

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

Dear Members of the Committee:

I am writing on behalf of Internet Safety Labs in support LD 1822, An Act to Enact the Maine Online Data Privacy Act.

Internet Safety Labs (ISL) is a non-profit digital product safety testing organization and has been assessing and reporting on safety risks (including privacy risks) since 2019. We conduct independent safety research and create Safety Labels for mobile apps which can be viewed on our App Microscope (<https://appmicroscope.org>). Our safety labels report on observed data sharing between the app and the developer, and all third parties as evidenced by the network traffic between the app and these entities. In other words, we assess privacy based on the observed behavior of apps and websites, and not on what the developers say in privacy policies or other notices.

In 2022 we conducted the first of its kind US K-12 Edtech safety benchmark, auditing more than 1700 apps that were recommended or required by a representative sample of K-12 schools across the US. We are intimately familiar with the kinds of privacy risks children (and adults) are exposed to by using technology the way it's intended (see in depth reports here:

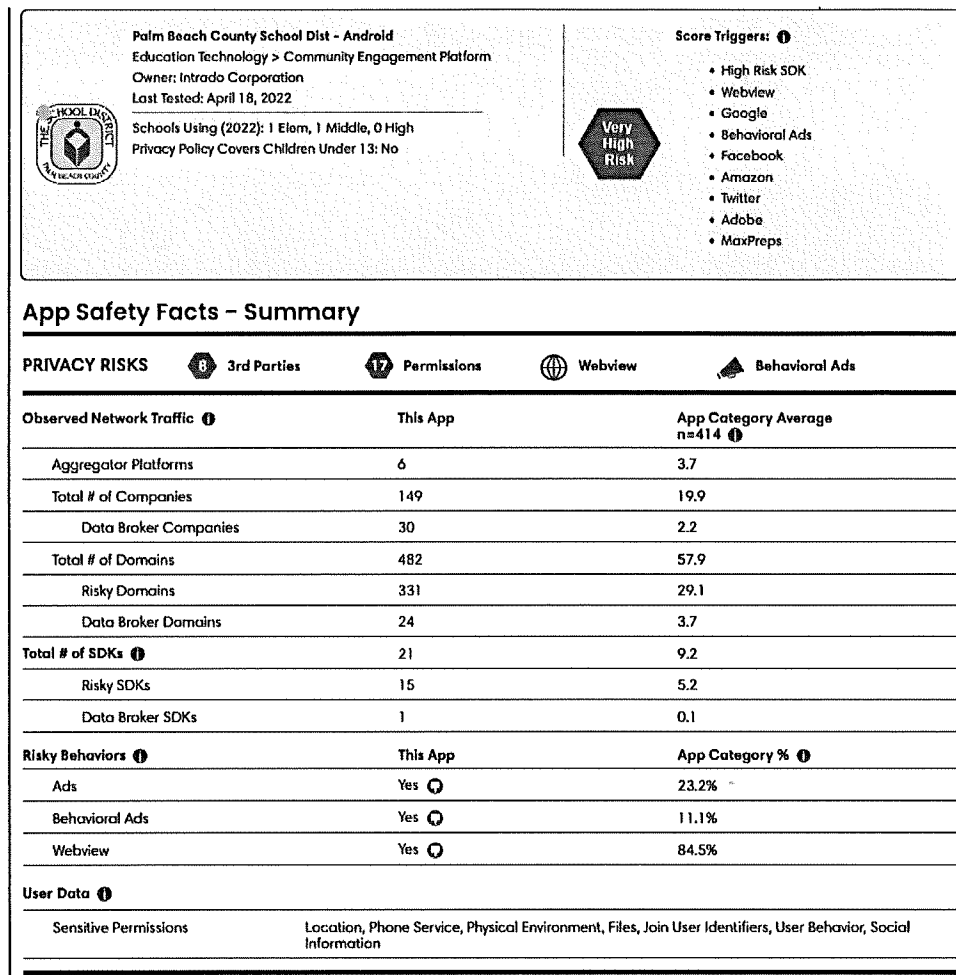
<https://internetsafetylabs.org/resources/reports/2022-us-k12-edtech-benchmark/>).

Figure 1 shows an example of the worst/leakiest app from our 2022 benchmark<sup>1</sup>. Note that there were 149 unique companies observed in the app's network traffic flow, thirty of which were registered data brokers.<sup>2</sup>

---

<sup>1</sup> Happily, this app is no longer available on the app stores.

<sup>2</sup> ISL believes the number of data brokers in the network traffic is significantly higher than this number due to the ineffective penalties in data broker laws, and due to deficiencies in current data broker laws.



### App Safety Facts - Summary

PRIVACY RISKS

8 3rd Parties

17 Permissions

Webview

Behavioral Ads

| Observed Network Traffic | This App                                                                                                                              | App Category Average<br>n=414 |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| Aggregator Platforms     | 6                                                                                                                                     | 3.7                           |
| Total # of Companies     | 149                                                                                                                                   | 19.9                          |
| Data Broker Companies    | 30                                                                                                                                    | 2.2                           |
| Total # of Domains       | 482                                                                                                                                   | 57.9                          |
| Risky Domains            | 331                                                                                                                                   | 29.1                          |
| Data Broker Domains      | 24                                                                                                                                    | 3.7                           |
| Total # of SDKs          | 21                                                                                                                                    | 9.2                           |
| Risky SDKs               | 15                                                                                                                                    | 5.2                           |
| Data Broker SDKs         | 1                                                                                                                                     | 0.1                           |
| Risky Behaviors          | This App                                                                                                                              | App Category %                |
| Ads                      | Yes                                                                                                                                   | 23.2%                         |
| Behavioral Ads           | Yes                                                                                                                                   | 11.1%                         |
| Webview                  | Yes                                                                                                                                   | 84.5%                         |
| User Data                | Sensitive Permissions: Location, Phone Service, Physical Environment, Files, Join User Identifiers, User Behavior, Social Information |                               |

Figure 1: ISL Safety Label for Palm Beach County School District Android App, tested on 04/18/2022.

From our research, we can state definitively that commercial surveillance is ubiquitous and the scale staggering. Last year, we identified and researched the foundational infrastructure that enables commercial surveillance at scale<sup>3</sup>. There is a global, decentralized network of advertising and marketing platforms called customer data platforms (CDPs, like Adobe) and identity resolution platforms (IDRPs, like LiveRamp) that are architected to ingest customer data from disparate sources, associating them to a unique person through “identity resolution” techniques. ISL tracked 93 identity resolution platforms and 246 customer data platforms, and 20 companies that provide both types of platforms worldwide<sup>4</sup>. Only 16.4% of these platforms were registered data brokers, whereas it’s highly likely that many more of them should be. Note also that these platforms

<sup>3</sup> “Worldwide Web of Human Surveillance: Identity Resolution and Customer Data Platforms”, July 24, 2024, Internet Safety Labs, <https://internetsafetylabs.org/wp-content/uploads/2024/07/Worldwide-Web-of-Human-Surveillance-Identity-Resolution-and-Customer-Data-Platforms.pdf>

<sup>4</sup> <https://internetsafetylabs.org/resources/references/identity-resolution-and-customer-data-platform-companies/>

indiscriminately hoover up and monetize personal data without regard to age. 539 (35%) of the K-12 apps in our 2022 research sent data to these commercial surveillance platforms.

As of today, the CDP Institute shows hundreds of CDPs with education data, non-profit data, and disturbingly, healthcare data. In preparing these comments, we found 350 CDPs with healthcare data, 37 of which also perform unique person identification (identification resolution).<sup>5</sup>

ISL constantly assesses these platforms and their sites proudly assert “cookieless tracking”, and “personalized experiences for *visitors*”. Note, this is a deliberate word choice; not customers but visitors<sup>6</sup>. There is nearly no place online where we aren’t being tracked.

There are two types of commercial surveillance infrastructures: (1) the decentralized one described above that enables entities to share customer data at tremendous scale, and (2) proprietary infrastructures from the Big Tech giants, including Google and Meta. Both of these infrastructures knit together disparate data sources to develop increasingly invasive and comprehensive profiles of people. Worse, the mechanisms for knitting this data together indiscriminately hoover up the data of everyone, including children. ISL found that 35% of the apps (539 apps) in our 2022 K12 Edtech benchmark sent data to CDPs or IDRs<sup>3,7</sup>.

Finally, the data collected by these surveillance infrastructures span digital sources and physical world sources and include highly sensitive data and inferences. Experian boasts of 1,900+ attributes per consumer<sup>3</sup>.

Consent alone won’t fix this problem. In fact, in recent research, ISL observed inaccurate information in two prominent edtech providers’ privacy policies incorrectly stating that COPPA allows the schools to provide consent on behalf of the students. Consent fails as privacy protection.

### **LD 1822: Prohibiting Risky Data Practices**

We are pleased to see that LD 1822 provides two crucial measures to make digital products safer. First, a limitation on the collection of sensitive personal information. In 2022, ISL published ten principles<sup>8</sup> for safe software and Principle #4 is Data Collection Minimization where data collection must be proportional to the deal being established between the product and the consumer. This kind of contextual proportionality is vital for meaningful data minimization. One of the easiest and best ways to keep people safe when using digital products is to collect/observe/and derive less personal information.

Secondly, prohibition on the sale of sensitive personal data is a much needed and profoundly important measure and we’re happy to see it in LD 1822. Selling of sensitive personal data has been shown repeatedly to present physical, emotional, and reputational risks to individuals and groups. ISL believes

---

<sup>5</sup> <https://www.cdpinstitute.org/vendors/>

<sup>6</sup> Here’s one example IDR: <https://getuntitled.ai/blog/website-visitor-tracking-software/>

<sup>7</sup> <https://internetsafetylabs.org/resources/references/identity-resolution-and-customer-data-platforms-found-in-2022-edtech-benchmark-network-traffic/>

<sup>8</sup> <https://internetsafetylabs.org/resources/specifications/principles-of-safe-software/>

personal data markets are profoundly risky to individuals and societies—and especially to children. The proposed LD 1822 robust definition of sensitive data in conjunction with the prohibition of the sale of it is an excellent start to keep everyone safer.

ISL also supports the list of “processing activities that present a heightened risk of harm to a consumer” in section 9611, Data protection assessment.

Finally, ISL appreciates the specifications to ensure that downstream processors uphold both the user’s and the controller’s data processing requirements.

### **LD 1822: Concerns**

- **FERPA data exception:** While we’re glad to see the wholesale prohibition of the sale of personal information of minors, we are concerned about excluding data covered under FERPA. Edtech and other technology used by K-12 students is under-scrutinized when it comes to *actual* data sharing behaviors. Schools often don’t have the technical resources to assess claims from edtech vendors and instead take them at their word<sup>9</sup>. In 2024, ISL compared 84 edtech and educational apps against the data processing agreements made between tech vendors and local education agencies (LEAs; schools, districts, and state level entities). Only 12% of the studied apps with data processing agreements (DPAs) accurately listed all the data elements collected by the app in practice<sup>10</sup>. 44% of the DPAs failed to correctly identify the 3<sup>rd</sup> parties receiving the data. Finally, 55% of the apps with DPAs were found to be sending data to adtech entities. (Note that this doesn’t always mean that ads or behavioral ads were observed in the apps.) In short, FERPA doesn’t effectively serve to minimize risky student data sharing.
- **Excluded businesses:** ISL believes that *all* institutions should be held to strict personal data privacy protections. **Non-profit organizations:** Non-profit entities like the AARP, political action committees, and churches hold volumes of sensitive information that can—and is—weaponized. Non-profits should not be excluded from privacy protections, particularly prohibiting the sale of sensitive personal data. **Medical apps:** LD 1822 seems to defer to privacy protections provided by HIPAA. We are in the early stages of conducting research on medical apps and from our preliminary results, we have reason to believe that “HIPAA compliant” apps are sharing personal data sharing with marketing and advertising entities. As noted earlier, there is a sizeable market for healthcare data

---

<sup>9</sup> Only 29% of the 663 schools studied had evidence of broad scale vetting of technologies being recommended to students. “2022 K-12 EdTech Benchmark Findings Report 2: School Technology Practices & 3<sup>rd</sup> Party Certifications Analysis”, pg. 29, Internet Safety Labs, June 27, 2023.

<sup>10</sup> As detected by our testing and review of actual network traffic from the app.

and despite regulations, this highly sensitive information is being trafficked.

**Higher Education:** While our sample set of studied universities and colleges is small yet (only 17 schools), we found evidence of data monetization in at least one <sup>11</sup> which also claims that contact information is non-sensitive. However, email addresses—even when hashed-- can uniquely identify people.<sup>12</sup>

- **Opting out of data selling:** We understand the tradition of this legal precedent and also appreciate the existence of the Global Privacy Control<sup>13</sup> (GPC) mechanism for opting users out, but the safest option is for consumers to opt *into* data selling. Data monetization creates unacceptable privacy risks to consumers and violates ISL Safe Software Principle #5: Private by Default<sup>14</sup>. Moreover, research confirms that users rarely modify default settings in apps and websites<sup>15</sup>.

Thank you for the opportunity to testify. ISL, our empirical research, and reference tools are at your service. We appreciate the Committee's leadership on this critical issue.



Lisa LeVasseur  
Executive Director & Research Director  
Internet Safety Labs

---

<sup>11</sup> <https://www.devry.edu/compliance/notice-of-right-to-opt-out.html>

<sup>12</sup> Even when hashed, emails can be, through probabilistic identification methods, used as a unique personal identifier. <https://www.adexchanger.com/ad-exchange-news/burning-a-hole-in-the-invincibility-of-email-hashing/>

<sup>13</sup> <https://globalprivacycontrol.org/>

<sup>14</sup> <https://internetsafetylabs.org/resources/specifications/principles-of-safe-software/>

<sup>15</sup> <https://www.cnet.com/tech/tech-industry/default-settings-for-privacy-we-need-to-talk/>



TO: The Honorable Anne Carney  
The Honorable Amy Kuhn, Co-Chairs  
Members of the Joint Standing Committee on the Judiciary

DATE: May 5, 2025

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

---

Good morning Senator Carney and Representative Kuhn.

My name is Ann Luther. I am a resident of Trenton. I'm submitting this written testimony on behalf of the League of Women Voters of Maine, where I serve as a volunteer and chair the League's Advocacy Committee. I am testifying in support of LD 1822.

The League of Women Voters of Maine is a nonpartisan political organization that has been working for over 100 years to encourage informed and active participation in government, to increase understanding of major public policy issues, and to influence public policy through education and advocacy. We never support or oppose any political party or candidate.

The League of Women Voters believes that, especially in the context of elections:

- voters should have sufficient information about candidates and campaign issues to make informed choices;
- transparency and the public's right to know who is using what resources to influence elections are vital to their ability to cast an informed vote;
- and undue influence in the marketplace of ideas can have a corrosive effect on public discourse and election outcomes.

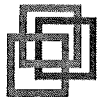
We see profound new challenges that threaten these principles. The massive accumulations of private data — bought and sold as a commodity — allows unknown entities to exert undue influence over voters and elections without disclosure or disclaimer.

Here's how that works: Commercial interests with unprecedented power and reach gather information about us from surveillance devices, our actions on-line, and our smartphones. They know where we live and who our friends are and what we buy. They know our likes and dislikes, our politics and sleep habits. They use or sell that information to political actors who have an interest in manipulating us with targeted messages. Often, that content is mis-, dis-, or mal-information, micro-targeted to susceptible voters. Neither the identities nor the spending of these actors is public. And the public may not even be aware of the purposeful distortion in the information ecosystem. All of this has little connection to rational, issue-based discussion of public policy, candidates, or our shared future. We are not free agents in the marketplace of ideas.

The abuse of our personal data and the resulting distortion of our public conversation was never anticipated by law or regulation and is now out of control. The data privacy measures proposed in LD 1822 would effectively “starve the beast” while also safeguarding vital personal privacy interests. Without the massive accumulation of private data, those who seek to disrupt the marketplace of ideas would not be able to exert as much influence or as effectively tilt the landscape in political campaigns. Legislation with data minimization, data retention, and affirmative opt-in requirements would cut off these malicious actors from the data that allows them to distort our public discourse.

For these reasons, we support LD 1822.

Thank you for the opportunity to testify. I would be happy to answer any questions from the Committee.



# MCEDV.

The Maine Coalition  
to End Domestic Violence

101 Western Ave.  
P.O. Box 5188  
Augusta, ME 04332-5188  
207.430.8334

---

**Testimony of Andrea Mancuso**  
**In Support of LD 1822: "An Act to Enact the Online Data Privacy Act"**  
**Monday, May 05, 2025**

Senator Carney, Representative Kuhn, and members of the Joint Standing Committee on Judiciary, I am writing on behalf of the Maine Coalition to End Domestic Violence (MCEDV)<sup>1</sup> in support of LD 1822, "An Act to Enact the Online Data Privacy."

Weak consumer privacy protections impact us all but are particularly dangerous for the safety efforts of victims of domestic abuse and violence. Survivors often require the most privacy when they are being targeted by the person choosing to use abuse and violence. And so, strengthening privacy protections necessarily strengthens the safety of survivors and their children in our state. Of the bills before you for consideration on this issue, only LD 1822 truly represents a step forward.

To be able to keep a wide range of information confidential or private is often essential to the planning that survivors of domestic abuse engage in to try to keep themselves, and often their children, safe. On the other end of the spectrum, people who perpetrate domestic abuse and violence become quite skilled at identifying and exploiting mechanisms to access and misuse information to further perpetrate abuse. Those who perpetrate domestic abuse are often highly familiar with the personal details of their victim, and so they are more able to be successful in their attempts to violate their victim's privacy and access information that they shouldn't, information that could further jeopardize their victim's physical, emotional or financial wellbeing.

Importantly, LD 1822 would give all Maine people, including survivors, the right to have transparent information about what has been collected and who that information has been shared with. It also prohibits the sharing of certain information that, if shared, would be ripe for misuse by the person harming them, importantly including information about their location. LD 1822 does these things without creating an opportunity for a survivor to unknowingly waive their rights to not have this information shared by doing something we all do mostly on auto-pilot in today's digital age – check the box to accept lengthy terms and conditions to access a service. This likelihood to inadvertently waive your information

---

<sup>1</sup> MCEDV serves and supports a membership of Maine's eight regional domestic violence resource centers as well as two culturally specific service providers. Together, these programs served more than 12,000 victims of domestic violence in Maine last year.

protection rights is a critically important defect in the other proposals the Committee is considering alongside LD 1822.

In 2019, MCEDV supported and celebrated the enactment of An Act to Protect the Privacy of Online Consumer Information. When companies sell customer data, that data ends up in the hands of those not authorized to possess it. When it lands in the hands of an abuser, it can and does cripple a survivor's safety plan and leaves the survivor unsuspectingly vulnerable. We encourage the Committee to not undermine the data protections that were created in 2019. LDs 1088 and 1284 would work to make more information about vulnerable survivors available for sale – giving abusive people a mechanism to access intimate details about their victim's everyday lives – where they're now living, restaurants they frequent, and the stores they shop at.

Understanding the intersection between safety of survivors of domestic abuse and violence and their ability to keep certain information confidential, there are several Maine statutes that attempt to support survivors' needs for privacy and confidentiality in various ways. These are important tools that survivors in our state use every day. As this Committee reviews data privacy proposals before you this session, and understanding all the ways that using technology is essential to functioning in our communities every day, we encourage you to recognize LD 1822 as the approach that best addresses the needs of survivors for transparent and categorical privacy around their online data.

Please do not hesitate to contact me if any additional information from our network would be helpful to your work on these issues.

**Contact Information:**

Andrea Mancuso, Public Policy Director

Ph: (207) 430-3569, Email: [andrea@mcedv.org](mailto:andrea@mcedv.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;<sup>i</sup>
- 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;<sup>ii</sup>
- The prosecution of a woman who experienced a pregnancy loss based on cell phone information after she searched online for medication abortion information;<sup>iii</sup>
- 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;<sup>iv</sup>

- 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.<sup>v</sup>

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,<sup>vi</sup> and the large majority of consumers (nearly 68%) are somewhat or very concerned about their online privacy.<sup>vii</sup>

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<sup>viii</sup> 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.

---

<sup>i</sup> 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/>

<sup>ii</sup> 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/>

<sup>iii</sup> 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>

<sup>iv</sup> 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/>

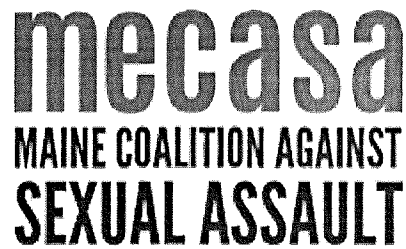
<sup>v</sup> "FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google and Others"; *Federal Trade Commission: Press Releases*; June 22, 2021; <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>

---

<sup>vi</sup> 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/>

<sup>vii</sup> Fazliloglu, 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](https://iapp.org/media/pdf/resource_center/privacy_and_consumer_trust_report_summary.pdf)

<sup>viii</sup> "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>



May 5, 2025

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

My name is Melissa Martin, and I am offering testimony today on behalf of the Maine Coalition Against Sexual Assault (MECASA), the organization which represents and serves Maine's sexual violence prevention and response programs as well as Maine's Children's Advocacy Centers. MECASA initiates and advocates for victim-centered public policy; provides expert training, technical assistance, and resources for providers and partners; and funds the service providers in your communities.

**MECASA is here today in support of LD 1822, "An Act to Enact the Maine Online Data Privacy Act."** Thank you to Representative Kuhn for sponsoring this important legislation.

LD 1822 would give consumers a range of rights regarding their digital data. The bill would apply to for-profit companies also known as "controllers." LD 1822 would prohibit controllers from the collection, processing, and sharing of consumer data, except where it's strictly necessary to provide or maintain a specific product or service requested by the consumer. Controllers would be banned altogether from selling sensitive data, such as sexual history and precise geolocation data. If LD 1822 passes, all Maine consumers would be able to access personal data collected and opt out of the processing of personal data for targeted advertising; the sale of personal data; and profiling, if the data are used to make decisions that produce legal or other significant effects

Among stalking victims 18-24 years old, 16% said their stalker shared nude, semi-nude, and/or sexually explicit photos/videos of them.<sup>1</sup> Sexual violence may be part of a stalker's pattern of behavior. There are many types of sexually violent stalking that could better be prevented with the passage of LD 1822 including following, monitoring, and/or surveilling a victim while planning or after committing a sexual assault; nonconsensual creation of sexual images (photoshop, deepfake); and posing as the victim to solicit sexual activity.<sup>2</sup>

---

<sup>1</sup> <https://www.stalkingawareness.org/wp-content/uploads/2022/04/Stalking-Sexual-Violence-Fact-Sheet.pdf>

<sup>2</sup> *Id.*

Passing LD 1822 helps support the privacy and access rights of survivors of sexual harm and stalking who vitally need access and control over their personal data to protect their own safety.

For these reasons, we strongly support the bill. Thank you for your consideration. We hope you will support LD 1822 and would be pleased to answer any questions you might have.

---

### About Maine's Sexual Assault Service Providers

One in five Mainers will experience sexual assault at some point in their lifetime.<sup>3</sup> Each year, 19,000 Mainers will experience sexual violence.<sup>4</sup>

Maine's sexual violence service providers provide free and confidential services across the state to victims/survivors of sexual harassment and sexual assault and those close to them, as well as to individuals who wish to increase their understanding of the issues. Just some of the services include a 24-hour statewide sexual assault helpline, crisis intervention and information, support groups, in-person accompaniment and advocacy through the medical and legal systems, and school- and community-based prevention education. Services are provided for a victim/survivor regardless of when they experienced sexual violence, and regardless of what type of sexual violence they experienced. Types of sexual violence include, but are not limited to, sexual harassment and gender-based bullying, child sexual abuse, elder sexual abuse, stalking, sex trafficking, and sexual violence within an intimate partner relationship.

*24/7 Confidential  
Maine Sexual Assault Helpline: 1-800-871-7741*

---

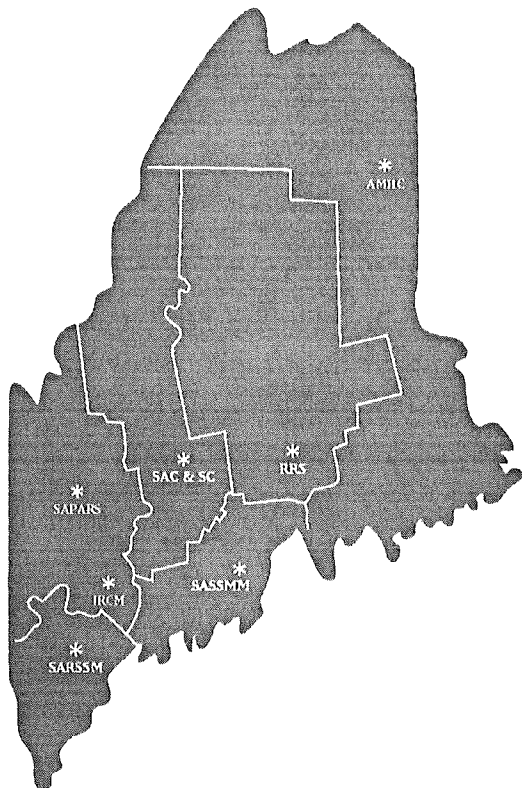
<sup>3</sup> Murray, C., Dumont, R & Shaler, G. (2022). *Maine Crime Victimization Report: Informing public policy for safer communities*. Maine Statistical Analysis Center. University of Southern Maine.

<sup>4</sup> *Id.*

# **mecasa**

**MAINE COALITION AGAINST  
SEXUAL ASSAULT**

info@mecasa.org | mecasa.org  
207-626-0034



**STATEWIDE  
SEXUAL ASSAULT HELPLINE  
1-800-871-7741**

**Free. Private. 24/7.**

## **MAINE'S SEXUAL ASSAULT SUPPORT CENTERS**

### **AMHC Sexual Assault Services (AMHC)**

Serving Aroostook, Hancock, & Washington Counties •  
amhesas.org

### **Immigrant Resource Center of Maine**

Serving Androscoggin & Cumberland Counties • ircofmaine.org

### **Rape Response Services (RRS)**

Serving Penobscot & Piscataquis Counties • rrsonline.org

### **Sexual Assault Prevention & Response Services (SAPARS)**

Serving Androscoggin, Oxford & Franklin Counties and the towns of  
Bridgton & Harrison • sapars.org

### **Sexual Assault Crisis & Support Center (SAC & SC)**

Serving Kennebec & Somerset Counties • silentnomore.org

### **Sexual Assault Response Services of Southern Maine (SARSSM)**

Serving Cumberland & York Counties • sarssm.org

### **Sexual Assault Support Services of Midcoast Maine (SASSMM)**

Serving Eastern Cumberland, Sagadahoc, Knox, Waldo & Lincoln  
Counties • sassmm.org

## **MORE SEXUAL VIOLENCE SERVICES**

Maine TransNet • mainetrans.net • info@mainetransnet.org

Wabanaki Women's Coalition • wabanakiwomenscoalition.org  
207-763-3478

Aroostook Band of Micmacs, Domestic & Sexual Violence  
Advocacy Center • 207-551-3639

Houlton Band of Maliseets, Domestic & Sexual Violence  
Advocacy Center • 207-532-6401

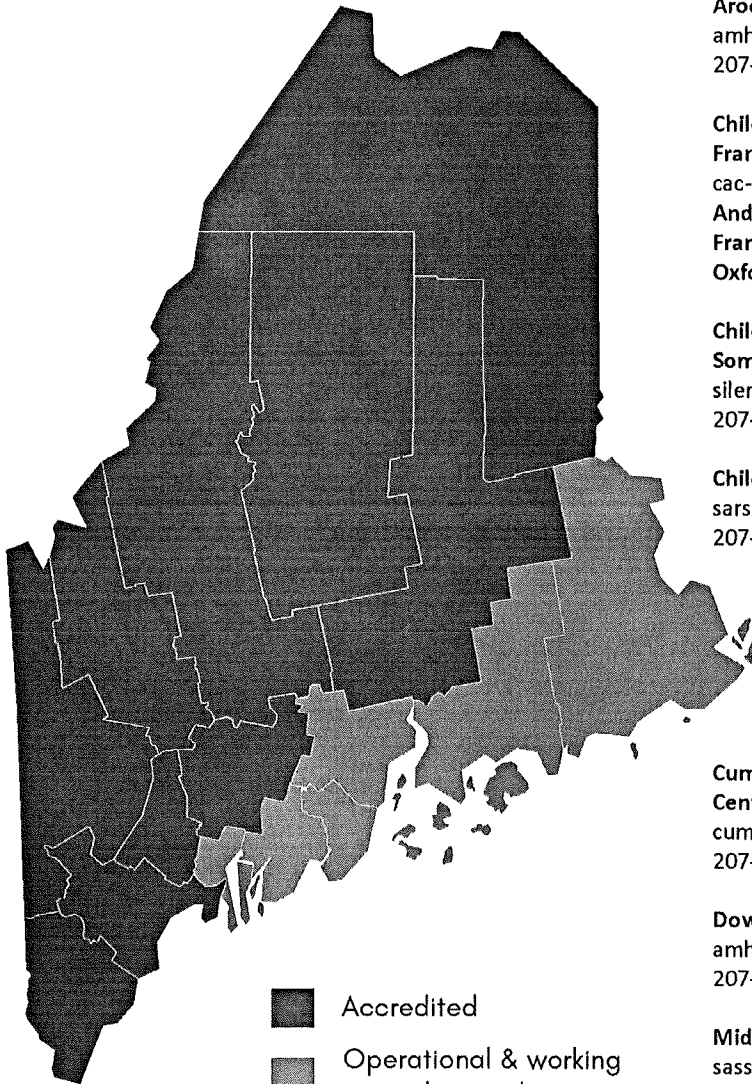
Indian Township Passamaquoddy, Domestic & Sexual  
Violence Advocacy Center • 207-214-1917

Passamaquoddy Peaceful Relations • 1-877-853-2613

Penobscot Indian Nation, Domestic & Sexual Violence  
Advocacy Center • 207-631-4886



# Maine's Children's Advocacy Centers



- Accredited
- Operational & working toward accreditation

**Aroostook County Children's Advocacy Center**  
amhcsas.org  
207-472-6134

**Children's Advocacy Center of Androscoggin, Franklin, and Oxford Counties**  
cac-afco.org  
Androscoggin: 207-784-0436  
Franklin: 207-778-9777  
Oxford: 207-739-1228

**Children's Advocacy Center of Kennebec & Somerset Counties**  
silentnomore.org/about-our-cac  
207-861-4491

**Children's Advocacy Center of York County**  
sarsmm.org  
207-459-2380

**Cumberland County Children's Advocacy Center**  
cumberlandcountycac.org  
207-879-6160

**Downeast Children's Advocacy Center**  
amhcsas.org  
207-255-3687

**Midcoast Children's Advocacy Center**  
sassmm.org  
207-522-7162

**Penquis Children's Advocacy Center**  
penquiscac.org  
207-974-2469



Testimony of Whitney A Parrish Perry

American Heart Association

**In Support of LD 1822**

*An Act to Enact the Maine Online Data Privacy Act*

May 5, 2025

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

Thank you for the opportunity to submit comments to the committee today. My name is Whitney Parrish Perry, and I am the Director of Government Relations for the American Heart Association—the nation’s oldest voluntary and largest voluntary organization dedicated to fighting heart disease and stroke, and whose mission is to be a relentless force for a world of longer, healthier lives. AHA supports the passage of LD 1822, “*An Act to Enact the Maine Online Privacy Act.*”

We appreciate Representative Kuhn for sponsoring this bill, and for the committee’s ongoing work on the important issue of consumer data privacy. The American Heart Association supports the Legislature’s desire to establish important consumer protections and shares this goal—as such, we use industry standard security protocols to protect our donors’ and volunteers’ information and make our privacy policy readily available to the public.

Given this shared goal and AHA’s longstanding, dedicated efforts to protect donor and volunteer information, we believe it is important to maintain—and highlight the importance of—LD 1822’s exemption language, specifically pertaining to not-for-profit organizations exempt from federal income tax under section 501(c)(3) of the U.S. Internal Revenue Code. The cost of proving compliance is high, and every dollar that a public charity must devote to proving data privacy compliance is a dollar that we cannot use to further our missions.

For the American Heart Association, this means fewer dollars going toward funding cardiovascular research, setting clinical guidelines for cardiac and stroke care, and providing CPR training materials and courses that are used throughout Maine and across



American  
Heart  
Association.

the country. Moreover, when a public charity like AHA does not commercialize its data (i.e. sell it), the costs are even more painful. Donors expect their funds to support the organization's mission, not for handling consumer data requests and portability support requests. Any consumer can easily access privacy policies and charity watchdog ratings, such as the rating provided by the Better Business Bureau Standards for Charity Accountability,<sup>1</sup> to see how their data is used.

In closing, LD 1822 strikes a thoughtful and necessary balance between safeguarding individual data privacy and recognizing the distinct operational realities of nonprofit organizations. The bill's measured approach acknowledges that overly broad or rigid requirements risk diverting limited resources away from community impact and toward complex compliance burdens; we believe this proposal both advances critical consumer privacy rights and carefully considers the practical implications for organizations dedicated to the public good. We respectfully ask the committee to consider and support this balanced approach when evaluating any data privacy legislation that comes before it.

Thank you for your time, attention, and consideration. If you have any questions about this testimony, please do not hesitate to email me at the email address provided below.

***Respectfully,***

Whitney Parrish Perry, Government Relations Director

American Heart Association

whitney.parrishperry@heart.org

---

<sup>1</sup> BBB Wise Giving Alliance and Charity Standards may be accessed at: <https://give.org>



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 Null, 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.<sup>1</sup> We know people do not read privacy policies.<sup>2</sup> And we know that reading privacy policies, even if people wanted to, would require hundreds of hours per year.<sup>3</sup> 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.<sup>4</sup>

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

---

<sup>1</sup> 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>.

<sup>2</sup> 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*.

<sup>3</sup> 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](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>.

<sup>4</sup> 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.<sup>5</sup> 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.”<sup>6</sup>

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,<sup>7</sup> and by limiting collection, processing, and sharing of sensitive data to that which is strictly necessary to provide a product or service.<sup>8</sup> 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,<sup>9</sup> 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

---

<sup>5</sup> 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>.

<sup>6</sup> 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>.

<sup>7</sup> §9608(2)(A).

<sup>8</sup> §9608(1)(A).

<sup>9</sup> See generally, FTC Statement on Deception, FTC (Oct. 14, 1983), [https://www.ftc.gov/system/files/documents/public\\_statements/410531/831014deceptionstmt.pdf](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.<sup>10</sup> 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.<sup>11</sup>

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

---

<sup>10</sup> 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.”).

<sup>11</sup> 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.<sup>12</sup> 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.<sup>13</sup> 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 overall<sup>14</sup>) 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.

---

<sup>12</sup> 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).

<sup>13</sup> *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>.

<sup>14</sup> *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>

**Maine Broadband Coalition Testimony**  
**In SUPPORT of LD 1822**  
**and in OPPOSITION to LD 1088 and LD 1224**  
May 5, 2025



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

My name is Joe Oliva, and I am submitting testimony on behalf of the Maine Broadband Coalition (MBC), a non-profit organization dedicated to expanding broadband access and digital equity in Maine. We represent dozens of organizations and thousands of internet users.

We submit this testimony today **in support of LD 1822**, which strengthens Maine's leading data privacy laws and **in opposition to LD 1088 and LD 1224**, which would repeal and replace good, effective data privacy regulations with an industry-preferred framework that falls short of what Maine internet users deserve.

Maine led the nation in passing a landmark bill in 2019 that gave Maine internet users the option to opt-in to any use, sell, sharing or disclosure of their information by their Internet Service Providers (ISPs). It protected people from discrimination in prices or services if they refused to have their data used in this way, provided an individual right of action if the users' privacy was violated without consent, and limited what data ISPs could collect and required them to take reasonable steps to protect it.

That bill was supported by MBC members, including GWI, an ISP based in Maine that refused to profit off customer data anyway. Smaller Maine-based ISPs are unlikely to have enough user data to be of interest to buyers, unlike the larger ISPs such as Charter Communications (Spectrum), Comcast, and data mining and advertising firms like Google, Facebook, and Amazon. The bill passed on a bipartisan basis, 85-45 in the House of Representatives and unanimously in the Senate. Maine was one of two states that established this "opt-in" standard of privacy online.

This is the standard for internet privacy that we should build upon. Only one bill before the committee today, LD 1822, builds upon the high privacy standards Maine set in 2019. This bill recognizes the high sensitivity of personal health data and biometric identifiers and sets a high bar for the use

**Maine Broadband Coalition Testimony**  
**In SUPPORT of LD 1822**  
**and in OPPOSITION to LD 1088 and LD 1224**  
May 5, 2025



of that data. It gives the individual the freedom to choose what data they share, and gives them the freedom to take action if their rights are violated.

We have already seen the misuse of these types of data, such as the purchase of personal health data by politically-motivated actors who seek to influence individual behaviors. Biometric identifiers can be used to profile individuals, track their movements in public places, and are the basis of the police state in other, less democratic countries. We also appreciate that this bill makes no special exception or distinction for how the data was collected. Technology companies scraping your data from your browsing history, where you navigate in your car, videos you post to social media and emails you send should not get a free pass to exploit the data they harvest from you. **We ask you to support LD 1822.**

Unfortunately, LD 1088 and LD 1224 do not yet meet the high standards for privacy that Mainers and this committee want to see. The bill was written to repeal the strong privacy protections of the 2019 ISP privacy law, and would otherwise codify Big Tech's current practices, requiring very little change or accountability. These bills are largely copy-pasted from bills that Charter, Facebook, and other tech companies are trying to pass in the states, as the FTC and Congress have failed to take any action that protects the users they exploit. This draft does improve upon some of the industry practices, but its enforcement provisions are so weak that the bill would have no positive effect on the practices of these companies.

Here's some of what's in the bill:

- Returns to the "Notice and Consent" standard for most types of data, where providers of services force you to sign your rights away as part of a long "terms of service" (ToS) document. This is distinct from the Opt-In approach Maine took in the ISP privacy law, which this bill would repeal.
- It gives companies broad discretion to collect any of your data that they can, not just what is necessary to provide you the service you are trying to use.
- It allows companies to discriminate against users who opt-out of privacy protections, by charging them more or refusing them service.

Maine Broadband Coalition Testimony  
In SUPPORT of LD 1822  
and in OPPOSITION to LD 1088 and LD 1224  
May 5, 2025



- Requires the Maine Attorney General to give tech companies a warning before taking any enforcement action, and gives those companies a very low burden of proof that they've complied.
- Prohibits individuals from taking action against companies that violate their rights.

The big corporate ISPs that didn't like the precedent Maine set in 2019 challenged that law in court, claiming it was an unconstitutional violation of their free speech rights. They also complained that the law only applied to data that ISPs collect on users, not to data collected by data harvesters like Facebook, Amazon, and Google. On this point, we agree! The ISPs lost in federal court, paid Maine's Attorney General's costs, and dropped their appeal.

The timing of this conversation could not be more important, as thousands, if not tens of thousands, of Maine households are set to connect to high-speed broadband infrastructure for the very first time. When MBC conducted community outreach asking residents in every corner of the state about barriers to getting online, trepidation about online safety was consistently ranked as the primary concern around using the internet. The usage of private data is at the core of this sentiment. As telehealth, remote work, and educational opportunities continue to shift online, let's assure Mainers that they can access essential services without their data being sold to the highest bidder.

We appreciate the effort by members of this legislature to tackle this issue. We believe we should go further to protect our citizens' privacy. We already have a strong foundation in law. Let's extend our opt-in standard to other tech platforms. We'd be happy to work with the sponsors and other members on strengthening the proposed bill. As written, however, **we urge you to vote Ought Not to Pass on LD 1088 and LD 1224**. We would be pleased to partner with the sponsors to improve the bill.

May 7, 2025

Senator Anne Carney  
Chair of the Maine Judiciary Committee  
3 State House Station  
Augusta, Maine 04333

Representative Amy Kuhn  
Chair of the Maine Judiciary Committee  
2 State House Station  
Augusta, Maine 04333

**RE: Letter in Opposition to Maine LD 1822**

Dear Chair Carney and Chair Kuhn:

On behalf of the advertising industry, we write to oppose Maine LD 1822.<sup>1</sup> We provide this letter to offer our non-exhaustive list of concerns about this bill. Our organizations support meaningful privacy protections for Maine residents. As described in more detail below, LD 1822 contains provisions that would make Maine's privacy law out-of-step with privacy laws in other states, thereby adding to the increasingly complex privacy landscape for both businesses and consumers across the country. Accordingly, we ask you to decline to advance the bill as drafted out of the Maine Judiciary Committee ("Committee").

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country that make up and support the digital economy. These companies range from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet and the digital economy, which accounted for 18 percent of total U.S. gross domestic product ("GDP") in 2024.<sup>2</sup> By one estimate, nearly 33,000 jobs in Maine are related to the ad-subsidized Internet.<sup>3</sup> We would welcome the opportunity to engage with the Committee further on the non-exhaustive list of issues with LD 1822 outlined here.

**I. Harmonization Across State Privacy Laws Fosters Consistency and Clarity for Consumers and Businesses**

If enacted, LD 1822 would make the state's approach to privacy an outlier in ways that would harm consumers and businesses of all sizes. Maine should instead focus its efforts on harmonizing the bill with the approach to privacy in other states. A patchwork of differing privacy standards across the states would create significant costs for businesses and consumers alike. Efforts to harmonize state privacy legislation with existing privacy laws are critical to minimizing costs of compliance and fostering similar privacy rights for consumers no matter where they live. Below we provide a non-exhaustive list of ways LD 1822 would deviate from the dominant approach to privacy across states:

---

<sup>1</sup> Maine LD 1822 (132<sup>nd</sup> Maine Legislature), located [here](#) (hereinafter, "LD 1822").

<sup>2</sup> John Deighton and Leora Kornfeld, *Measuring the Digital Economy*, INTERACTIVE ADVERTISING BUREAU, 8 (April, 2025), located at [https://www.iab.com/wp-content/uploads/2025/04/Measuring-the-Digital-Economy\\_April\\_29.pdf](https://www.iab.com/wp-content/uploads/2025/04/Measuring-the-Digital-Economy_April_29.pdf).

<sup>3</sup> *Id.* at 136 (estimating approximately 32,972 Internet-dependent jobs in the state of Maine).

- LD 1822 would include an overly restrictive limitation on personal data collection that would stifle the economy and impede the availability of data to improve products and services and combat fraud.
- LD 1822 would define “sensitive data” to include data elements no other state deems sensitive, would permit sensitive data processing only if “strictly necessary,” and would flatly ban sales of such data, which would harm consumers’ access to beneficial products and services.
- LD 1822 would require controllers to provide the names of their third-party business partners in responses to access requests, creating an onerous compliance requirement and competition concerns for controllers.
- LD 1822 would impose burdensome notice requirements on third parties that would not realistically account for ways in which these entities receive and process personal data.
- LD 1822 would include an untested “should have known” knowledge standard for determining minors’ ages, creating confusion and adopting an approach to “knowledge” taken in no other state or federal privacy law.

Compliance costs associated with divergent privacy laws are significant. To make the point: a regulatory impact assessment of the California Consumer Privacy Act of 2018 concluded that the initial compliance costs to California firms would be \$55 billion.<sup>4</sup> Another recent study found that a consumer data privacy proposal in a different state considering privacy legislation would have generated a direct initial compliance cost of \$6.2 billion to \$21 billion and ongoing annual compliance costs of \$4.6 billion to \$12.7 billion for the state.<sup>5</sup> Other studies confirm the staggering costs associated with varying state privacy standards. One report found that state privacy laws could impose out-of-state costs of between \$98 billion and \$112 billion annually, with costs exceeding \$1 trillion dollars over a 10-year period, and with small businesses shouldering a significant portion of the compliance cost burden.<sup>6</sup> Harmonization with existing privacy laws is essential to create an environment where consumers in Maine have privacy protections that are consistent with those in other states, while minimizing unnecessary compliance costs for businesses. Maine should not add to this compliance bill for businesses and should instead opt for an approach to data privacy that is in harmony with already existing state privacy laws.

## **II. Overly Restrictive Limitations on Data Collection Would Stifle the Economy**

LD 1822 includes data minimization terms that would permit collection of personal data only if reasonably necessary and proportionate “to provide or maintain a product or service specifically

---

<sup>4</sup> See State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations*, 11 (Aug. 2019), located at [https://dof.ca.gov/wp-content/uploads/sites/352/Forecasting/Economics/Documents/CCPA\\_Regulations-SRIA-DOF.pdf](https://dof.ca.gov/wp-content/uploads/sites/352/Forecasting/Economics/Documents/CCPA_Regulations-SRIA-DOF.pdf).

<sup>5</sup> See Florida Tax Watch, *Who Knows What? An Independent Analysis of the Potential Effects of Consumer Data Privacy Legislation in Florida*, 2 (Oct. 2021), located at <https://floridataxwatch.org/DesktopModules/EasyDNNNews/DocumentDownload.ashx?portalid=210&moduleid=34407&articleid=19090&documentid=986>.

<sup>6</sup> Daniel Castro, Luke Dascoli, and Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws* (Jan. 24, 2022), located at <https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws> (finding that small businesses would bear approximately \$20-23 billion of the out-of-state cost burden associated with state privacy law compliance annually).

requested by the consumer to whom the data pertains.”<sup>7</sup> This overly restrictive limitation on personal data collection would impede business’ ability to process data for the benefit of consumers and to enrich the availability of goods and services in the economy. The proposed data minimization term could impose significant limitations on the availability of personal data for developing new technologies, providing pertinent messaging and advertising to consumers, creating cost-effective and efficient services, and combatting fraud.

For example, the term would functionally prohibit the collection of personal data to develop new and innovative offerings unrelated to requested products, or to improve existing offerings, because controllers would be prohibited from collecting data outside of the context of providing a specific product or service requested by the consumer. The term would also hinder businesses from cross-selling products and services to their own customer base because collection of data for such a purpose would not necessarily be tied to a product or service the customer already knew about or requested specifically. The term could also impede the general availability of personal data for prospecting, *i.e.*, taking steps to find new customers who may be interested in a business’s products or services. In addition, the proposed term would severely inhibit third-party data sources from collecting personal data to further vital consumer fraud prevention efforts. As a result of this data minimization term, third-party fraud prevention services may be forced to refrain from collecting and making data available that Maine businesses rely on to prevent fraud, thereby making Maine consumers more susceptible to identity theft and other negative outcomes.

The vast majority of states that have passed a data privacy law permit businesses to collect and process personal data as reasonably necessary and proportionate to achieve the purposes for which the personal data was collected, as disclosed to the consumer.<sup>8</sup> LD 1822 would contradict this reasonable, majority approach, thereby subjecting Maine consumers to fewer benefits of data processing than their counterparts in nearby states and other parts of the country. Maine should take steps to align LD 1822’s data minimization terms with other states instead of adopting an onerous and untested approach to data collection and processing that could disadvantage Maine consumers and businesses.

### **III. LD 1822’s Restrictions on Sensitive Data Processing Would Hinder Delivery of Beneficial Services to Maine Consumers**

LD 1822 would prohibit a controller from collecting, processing, or sharing sensitive data concerning a consumer, unless the collection or processing is “strictly necessary to provide or maintain a specific product or service requested by the consumer.”<sup>9</sup> The bill would also flatly ban sales of sensitive data, without providing exceptions to this broad restriction for instances where consumers consent to sensitive data transfers or when such transfers are expected by consumers in the context of their relationship with controllers.<sup>10</sup> Given the bill’s definition of sensitive data, which includes data elements that no other state considers sensitive (such as gender identity),<sup>11</sup> the proposed limitation on sensitive data processing and sales would severely hinder the delivery of beneficial products and services to Maine consumers. Instead of advancing this broad proposal, the Committee should amend

---

<sup>7</sup> LD 1822 at at Sec. 9608(2)(A).

<sup>8</sup> *See, e.g.*, Cal. Civ. Code § 1798.100(c); Va. Code Ann. § 59.1-578(1).

<sup>9</sup> LD 1822 at Sec. 9608(1)(A).

<sup>10</sup> *Id.* at Sec. 9608(1)(B).

<sup>11</sup> *Id.* at Sec. 9602(34).

the bill to mirror approximately 20 other state privacy laws that have been enacted to date by requiring consumer consent to process sensitive data.

Sensitive data is processed and transferred (i.e., “sold”) to provide consumers with messaging about various products and services from which they derive significant benefits. Without the ability to “sell” and process sensitive data for advertising purposes subject to consumer consent, businesses will have a more difficult time, and face higher costs, reaching individuals with relevant marketing. For example, the provisions in LD 1822 could functionally prohibit religious organizations from reaching out to potential new parishioners and bespoke cultural product providers from reaching individuals of particular ethnicities with messaging and advertising about their products. The ability to use this data to advertise is also especially meaningful for Maine’s small and medium-sized businesses who provide products and services that may be particularly relevant to specific constituencies.

The bill’s ban on sensitive data sales and extreme limits on processing would also have other downstream effects. For instance, precise location data—a type of sensitive data under the bill—powers important emergency notices, particularly AMBER alerts and severe weather notices, allowing these notices to be immediately displayed to users in the impacted area on any device they are using. Location information also enables effective fraud prevention to protect consumers and businesses. Financial institutions, retailers, and others rely on anti-fraud services that include location information provided by third parties. The “sale” and processing of location information allows anti-fraud and identity protection services to flag suspicious behavior and protect vulnerable communities. For example, companies can more easily detect credit card theft or fraud if they or their service providers have access to location information showing that a consumer is not in the location where a purchase is being made. However, such processing may not be “strictly necessary” for providing a product or service requested by a consumer, and therefore, could be outlawed if LD 1822 becomes law. As a result, the Committee should update the bill to remove the onerous limits on sensitive data processing and the ban on sensitive data sales. The Committee should replace these provisions with a requirement for controllers to obtain consumer consent to process sensitive data.

#### **IV. LD 1822 Would Diverge from Existing Privacy Laws by Requiring Controllers to Disclose the Names of Specific Third-Party Partners**

Another way LD 1822 diverges from existing state privacy laws is that it would require controllers to disclose the names of their third-party partners in response to a consumer access request.<sup>12</sup> The overwhelming majority of state privacy laws require companies to disclose the *categories* of third parties to whom they transfer personal data rather than the specific names of such third parties themselves in response to access requests.<sup>13</sup> Requiring disclosure of the names of entities would provide little to no benefits to consumers, would not materially enhance consumers’ understanding of controllers’ data practices, and would be operationally burdensome, as controllers change business partners frequently, and companies regularly merge with others and change names. For instance, a controller may engage in a data exchange with a new business-customer on the same day it responds to a consumer disclosure request. This requirement would either force the controller to refrain from engaging in commerce with the new business-customer until its consumer access

---

<sup>12</sup> *Id.* at Sec. 9606(1)(F).

<sup>13</sup> *See, e.g.,* Cal. Civ. Code § 1798.110; Va. Code Ann. § 59.1-578(C); Colo. Rev. Stat. § 6-1-1301(1)(a); Utah Rev. Stat § 16-61-302(1)(a).

disclosures are updated, or risk violating the law. This is an unreasonable restraint. From an operational standpoint, constantly updating a list of all third-party partners a controller works with would take significant resources and time away from companies' efforts to comply with other new privacy directives in LD 1822.

Even international privacy standards like the European Union's General Data Protection Regulation ("GDPR") do not require burdensome disclosures of specific third parties in response to data subject access requests, according to the text of the law. Mandating that companies disclose the names of their third-party partners could obligate companies to abridge confidentiality clauses they maintain in their contracts with partners and expose proprietary business information to their competitors. Finally, the consumer benefit that would accrue from their receipt of a list of third-party partners to whom a controller discloses data would be minimal at best where the cost clearly outweighs the benefit. For these reasons, we encourage you to reconsider this onerous requirement, which severely diverges from the approach to required disclosures taken in existing state privacy laws.

\* \* \*

We and our members strongly support meaningful privacy protections for consumers. We believe, however, that LD 1822 will not further meaningful consumer protections in Maine and instead will diverge significantly from other state privacy laws in ways that will hinder Maine consumers' access to digital resources. We therefore respectfully ask the Committee to decline to advance LD 1822 as proposed.

Thank you for your consideration of this letter.

Sincerely,

Christopher Oswald  
EVP for Law, Ethics & Govt. Relations  
Association of National Advertisers  
202-296-1883

Alison Pepper  
EVP, Government Relations & Sustainability  
American Association of Advertising Agencies, 4As  
202-355-4564

Michael Hahn  
EVP & General Counsel  
Interactive Advertising Bureau  
212-380-4700

Clark Rector  
Executive VP-Government Affairs  
American Advertising Federation  
202-898-0089

Lou Mastria  
CEO  
Digital Advertising Alliance  
347-770-0322

CC: Maine Judiciary Committee

Mike Signorelli, Venable LLP  
Allie Monticollo, Venable LLP

Chris Oswald  
Advertising Trade Associations  
LD 1822

Dear Chair Carney and Chair Kuhn:

Please find attached a letter from the following advertising trade associations in opposition to LD 1822: the Association of National Advertisers, the American Association of Advertising Agencies, the American Advertising Federation, the Interactive Advertising Bureau, and the Digital Advertising Alliance. We appreciate your consideration of this letter.

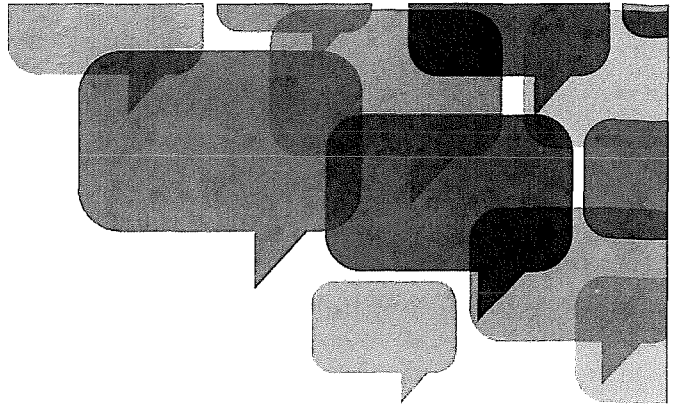
If you have any questions about this letter, please feel free to reach out to Chris Oswald at [coswald@ana.net](mailto:coswald@ana.net).

Best Regards,  
Chris Oswald



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

45 Melville Street, Suite 1  
Augusta, ME 04330  
Phone: 207.623.1149  
[www.retailmaine.org](http://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](mailto: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](mailto: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

Roger Pomerleau  
Retail Association of Maine  
LD 1822

Please oppose LD 1822: It goes too far and hurts small businesses. It is in conflict  
with what other states are doing. LD 1224  
makes Maine competitive with other states. I support LD 1224.



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.<sup>1</sup> 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.

---

<sup>1</sup> *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.<sup>2</sup> 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.<sup>3</sup> 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.<sup>4</sup>

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.<sup>5</sup> In 2017, an online search for the abortion medication misoprostol was used to charge one woman with second-degree murder.<sup>6</sup> In 2015, a series of text messages with a friend about getting an abortion helped convict another woman of feticide and child neglect.<sup>7</sup>

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

---

<sup>2</sup> 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>.

<sup>3</sup> *Id.*

<sup>4</sup> 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](https://www.wyden.senate.gov/imo/media/doc/signed_near_letter_to_ftc_and_sec.pdf).

<sup>5</sup> 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>.

<sup>6</sup> 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/>.

<sup>7</sup> 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."<sup>8</sup>

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

---

<sup>8</sup> 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-burnill/>.

data.<sup>9</sup> 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.<sup>10</sup>

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.<sup>11</sup>

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.

---

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

<sup>10</sup> 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/>.

<sup>11</sup> 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.

The Honorable Anne Carney, Senate Chair  
The Honorable Amy Kuhn, House Chair  
Joint Committee on Judiciary  
Maine Legislature

May 5, 2025

Re: LD 1822 – the Maine Online Data Privacy Act

Dear Senator Carney, Representative Kuhn, and Distinguished Committee Members,

Thank you for the opportunity to comment on LD 1822, which would enact the Maine Online Data Privacy Act. While ACLI appreciates the inclusion of a safe harbor in Section 9604(1)(G) of the bill for insurance licensees, we respectfully request that you consider revising the exemption such that it would not subject insurers to unnecessary, complicated, and potentially harmful dual regulation.

ACLI is proud of the fact that the insurance industry has been and continues to be the conscientious and responsible guardian of customers' highly vulnerable personal information. Insurers collect and use personal information for the benefit of consumers and industry alike – to know and understand individuals for purposes of recommending appropriate products, effective risk management, compliance with a complex array of federal, state, and sector-specific laws and regulations, and perform other essential business functions such as underwriting applications, paying claims, providing customer service, combating fraud, and offering investment and retirement products. Personal information is also fundamental to insurers' ability to provide the innovative insurance and financial products that consumers seek. Our industry has judiciously managed consumers' confidential medical and financial personal information for decades.

Appropriately, insurers have long been subject to comprehensive federal and state privacy laws and regulations, including the GLBA, arguably one of the most comprehensive information privacy laws to date, the Maine Insurance Information and Privacy Protection Act (Title 24-A, Chapter 24), and the Maine Insurance Data Security Act (Title 24-A, Chapter 24-B). These existing federal and state requirements provide a complex, broad, and rigorous regulatory framework that requires our industry to protect the privacy, use, and security of customers' personal information. They reflect a critically important balance between consumers' legitimate privacy concerns and the proper use of personal information to the benefit of existing and prospective customers. ACLI members recognize their affirmative and continuing commitment to respect consumer privacy through transparency in the collection, use, and disclosure of personal information.

---

American Council of Life Insurers | 101 Constitution Ave, NW, Suite 700 | Washington, DC 20001-2133

---

The American Council of Life Insurers (ACLI) is the leading trade association driving public policy and advocacy on behalf of the life insurance industry. 90 million American families rely on the life insurance industry for financial protection and retirement security. ACLI's member companies are dedicated to protecting consumers' financial wellbeing through life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, and dental, vision and other supplemental benefits. ACLI's 280 member companies represent 94 percent of industry assets in the United States.

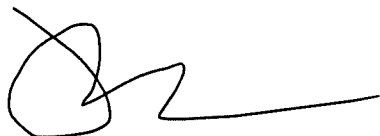
The Bureau of Insurance properly and ably regulates insurance licensees and enforces all applicable laws and regulations, including those relating to consumer data privacy. The proposed safe harbor for insurance licensees in LD 1822 would subject them to dual regulation by the attorney general. The safe harbor may be read to provide the attorney general with the authority to determine whether an insurance licensee is "is in compliance with any applicable data security and data privacy requirements of Title 24-A" such that it is exempt from the Act. Whether an insurance licensee is compliant with Title 24-A is a determination properly made by the Bureau of Insurance.

ACLI respectfully requests that the Committee exempt any data, entity, or affiliate of an entity subject to the Gramm-Leach-Bliley Act from the scope of LD 1822. The GLBA serves as a critical safeguard for consumer privacy within the life insurance sector, emphasizing transparency, confidentiality, and security obligations. Its provisions, including clear privacy notices and robust data safeguards, underscore the protection of nonpublic personal information. An entity-level GLBA exemption would align Maine regulations with existing federal standards, promoting efficiency, cost-effectiveness, and a harmonized approach to consumer protection across federal and state financial service sectors and business operations.

If the Committee is not willing to exempt entities subject to the GLBA, then ACLI requests that the bill be revised to exempt any licensee under Title 24-A, section 2263, subsection 8.

Thank you for considering our comments. Please contact me with any questions you may have.

Sincerely,

A handwritten signature in black ink, consisting of a large, stylized 'J' followed by a horizontal line and a small flourish.

Jill Rickard  
American Council of Life Insurers  
Regional Vice President—State Relations  
202-624-2046 t  
jillrickard@acli.com



## MAINE COMMITTEE ON JUDICIARY

### MEMORANDUM IN OPPOSITION TO LD 1822 (HP 1220)

May 5, 2025

RMAI is a trade association of over 600 members composed of banks, non-bank lenders, debt buyers, and the companies that support them. These are primarily financial institutions under the Gramm-Leach-Bliley Act ("GLBA").

Respectfully, RMAI opposes LD 1822.

#### **LD 1822 WILL CONFUSE BUSINESSES AND CONSUMERS**

LD 1822 creates a situation where financial institutions' data subject to the Gramm-Leach-Bliley Act ("GLBA") would be exempt, but the financial institutions themselves would not be exempt. This is problematic.

First, if financial institutions would be subject to the act but their data would not, it raises practical and unaddressed questions for businesses and consumers:

- Would a financial institution technically be exempt from the act if it only collects and processes GLBA-exempt data?
- If not, with which provisions must it comply?
- Must it develop costly compliance procedures to receive and respond to consumer requests?
- If so, will consumers be confused when their requests are denied because all the data is GLBA-exempt?

Second, sixteen states that have adopted comprehensive consumer data privacy acts exclude both financial institutions *and* data that are subject to the GLBA. Providing an exemption only for GLBA data therefore creates an unnecessary compliance anomaly with additional burdens, as well as enforcement risk associated with the unaddressed questions discussed above.

Third, financial institutions subject to the GLBA should be exempt because they are already highly regulated at the federal level:

- The GLBA Privacy Rule<sup>1</sup> addresses consumers' privacy rights. The Privacy Rule:
  - Requires a financial institution to provide notice to customers about its privacy policies and practices;
  - Describes when a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and
  - Provides a method for consumers to opt out of such sharing.<sup>2</sup>

---

<sup>1</sup> 16 C.F.R. § 313.1, *et seq.*

<sup>2</sup> 16 C.F.R. § 313.1(a).



- The GLBA Safeguards Rule,<sup>3</sup> as the name implies, requires financial institutions to implement safeguards sufficient to protect consumers' nonpublic personal information.
- Section 1033 of the Dodd-Frank Act<sup>4</sup> requires that financial institutions provide consumers with access to their information relating to financial products or services that have been provided.

For these reasons, RMAI respectfully recommends the following amendment following subparagraph H of subsection 1 of section 9604:

I. A financial institution or an affiliate of a financial institution as defined by and that is subject to the federal "Gramm-Leach-Bliley Act", 15 U.S.C. sec. 6801 et seq., as amended, and implementing regulations, including Regulation P, 12 CFR 1016.<sup>5</sup>

Thank you for your time and consideration, and please let us know if we can be of assistance or answer any questions.

David Reid  
General Counsel  
Receivables Management Association  
International  
1050 Fulton Avenue, Suite 120  
Sacramento, CA 95825  
916-779-2492  
[dreid@rmaintl.org](mailto:dreid@rmaintl.org)

Eric Rosenkoetter  
Outside Counsel, CIPP-US  
Maurice Wutscher LLP  
13785 Research Blvd., Suite 125  
Austin, TX 78750  
512-672-7068  
[erosenkoetter@mauricewutscher.com](mailto:erosenkoetter@mauricewutscher.com)



---

<sup>3</sup> 16 C.F.R. § 314.1, *et seq.*

<sup>4</sup> 12 U.S.C. § 5533.

<sup>5</sup> See, for example, Colo. Rev. Stat. § 6-1-1304(2)(q).



May 12, 2025

Chair Anne Carney  
Chair Amy Kuhn  
Joint Standing Committee on the Judiciary  
Maine Legislature  
100 State House Station  
Room 438  
Augusta, ME 04333

Re: Maine L.D. 1822, Maine Data PrivacyProtection Act — *SUPPORT*

Dear Chair Carney and Chair Kuhn,

Consumer Reports<sup>1</sup> strongly supports L.D. 1822, which would provide Maine consumers with privacy protections matching those in some of the strongest state laws passed to-date. The bill would require businesses to abide by meaningful data minimization provisions, which would prevent them from collecting information that is not reasonably necessary to provide the specific product or service requested by consumers. It would also extend to Maine consumers important new protections relating to their personal information, including prohibitions against collecting, processing, or sharing sensitive data unless it is strictly necessary, a ban on the sale of sensitive data, restrictions against targeting advertisements to children, and more.

These provisions largely reflect the last several years of work on privacy legislation around the states, adopting targeted improvements made in other state privacy laws that incorporate feedback from regulators tasked with enforcing these laws,<sup>2</sup> as well as other key stakeholders.

---

<sup>1</sup> Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

<sup>2</sup> Connecticut Attorney General, Report to the General Assembly's Joint General Laws Committee, February 1, 2024, [https://portal.ct.gov/-/media/ag/press\\_releases/2024/ctdpa-final-report.pdf?rev=8fbba0ba237a42748d3ad6544fd8228c&hash=41BCE2F7485413487EE5F534E6AC6C60](https://portal.ct.gov/-/media/ag/press_releases/2024/ctdpa-final-report.pdf?rev=8fbba0ba237a42748d3ad6544fd8228c&hash=41BCE2F7485413487EE5F534E6AC6C60); Connecticut Attorney General, Updated Enforcement Report Pursuant to Connecticut Data Privacy Act, April 17, 2025,

Under current law, consumers possess very limited power to protect their personal information in the digital economy, while online businesses operate with virtually no limitations as to how they collect and process that information (so long as they note their behavior somewhere in their privacy policy). As a result, companies have amassed massive amounts of data about consumers, which is often combined with their offline activities to provide detailed insights into their most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is often retained for indeterminate amounts of time, sold as a matter of course, and is used to deliver targeted advertising, facilitate individual pricing, and enable opaque algorithmic scoring—all of which, aside from reducing individual autonomy and dignity, can result in concrete harms for consumers, financial and otherwise.<sup>3</sup>

L.D. 1822 corrects that imbalance by establishing strong privacy protections over consumers' personal information. In particular, we appreciate that L.D. 1822 includes:

### **Strong Data Minimization Provisions**

First and foremost, this bill's data minimization provision (Section 9608(2)), which is aligned with Maryland's recently passed privacy law and concurrent efforts in several other states,<sup>4</sup> would go a long way toward mitigating the rampant over-collection of consumer data that has led to a panoply of consumer harms.<sup>5</sup> A strong privacy law should limit the data companies can collect to match what consumers expect based on the context of their interaction with the business. For example, a mobile flashlight application should not be permitted to collect a consumer's precise geolocation information because such information is not necessary to provide the service requested and the collection of that data is unlikely to be in the consumer's interest.

In contrast, the core of the framework currently found in many state privacy laws — and the other privacy bills sitting before the committee (LD 1224 and LD 1088) — is “notice-and-choice,” which focuses on disclosures in privacy policies. This framework allows

---

[https://portal.ct.gov/-/media/ag/press\\_releases/2025/updated-enforcement-report-pursuant-to-connecticut-data-privacy-act-conn-gen-stat--42515-et-seq.pdf](https://portal.ct.gov/-/media/ag/press_releases/2025/updated-enforcement-report-pursuant-to-connecticut-data-privacy-act-conn-gen-stat--42515-et-seq.pdf)

<sup>3</sup> Office of the Texas Attorney General, Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies, (January 13, 2025),

<https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf>

<sup>4</sup> E.g., Vermont H. 207, Connecticut S.B. 1356, (as passed by the Joint General Laws Committee), Massachusetts H. 78/S.45/S.29/H.104

<sup>5</sup> See, e.g., Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024),

[https://www.ftc.gov/system/files/ftc\\_gov/pdf/2123035gravyanalyticscomplaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf); Consumer Financial Protection Bureau, Protecting Americans from Harmful Data Broker Practices (Regulation V), Proposed Rule; request for public comment, (December 3, 2024),

[https://files.consumerfinance.gov/f/documents/cfpb\\_nprm-protecting-ams-from-harmful-data-broker-practices\\_2024-12.pdf](https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf)

businesses to continue collecting whatever personal data they want and using it for any reason they want as long as they disclose those practices in their privacy policies and allow consumers to opt out. However, very few consumers have the time to read privacy policies in practice, and would likely struggle to decipher their lengthy legalese even if they did. Moreover, the opt-out framework offloads all of the burden of consumer protection onto consumers themselves, while absolving companies of the responsibility to engage in responsible data collection. Rather than continue with this approach that harms consumers, LD 1822 appropriately sets out a rule that businesses can only collect and use data when it is “reasonably necessary” to provide the services the consumer asks for.

Ultimately, we prefer privacy legislation that also limits companies’ *use* and *disclosure* of data to what is reasonably necessary to provide the service requested by the consumer. Unlike Representative O’Neill’s LD 1977 from last year, LD 1822 only currently applies this standard to data collection, while allowing a much looser standard for processing activities. But simply reining in systemic overcollection of consumers’ personal information alone would help eliminate common practices that have contributed to persistent surveillance that threatens individuals’ physical safety and autonomy,<sup>6</sup> leads to a persistent drip of massive data breaches that facilitate identity theft and other scams,<sup>7</sup> and further embeds Big Tech’s undemocratic control over society.<sup>8</sup>

### **Sensitive Data Protections**

Companies should not be profiting from the sale of consumers’ most personal data, such as children’s data or data about a consumer’s race, religion, sex life, finances, precise geolocation, or health. The bill appropriately bans this behavior, as opposed to the more permissive opt-in framework found in LDs 1224 and 1088.

While industry will argue that opt-ins are sufficient (some even arguing that they are *more* consumer friendly than a blanket ban), the reality is that opt-in frameworks aren’t working to protect consumers’ sensitive data in state privacy laws that include these provisions. Because

---

<sup>6</sup> See, e.g. Justin Sherman, Lawfare, People Search Data Brokers, Stalking, and ‘Publicly Available Information’ Carve-Outs, (October 30, 2023), <https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs>; Office of Senator Ron Wyden, Wyden Reveals Phone Data Used to Target Abortion Misinformation at Visitors to Hundreds of Reproductive Health Clinics, (February 13, 2024), <https://www.wyden.senate.gov/news/press-releases/wyden-reveals-phone-data-used-to-target-abortion-misinformation-at-visitors-to-hundreds-of-reproductive-health-clinics>

<sup>7</sup> Farhad Manjoo, the New York Times, Seriously, Equifax? This Is a Breach No One Should Get Away With, September 8, 2017, <https://www.nytimes.com/2017/09/08/technology/seriously-equifax-why-the-credit-agencys-breach-means-regulation-is-needed.html>

<sup>8</sup> Adrienne LaFrance, The Atlantic, The Rise of Technoauthoritarianism, January 30, 2024, <https://www.theatlantic.com/magazine/archive/2024/03/facebook-meta-silicon-valley-politics/677168/>

companies aren't typically required to separate their request for consent for necessary processing (e.g. data collection) from unnecessary processing (e.g. data sales), consumers are still often presented with take-it-or-leave-it choices that don't leave them any better off than before. Furthermore, last year CR released a report on sensitive data opt-in provisions and found that some companies appeared to be ignoring their responsibility to obtain opt-in consent or continued to share our personal data even when we declined to opt-in.<sup>9</sup> To our knowledge, there hasn't been a single enforcement action related to this provision under existing state privacy laws. And ultimately, the solution to this issue isn't more consent boxes; consumers need stronger baseline protections.

Some examples of harmful uses of consumers' sensitive data include:

- *Scamming, stalking, and spying.* Fraudsters and other bad actors can use sensitive data to target vulnerable individuals for scams, or otherwise use personal information to cause harm. For example, scammers can use commercially available location data to increase the specificity of their phishing or social engineering scams, such as by including location-specific details, like mentioning a nearby business or the individual's recent activity.<sup>10</sup> Location data brokers are also commonly used by abusive individuals to locate people, hunt them down, and stalk, harass, intimidate, assault, or even murder them.<sup>11</sup>
- *Predatory use of consumer data.* The sale of consumer data can result in financially disastrous consequences for consumers. Some data brokers sell lists of consumers sorted by characteristics like "Rural and Barely Making It" and "Credit Crunched: City Families," which can be used to target individuals most likely to be susceptible to scams or other predatory products. And a recent case brought by the Texas Attorney General alleged that the insurance company Allstate secretly purchased information about consumers' driving behaviors (including their precise geolocation data), which it used in some cases to raise consumers' premiums or deny them coverage altogether.<sup>12</sup> They also sold the driving data to several other insurance companies without consumers' knowledge or consent.

---

<sup>9</sup> Maggie Oates et al., Consumer Reports, Companies Continue to Share Health Data Despite New Privacy Laws,

<sup>10</sup> Phishing Box, Tracking Data: Identifying the Anonymized, January 16, 2024, <https://advocacy.consumerreports.org/wp-content/uploads/2024/01/Companies-Continue-to-Share-Health-Data-1-16-2024-Consumer-Reports.pdf>

<sup>11</sup> Justin Sherman, Lawfare, People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs, (October 30, 2023), <https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs>

<sup>12</sup> Office of the Texas Attorney General, Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies, (January 13, 2025), <https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf>

Moreover, online and in-person retailers can use information about individuals' location, demographics, finances, and more to make inferences about them that are then used to set individualized prices. Some grocery chains, such as Kroger, already collect this type of information on consumers and have sold it to third-parties as part of their "alternative profit" business lines.<sup>13</sup> Last year, the Federal Trade Commission released initial findings from its Surveillance Pricing study, confirming that sensitive data categories can be a key input of individualized prices shown to consumers.<sup>14</sup>

- *Tracking of sensitive locations.* Location information can be used to track individuals' visits to especially sensitive locations, such as reproductive or mental health facilities,<sup>15</sup> political rallies,<sup>16</sup> religious facilities,<sup>17</sup> and more. This information is often sold (or in some cases, inadvertently shared)<sup>18</sup> by app developers to data brokers, who then re-package the information and sell it to a variety of third-parties, including advertisers, political extremist groups, and law enforcement. The Federal Trade Commission has recently enforced against several location data brokers, including one that allegedly maintained and sold access to nearly 2,000 lists of individuals sorted by characteristics they had inferred from their collection of location data, including categories such as "parents of preschoolers," "Christian church goers," and "wealthy and not healthy."<sup>19</sup>
- *Data breaches.* Data brokers sit on trillions of data points, many of them sensitive and purchased from other businesses. Unsurprisingly, this makes them a top target for hackers and cyber criminals. For example, the data broker Gravy Analytics, which has claimed to "collect, process and curate" more than 17 billion signals from people's smartphones

---

<sup>13</sup> Jon Keegan, the Markup, Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You, (February 16, 2023), <https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you>

<sup>14</sup> Federal Trade Commission, FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices, (January 17, 2025), <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer>

<sup>15</sup> Office of Senator Ron Wyden, Wyden Reveals Phone Data Used to Target Abortion Misinformation at Visitors to Hundreds of Reproductive Health Clinics, (February 13, 2024), <https://www.wyden.senate.gov/news/press-releases/wyden-reveals-phone-data-used-to-target-abortion-misinformation-at-visitors-to-hundreds-of-reproductive-health-clinics>

<sup>16</sup> Charlie Warzel and Stuart A. Thompson, New York Times, How Your Phone Betrays Democracy, (December 21, 2019), <https://www.nytimes.com/interactive/2019/12/21/opinion/location-data-democracy-protests.html>

<sup>17</sup> Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers>

<sup>18</sup> Joseph Cox, Wired, Candy Crush, Tinder, MyFitnessPal: See the Thousands of Apps Hijacked to Spy on Your Location, (January 9, 2025), <https://www.wired.com/story/gravy-location-data-app-leak-rtb/>

<sup>19</sup> *Id.*

every day,<sup>20</sup> reportedly suffered a massive data breach that may have leaked the location data of millions of individuals.<sup>21</sup> This type of data makes it trivially easy to reconstruct the everyday comings and goings of individuals, politicians, and even servicemembers.<sup>22</sup>

### **Appropriately Scoped Non-discrimination Provisions**

Not only does the non-discrimination language in Section 9608 clarify that consumers cannot be charged for exercising their rights under the law, but it makes it clear that legitimate loyalty programs, that reward consumers for repeated patronage, are supported by the bill.

At the same time, there are a few provisions that we recommend the drafters tweak in order to provide the level of protection that Maine consumers deserve:

### **Include Strong Enforcement Provisions**

While we understand the importance of balancing the equities at stake in privacy legislation, consumers should be able to hold companies accountable in some way for violating their rights. As the representative from the Maine Attorney General's Office outlined in his testimony,<sup>23</sup> AG-only enforcement is likely to be insufficient. Unfortunately, most state Attorney General offices are underresourced and do not have the capacity to bring enough actions to meaningfully deter illegal behavior, meaning consumers may have no recourse in the event of a violation that harms them. Despite ample evidence suggesting widespread non-compliance with existing privacy laws,<sup>24</sup> there have not been commensurate enforcement efforts to-date. Consumer Reports has put out a number of reports demonstrating noncompliance with state privacy laws, including a report from earlier this month showing that many companies were showing targeted

---

<sup>20</sup> Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/2123035gravyanalyticscomplaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf)

<sup>21</sup> Joseph Cox, 404Media, Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data, (January 7, 2025), <https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/>

<sup>22</sup> Justin Sherman et al., Duke Sanford School of Public Policy, Data Brokers and the Sale of Data on U.S. Military Personnel, (November 2023), <https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf>

<sup>23</sup> Aaron Frey, Maine Attorney General's Office, Testimony in Support of LD 1822, (May 5, 2025) <https://legislature.maine.gov/testimony/resources/IUD20250505Frey133909563028562659.pdf>

<sup>24</sup> See, e.g. two separate studies indicating that less than 30 percent of top websites comply with universal opt-out requests: Privado, State of Website Privacy Report 2024, (December 2024), <https://www.privado.ai/state-of-website-privacy-report-2024>; Data Grail, Data Privacy Trends Report, <https://www.datagrail.io/resources/interactive/data-privacy-trends/>, (December 2024)

ads despite receiving legally binding universal opt-out signals.<sup>25</sup> Yet, to our knowledge, there are more states with active comprehensive privacy laws (13) than there have been public enforcement actions. It is therefore unsurprising that market behavior has yet to improve.

While we think an allowance for both public and private enforcement mechanisms would make sense — dozens of other consumer protection laws do the same — and are generally skeptical of claims that such an approach would open the floodgates to frivolous litigation, we are open to discussing guardrails to prevent that outcome if raised in good-faith. We would also support limited exclusions from the private right of action for small businesses, as is being considered in Vermont's H. 208.<sup>26</sup>

### **Mandate the Universal Opt-Out**

Section 9608(6) currently provides that “a controller may satisfy the controller's obligation under this subsection to establish a secure and reliable mechanism for a consumer to exercise the right to opt out under subsection 5” by **either** providing an accessible link **or** allowing a consumer to opt-out via an opt-out preference signal (OOPS). None of the 13 currently effective state privacy laws that allow consumers to opt-out via an OOPS provide this sort of optionality. OOPSs allow consumers to broadcast to businesses they interact with online their preference to opt out from their personal information being sold or shared with third parties through a simple toggle. Otherwise, consumers must hunt down and navigate divergent opt-out processes for potentially thousands of different companies, which is simply not tenable. Changing the “or” in Section 9608(6)(C)(1) to an “and,” would resolve this issue, which does not appear to be intentional on the part of the drafters.

### **Remove Entity Level Exemptions**

The bill currently exempts from coverage any financial institution or an affiliate of a financial institution, as well as covered entities and business associates under the Health Insurance Portability and Accountability Act. These carveouts arguably make it so that large tech companies (Apple, Amazon, Google, Facebook, and Microsoft) would be exempted from the entire bill if one arm of their business receives enough financial information from banks or crosses the threshold into providing traditional healthcare services, a line many of them are already currently skirting.<sup>27</sup> At most, the bill should exempt *information* that is collected

---

<sup>25</sup> Matt Schwartz *et al.*, *Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws*, Consumer Reports, (Apr. 1, 2025), <https://innovation.consumerreports.org/Mixed-Signals-Many-Companies-May-Be-Ignoring-Opt-Out-Requests-Under-State-Privacy-Laws.pdf>

<sup>26</sup> Vermont H. 208, Section 2424(d)(2)(A), <https://legislature.vermont.gov/Documents/2026/Docs/BILLS/H-0208/H-0208%20As%20Introduced.pdf>

<sup>27</sup> See e.g., The Economist, “Big Tech Pushes Further into Finance,” (Dec. 15, 2022), <https://www.economist.com/business/2022/12/15/big-tech-pushes-further-into-finance>; Richard Waters,

pursuant to those laws, applying its protections to all other personal data collected by such entities that is not currently protected.

\*\*\*\*\*

We look forward to working with you to ensure that Maine consumers have the strongest possible privacy protections.

Sincerely,

Matt Schwartz  
Policy Analyst

Senator Carney, Representative Kuhn, and distinguished members of the judiciary committee,

My name is Myles Smith, I live in Portland, and I write today **in support of LD 1822**, and in **opposition to LD 1088, LD 1224, and LD 1294**.

I submit this testimony in my personal capacity. I am the former director of the Maine Broadband Coalition, which supported Maine's ISP data privacy law. I am disappointed, and not the least bit surprised, that Facebook, Charter/Spectrum, Google and other data miners and profiteers are back to lock in their faux privacy standards. I just spoke to friends with whom I worked to defend our privacy rights last year, who alerted me to these bills.

Before coming home to Maine a couple years ago, I spent almost two decades living and working in unfree societies in Eastern Europe and Central Asia. I spent much of that time supporting journalists and internet freedom defenders. While there, I saw the consequences of the unregulated collection and circulation of Internet user data by their governments.

We are not in that place quite yet. Here, corporations are doing as good a job or better of profiling us and our children and selling off those profiles to anyone. Governments have all the data they need to monitor and manipulate us, which can be freely bought for a miniscule price. Until recently, this data has been used to sell us things. Now, it is used to train machines to mimic our behaviors. Soon, user data profiles will be good enough to allow AI to mimic specific individuals. All the data needed to do this is freely collected by for-profit companies, from ISPs to social media platforms, from email providers and search engines providers to gaming and gambling sites.

These companies value us as a collection of data points. They can't see us any other way - their fiduciary responsibility to shareholders and the competitive billionaire leadership mindset affords no other way. We must value ourselves as free thinking and freely associating individuals. And our government must affirm our value if we're going to have any.

Americans are rapidly losing trust in their government's ability to act in the interest of the public. Folks see a government serving the needs of the wealthy and powerful. Data is now the currency of the powerful, and the easiest vehicle to access wealth.

This was clear in the work of the broadband coalition, where our polling data showed concerns about privacy as the top reason to avoid going online for anything. The

ability to protect oneself online is correlated to youth, wealth, and tech proficiency. This is unfair, unjust, and unsustainable.

Without some expectation of privacy on the communication platforms of society, we are not free. Privacy lets us develop ideas and new patents. Privacy allows us to think outside current social norms, which makes progress possible. Privacy enables investigating power and holding it to account. Soon, the only places where we will expect some privacy will be our own homes, with the curtains drawn and all devices unplugged, or on a walk in the woods. This was the limit of freedom in places like Turkmenistan and Russia.

I urge you to send a strong signal to Mainers that we care about their privacy, and that we will take steps to protect each other. This is a critical next step we can take, building on our ISP privacy law, to turn the corner towards freedom.

Myles Smith  
Portland, ME

**Testimony of Greg and Lauren Soutiea – Co-owners of the Craignair Inn by the Sea LLC and Causeway Restaurant in St. George Maine.**

--

Sen. Carney, Rep. Kuhn, and members of the Joint Standing Committee on Judiciary, my name is Greg Soutiea and together with my wife Lauren Soutiea, we have owned the Craignair Inn by the Sea and Causeway Restaurant in St. George for over 6 years now. We have grown the seasonal restaurant from 7 employees to now over 50 in peak season and a year-round restaurant giving us the opportunity to support 20+ of our staff with year-round jobs.

We wish to advocate **in support of LD 1224** “An Act to Comprehensively Protect Consumer Privacy.” We believe that LD1224 is a balanced approach that offers business-friendly framework while also protecting Maine residents and their privacy. It would provide clarity and align with neighboring New England states like NH, RI, and CT in their recent data privacy legislations.

We wish to advocate **in opposition of L.D. 1822** “An Act to Enact the Maine Online Data Privacy Act.” This would introduce significant changes and rules to Maine businesses that would be extremely difficult for us to comply with and continue our digital marketing strategies. This would put us at a disadvantage by limiting our ability to market to potential customers. It also would make Maine an outlier in this type of legislation as federal standards are beginning to take shape. Maine does not need to set such a high bar with this legislation such that it will be yet another requirement and disadvantage to Maine small businesses.

We are already looking at down projections for our hotel and restaurant this year with economic uncertainty, rising food/labor costs, and declining sentiment on summer travel by consumers. Further limiting our ability to market and reach potential customers will be harmful to ours and many other Maine businesses.

Testimony respectfully submitted on May 4th, 2025.

Greg Soutiea  
SPRUCE HEAD  
LD 1822

We wish to advocate in opposition of L.D. 1822 "An Act to Enact the Maine Online Data Privacy Act." This would introduce significant changes and rules to Maine businesses that would be extremely difficult for us to comply with and continue our digital marketing strategies. This would put us at a disadvantage by limiting our ability to market to potential customers. It also would make Maine an outlier in this type of legislation as federal standards are beginning to take shape. Maine does not need to set such a high bar with this legislation such that it will be yet another requirement and disadvantage to Maine small businesses.

# MAINE BANKERS

Association

May 5, 2025

## Testimony to the 132<sup>nd</sup> 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

**BRANN & ISAACSON**  
ATTORNEYS AND COUNSELORS AT LAW

STACY O. STITHAM | Managing Partner  
sstitham@brannlaw.com  
(207) 689-9740

May 5, 2025

Senator Anne Carney, Senate Chair  
Representative Amy Kuhn, House Chair  
Joint Standing Committee on Judiciary  
100 State House Station  
Augusta, ME 04333

Re: MSCC Testimony on LD 1224 & 1822

Senator Carney, Representative Kuhn, and Members of the Judiciary Committee:

I am Managing Partner at Brann & Isaacson, a Maine law firm which has, for decades, represented catalog companies, ecommerce entities, and other online and multichannel businesses on matters of relevance to the industry. In my personal practice, I advise companies in Maine and across the country with respect to their compliance obligations under state consumer privacy laws, and am CIPP/US certified by the International Association of Privacy Professionals. On behalf of the Maine State Chamber of Commerce ("Chamber"), I write in support of LD 1224, a privacy bill in harmony with those of other New England states, and in opposition to LD 1822, a bill that would make Maine an outlier in its treatment of personal information.

First and foremost, the Chamber welcomes the adoption of a consumer privacy bill, and appreciates the time, effort, and thoughtfulness that the Judiciary Committee has shown in considering this subject matter over the last year or more. The fact that there are three pending bills on consumer privacy in and of itself indicates that attention is rightly being paid to this topic.

Ideally, each and every one of my clients would like to see a comprehensive federal privacy bill that offers a single suite of consumer rights and a well-defined set of privacy policy requirements and procedures to guide business operations. Short of that, a uniform set of state privacy laws which offer consistency from region to region is the common goal. Commerce does not stop at the New Hampshire/Maine border, especially in an interconnected online ecosystem, and compliance burdens increase exponentially when states differ wildly in their expectations of consumer data handling.

May 5, 2025  
Page 2

It is in that light that I respectfully submit the Chamber's comments to you on LD 1224, which closely tracks the framework that other New England states, and at least 15 states across the country, have adopted. This framework now covers over 100 million Americans. LD 1224 represents a well understood and clearly laid out path, as opposed to a nonconformist bill that—while well intentioned—would result in unintended or untested consequences. LD 1224 ensures consumer control over personal data, establishes a fair enforcement mechanism, and aligns Maine's privacy structure with both New England and national standards.

**Sensitive Data.** LD 1224 requires *explicit, opt-in consent* before businesses can collect or process sensitive data such as race, health information, biometric data, precise geolocation, and immigration status. Accordingly, the bill allows for *consumers* to actively decide how their most private information is used, rather than businesses automatically collecting it by default.

In contrast, LD 1822 takes a less flexible approach, limiting the collection, processing and sharing of sensitive data to what is “strictly necessary” for providing a requested product or service. While clearly intended to be more consumer-protective, by shifting the focus from consumer consent to disclosed purposes to whatever the business can characterize as needed to provide “or maintain” a requested product or service, the bill actually eliminates consumer choice and control, and potentially leaves room for businesses to justify broad data collection practices without the consumer's clear, informed consent. Moreover, it potentially decimates the ability of certain businesses to do any meaningful advertising. Take, for example, the retailer of religious books or LGBTQ products. Because the very nature of any customer purchase may “reveal” religious beliefs or sexual orientation about an individual, the retailer could arguably be prohibited under LD 1822 from “sharing” this data with any marketing partners to the extent it is not “strictly necessary” to fulfill the original customer request—even if the customer would welcome advertisements for similar products from the retailer.

**Data Collection.** LD 1224 protects consumers from unnecessary data collection by requiring that businesses only collect data that is “*adequate, relevant, and reasonably necessary*” for the specific purpose disclosed to the consumer. Companies, therefore, are prevented from hoarding excessive consumer information, reducing privacy risks and the potential for data misuse. This is drawn from the same standard used in the California (CCPA/CPRA) and European (GDPR) privacy frameworks.

By contrast, LD 1822's experimental approach may ultimately give businesses more discretion by once more cutting the consumer out of the equation. Businesses are allowed to determine what data is “reasonably necessary and proportionate” to provide the “specific product or service requested by the consumer to whom the data pertains,” a standard that does not have the same well-established track record in other jurisdictions as the framework deployed by LD 1224. Not only does this give businesses greater discretion, the limiting language regarding the specific product or service requested by the consumer is likely to result in less access to new

May 5, 2025  
Page 3

products, services, updates to existing products, etc., that consumers have come to expect, and to which consumers elsewhere in New England will have access.

More specifically, LD 1822's framing puts in serious jeopardy the ability of companies to measure the digital advertising that they have purchased or sold. Without ad measurement, the value of digital advertising for both targeted ads *and* contextual ads is lost and the free and open Internet falls apart. Brick-and-mortar businesses, plumbers, banks, etc. would all have trouble reaching their existing customers or finding new ones.

Likewise, this provision puts in jeopardy the ability of companies to offer personalized services by default (e.g. which have not been explicitly "requested"). Personalization is what organizes the massive quantities of Internet-available information into something manageable and usable – making it easier and faster for everyone to find what's most helpful and meets their needs. It is the foundation for a positive online experience. You can see and feel the benefit of it in many ways, including the search results that appear in your native language; and the way that small businesses get help finding – and being found by – the right customers.

This uncertainty around the future of digital advertising will likely negatively impact Maine's small businesses and leave them at a disadvantage against their competitors in neighboring states. This is not because these businesses are processing much, if any, of their customers' data directly. Rather, these businesses are themselves the customers of large online advertising platforms, including platforms sending emails to potential customers. A recent survey conducted by the Retail Association of Maine in partnership with the Connected Commerce Council of small and mid-sized businesses which sell products or services to businesses and/or consumers, including 200 from Maine, concluded that 66% use data-driven online advertisements. 61% of these Maine businesses answered that without access to personalized ads and analytics, they wouldn't be able to reach new customers efficiently. Tools such as Google Analytics and Google Ads drive customers to specialty companies around Maine, from the eleven-employee blanket store in Portland (where 30-40% of sales are driven by Google Ads) to the fourth-generation mustard business in Eastport utilizing Google Analytics to assess how best to reach customers. *See* "Google Economic Impact," Maine State Report, *available at* <https://economicimpact.google/state/me/> (last visited May 2, 2025). While these companies may not be large enough to be directly regulated under LD 1822, they are heavily reliant on platforms that are, and their ability to take advantage of services from Google and others will be hindered by the passage of LD 1822 and its restrictions on the usage of Maine consumer data.

Responsible targeted advertising like that which is taking place every day under the New England privacy framework lowers costs for small businesses and allows them to reach their customer base. An incompatible privacy bill like LD 1822 risks raising advertising costs and making online advertising less accessible for small advertisers with small marketing budgets, who must carefully choose the right markets and audiences in which to spend their advertising dollars. Large national brands will always be able to afford national, blanket ad campaigns to sell their products, but Maine's small businesses need the tools to allow them to effectively compete.

May 5, 2025  
Page 4

**Other Concerns With LD 1822:**

- **Section 9602[34], Sensitive Data definition.** The characterization of “billing, financial or payment method information” as sensitive data is ambiguous and uncertain in scope. It could potentially encompass data regarding the price paid for a particular product or service, which is important to business analytics. At least two states already include certain financial information within the definition of sensitive data, New Jersey and California. They share very similar definitions: (1) “*financial information, which shall include a consumer’s account number, account log-in, financial account, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer’s financial account*” [New Jersey Data Protection Act] and (2) “*A consumer’s account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account*” [California Privacy Rights Act]. We would urge the adoption of either of these formulations in lieu of the current recitation, a replacement which would protect sensitive payment details without the potential to sweep in broad categories of other, non-sensitive billing-related information. (Note that this type of formulation can be found in the definitional section of LD 1088, Representative Henderson’s bill. *See* Section 9602 [26]G).
- **Section 9610, “Third-party” responsibilities.** This provision is problematic for several reasons. First, it assumes that third parties will know the exact promises and disclosures made to the consumer at the time of data collection. Third parties certainly receive assurances that they have the needed rights to use the data procured from another party but would likely not know the exact wording of each initial consumer notice. Second, in many cases, third parties will not have any means of contacting consumers because they do not have contact information for individuals. Ironically, in such circumstances, in order to comply with this provision, third parties would need to obtain *more* personal information on consumers than they otherwise would want – which cannot be the intent.
- **Section 9611 [2], Algorithm usage.** As with the majority of state consumer privacy statutes, LD 1822 contains an obligation to conduct a data protection assessment in instances where there is a heightened risk of harm to consumers. Confusingly, however, the bill adds that an assessment must be done “for each algorithm that is used.” Inasmuch as data protection assessments focus on the *purpose* and *effects* of data processing (i.e. for what reasons is a company handling personal data, and what are the benefits and risks to consumers in doing so?), it seems out of place to add a requirement

May 5, 2025  
Page 5

that an assessment must be done *whenever* an algorithm is used, which seems to be a question of *methodology*. The term “algorithm” in this context is not defined, and considering that the word can encompass any set of instructions or rules that can be followed to solve a problem, its inclusion here would easily transform this provision into the tail that wags the dog. To the extent that deployment of a particular algorithm in the context of data processing causes a risk to consumers, it will *already* be subject to these requirements. To the extent it does not, it is unclear why these extra steps should be taken. In addition to the likelihood that this clause may cause a significant increase in compliance burdens unrelated to any danger of consumer harm, algorithmic designs and operations are often trade secrets of companies, which makes their exposure in a data protection assessment subject to production to the Attorney General’s Office particularly alarming.

**Regional Alignment.** LD 1224 ensures that Maine businesses can follow consistent privacy rules across multiple states, including New Hampshire, Rhode Island, and Connecticut. By aligning with the regional framework, the bill reduces compliance burdens for businesses and ensures that consumers have the same privacy rights and protections as residents in neighboring states, while also receiving similar access to goods and services.

Aligning with New England’s privacy framework ensures that Maine consumers benefit from a harmonized set of privacy protections, rather than being subject to a patchwork of different rules that could weaken enforcement or create confusion. A regional approach enhances consumer rights by providing a predictable and enforceable privacy framework that encourages businesses to adopt uniform, high-standard data protection measures across multiple states. Consumers benefit from greater transparency, stronger enforcement mechanisms, and more effective privacy safeguards when laws are cohesive and consistent across jurisdictions.

LD 1822, in contrast, creates a Maine-specific privacy framework, forcing businesses to develop a separate compliance system solely for Maine—or to potentially avoid the Maine market altogether. This fragmented approach drives up costs for businesses and is likely to reduce the services available for Maine consumers.

Thank you for the opportunity to present these remarks on behalf of the Chamber, and your consideration of the same.

Very truly yours,

BRANN & ISAACSON



Stacy O. Stitham  
[sstitham@brannlaw.com](mailto:sstitham@brannlaw.com)



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.

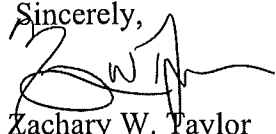
Further, this limitation fails to contemplate when one item of data may be provided from multiple sources. Consider a consumer's address derived from a public record included in a consumer report. CDIA members would have challenges understanding whether, when combined with other information, if it is 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,

A handwritten signature in black ink, appearing to read "Zachary W. Taylor", with a stylized flourish at the end.

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

**Testimony of the Maine Immigrants' Rights Coalition (MIRC)  
In Support of LD 1822**

An Act to Enact the Maine Online Data Privacy Act  
Public Hearing: May 5, 2025, 10:00 AM

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

My name is Ruben Torres and I serve as the Advocacy, Communications, and Policy Manager for the Maine Immigrants' Rights Coalition (MIRC). MIRC represents more than 100 organizations across Maine, including grassroots immigrant-led organizations, legal service providers, housing advocates, and direct service agencies, working collectively to improve the economic and social standing of Maine's immigrant communities, thereby uplifting the state as a whole. We are testifying in strong **support** of LD 1822, An Act to Enact the Maine Online Data Privacy Act.

This bill would establish essential rights for Mainers in the digital age, granting consumers the ability to access, correct, and control how their personal data is collected, processed, and shared. It holds companies to higher standards for transparency, data minimization, and consent, and crucially, it bans the sale of sensitive personal data outright. This means explicit protections for sensitive data, such as: racial or ethnic origin, religious beliefs, consumer health data, sex life, sexual orientation, citizenship or immigration status, genetic data or biometric data, personal data of a consumer the controller knows to be a child, and precise geolocation data.

In today's data economy, every digital interaction, whether it's going to the grocery store, paying a utility bill, or simply using a smartphone, can generate data that is commodified, shared, and weaponized. Our community members interact with public agencies, employers, landlords, health providers, and social media platforms every day. Often without knowing that behind those interactions, their personal data is being mined, resold, and used to track them. In a world where data is currency, non-citizens have become an especially lucrative target.

When personal data is harvested and repackaged for commercial or law enforcement purposes, it creates a climate of fear in all communities. It restricts people from accessing essential services, reporting abuse, or participating in civic life. We know from firsthand accounts in Maine that immigrants avoid accessing health care, education, and even emergency assistance because they fear where their information will end up.

If you wouldn't feel comfortable telling a stranger about personal private information, we must ask: why should corporations be allowed to profit from that same information. LD 1822 builds civil rights protections for all of Maine in the digital era. For these reasons we ask the committee vote **Ought to Pass** on LD 1822. Thank you for your time and thoughtful consideration.

Respectfully,

Ruben Torres  
Advocacy, Communications, and Policy Manager  
**Maine Immigrants' Rights Coalition (MIRC)**  
[rtorres@maineimmigrantrights.org](mailto:rtorres@maineimmigrantrights.org)



**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.<sup>1</sup> 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.

---

<sup>1</sup> <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.