AMERICAN CIVIL LIBERTIES UNION
Maine

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

December 18, 2023

RE: Request for information in connection with LDs 1973 and 1977

Dear Members of the Joint Standing Committee on Judiciary:

My name is Meagan Sway, and I am the Policy Director of the ACLU of Maine. I submit the following comments on behalf the ACLU of Maine in response to requests for information as the committee considers a comprehensive privacy bill that will best protect the people of Maine and be operable for Maine's many businesses and other organizations.

Question: **What "data minimization" do you recommend that the Legislature adopt in consumer data privacy legislation?**

Answer: **The data minimization framework contained in LD 1977 best protects Mainers' privacy.**

Data Minimization Shifts the Work of Protecting Privacy from Consumers to Companies

Data minimization is the basic idea that companies that use and profit from our data may collect, use, and share our data only for the purposes that we would expect based on the goods or services we have requested. This means the mobile game on your phone isn't surreptitiously collecting your location in the background to sell to data brokers; the game will only collect what it reasonably needs, which should be very little. Similarly, your weather app may need your location to provide the local forecast, but it can only be collected for that purpose – you wouldn't expect your weather app to *also* sell your location to data brokers, and data minimization rules would keep them from doing so.

Data minimization means you no longer need to sift through thousands of pages of opaque, legalese in privacy policies to understand how your data is being used. Data minimization rules shift the work of protecting privacy from consumers to the companies themselves. They collect and profit from our data; they should bear the chief responsibility in protecting it. That is why data minimization should be at the heart of any real privacy protections, like those in LD 1977.

Consumer Expectations – Not Opaque Disclosures – Should Be the Appropriate Measure of Data Minimization

The details matter here. LD 1977 appropriately limits the collection and use of our data to "what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the individual." This language does not rely on privacy policies or other disclosures to consumers. In contrast, statutory language in Connecticut and other states limits the "collection of personal data" (*but not uses or sharing!*) to purposes "disclosed to the consumer." This language simply means if you "disclose" the collection of data, even in an impenetrable privacy policy, it will be permissible under the law. These are not meaningful protections, but business as usual.

"Reasonably Necessary" and "Strictly Necessary" Appropriately Tailor the Rigor of Data Minimization to the Potential Harm

Data and information underly everything we do – how our small businesses operate, how we communicate with loved ones, and how we debate matters of public significance. Consequently, it's important that legislation tailor requirements to the risks posed by data and avoid cutting off commerce, communication, and public deliberation.

For the vast majority of use cases, the language of LD 1977 provides a flexible standard for data minimization: the data must be "reasonably necessary and proportionate" for the uses requested by the consumer. One data protection authority has suggested that this standard includes collection or use that is "simply helpful or convenient" to provide the requested good or service.[1]

Some use cases, however, pose higher risks and require more rigorous protections. Data such as Social Security numbers, biometrics like fingerprints or facial scans, genetic data, and the content of communications are closely tied with our individual identities, may be used to perpetuate fraud, or have long been awarded heightened privacy protections. Consequently, that data should be handled with the utmost care, and LD 1977 requires that its collection, use, and disclosure be limited to what is "strictly necessary." This means that the collection, use, and sharing of that data must be *essential* to provide the product or service – it could not be accomplished without it.

Data Minimization and Advertising

Data minimization, when properly constructed, permits businesses to advertise and reach customers, but with robust privacy protections, including adherence to data minimization requirements. LD 1977, like other robust privacy bills, does so by distinguishing among (1) first-party non-targeted advertising, (2) targeted

---

[1] Mark Young, *ICO Updates Guidance on Cookies and Similar Technology*, Covington & Burling LLP, July 4, 2019, available at https://www.insideprivacy.com/data-privacy/ico-updates-guidance-on-cookies-and-similar-technologies/.

advertising, and (3) cross-contextual behavioral advertising based on our profiles over time:

- "First party non-targeted advertising" refers to a company sending an advertisement directly to a consumer through mail, email, or text, based on data collected during the course of its relationship with the consumer. First-party non-targeted advertising is a permissible purpose under LD 1977. Such advertising is permitted so long as the data was originally collected pursuant to the data minimization rule – meaning that, when originally collected, the data was reasonably necessary to provide the good or service the consumer requested. Thus, a company would still be able to send emails or catalogs to a consumer based on information it collected to provide the consumer with goods or services.
- "Targeted advertising" refers to online advertising that is presented to an individual based on their predicted or known preferences. As with first-party non-targeted advertising, the data used must have been collected in compliance with the data minimization rule. In addition, before targeting an ad, companies must give individuals the opportunity to "opt-out" – that is, the chance to decline to be targeted. Thus, if consumer regularly buys slippers from LL Bean, LL Bean may use the related data to send them a personalized email suggesting they buy more slippers if it provides the consumer with a chance to opt-out. Similarly, LL Bean may work with a service provider to show online advertisements to a consumer based solely on LL Bean's first-party data, a practice sometimes known as "retargeting."[2]
- "Cross-contextual behavioral advertising" refers to advertising based on "an individual's online activities over time and across third party websites or online services." A consumer's online activity can be used to create a profile of their interests and to place them in groups called "audience segments" based on interests, behaviors, and demographics they share with others. For example, a recent FTC report found audience segments based on our data can include "viewership-gay," "pro-choice," "African American," "Assimilation or Origin Score," "Jewish," "Asian Achievers," "Gospel and Grits," "Hispanic Harmony," "working class," "unlikely voter," "last income decile," "tough times," "investor high-value," "seeking medical care," and "Political Views – Democrat and Republican."[3] Cross-contextual behavioral advertising is built on creating profiles of us over time and across apps and websites; it is tantamount to surveillance, giving advertisers insight into the most private parts of our lives. For that reason, LD 1977 takes a simply approach to this practice: it ends it.

---

[2] Evan Kaeding, *The end of third-party cookies and what it means for retargeting*, Supermetrics, Oct. 17, 2022, available at https://supermetrics.com/blog/retargeting-end-third-party-cookies#reta.

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

This tailoring of requirements is proportional to the harms posed by these types of advertising. Where we have already entrusted a company with our information, it may use that information to continue the relationship. Where the company seeks to predict our preferences, it must give us a chance to opt out first. And when the company seeks to track us across the internet and to profile us, the practice would be prohibited.

Question: **Whether the Legislature should exempt from new state consumer data privacy legislation either the data or the entities (or both) regulated by other federal laws, for example the data or entities regulated under HIPAA or the Gramm-Leach Bliley Act.**

Answer: **Exclusions for existing law should focus on data, not entities.**

Understandably, emerging state privacy laws seek to accommodate existing laws that already regulate the way that certain kinds of data are handled by certain kinds of entities. For example, the Health Insurance Portability and Accountability Act (HIPAA) regulates the way that certain healthcare providers handle individually identifiable health information; similarly, the Communications Act determines how telephone companies may handle their customers' telephone records. Those laws, however, do not cover every dimension of those entities' practices. HIPAA does not govern how hospitals handle employee information, and the Communications Act may not reach telephone companies' services outside of the provision of telephone services. Providing exemptions form state privacy legislation at the entity-level would mean that the many types of data these companies handle would be entirely exempt because one type of data happens to fall under the purview of a federal privacy law.

The fact that specific, existing federal privacy laws only apply to specific types of data is even more salient in light of increased corporate expansion and corporate consolidation. For example, Amazon recently launched Amazon Clinic to provide telehealth services. As a healthcare provider that engages in electronic transactions, Amazon Clinic is covered by HIPAA.[4] Particularly critical is that LD 1977 would provide protections for employee data; exempting Amazon – or other companies – from adhering to those protections simply because one line of business is covered by existing law would largely undermine the chief purpose of the law: *comprehensive* privacy protections.

[4] *See* Amazon Clinic, *Privacy questions, terms of use, and consents*, https://clinic.amazon.com/privacy (last accessed December 18, 2023).

Question: **Whether the Legislature should exempt small businesses from new state consumer data privacy legislation and, if so, how the legislation should define a "small business"? Should the measure be whether a business has a certain amount of annual gross revenue? Or whether the business collects or processes the personal data of a certain number of Maine consumers per year? What dollar amount of gross revenue or number of Maine consumers would you propose?**

Answer: **Entities of all sizes should generally be subject to the provisions of the law, but the committee can tailor provisions of the bill based on the risk of harm that an entity's data practices present.**

Courts have long recognized that the government has an important interest in protecting privacy. That interest is especially true when the entities we entrust with our information use it in ways that violate our expectations, if it is shared outside the bounds of our relationships with those entities, or when that information is collected by intruding into places we would reasonably expect to be private.

That important interest applies no matter the size of the entity – we expect the same respect for our privacy from our local family medicine practitioner as we would from a national hospital chain. We expect the same respect from local businesses as we do from national box stores. Given that commercial surveillance pulls data from all corners of the data ecosystem, large and small, privacy legislation should begin with the assumption that all entities have a role in protecting our privacy. This means that the core privacy protections like data minimization, data rights, and nondiscrimination protections should apply to all entities.

With that baseline assumption in mind, provisions may be tailored to adjust for the harms posed by data collection and use. These adjustments should *not* be based exclusively on an entity's size or revenue, but on the harms posed by their data collection and use. As described above, one of the riskiest uses of data is building profiles across millions of individuals or brokering data to enable that profiling. LD 1977 recognizes those risks and correspondingly adjusts various requirements across three classes of entities:

- Small businesses are those that operate below a specific threshold for annual gross revenue *and*, crucially, do not collect or process the more than 200,000 individuals. Appropriately, given the harm they may pose, data brokers are excluded from being a "small business." Because of the small amounts of data they process, LD 1977 exempts small businesses from provisions that would establish data governance controls, which are arguably better suited for larger data processors.

- In contrast, data brokers are entities whose principal source of revenue is derived from processing data the entity did not collect directly from the individuals. Because data brokers facilitate the harms of profiling, but are incredibly numerous, LD 1977 largely imposes on them additional disclosure and registration requirements, to make it easier for Mainers to exercise the data rights LD 1977 establishes.
- Finally, large data holders are those that meet several prongs regarding the scope of their data processing. Because of the scope of their processing, LD 1977 imposes additional requirements on large data holders regarding understandable, digestible privacy policies, additional record keeping requirements, and shorter response times for responding to an individual's exercise of data rights.

The particular thresholds and corresponding responsibilities (or exceptions) envisioned by LD 1977 may be adjusted, as the numbers in the bill appear large as compared to Maine's population. What we like about LD 1977's various categories, regardless of the size that the committee ultimately lands on, is that they reflect two critical principles: first, the most fundamental obligations are imposed on all entities, without exception, and second, the tailoring of requirements is based on the scope of the entities' data processing, and not on size or revenue alone.

Thank you for the opportunity to weigh in on these questions.

The Honorable Anne Carney
The Honorable Matt Moonen
Committee on the Judiciary
Maine State House, Room 438
Augusta, ME 04333

December 15, 2023

Dear Chair Carney & Chair Moonen,

BSA | The Software Alliance[1] supports strong privacy protections for consumers. BSA appreciates the Joint Judiciary Committee's interest in protecting consumer data privacy in Maine. In BSA's federal and state advocacy, we work to advance legislation that ensures consumers' rights — and the obligations imposed on businesses — function in a world where different types of companies play different roles in handling consumers' personal data. At the state level we have supported strong privacy laws across the country, including consumer privacy laws enacted in Colorado, Connecticut, and Virginia.

BSA is the leading advocate for the global software industry. Our members are enterprise software and technology companies that create the business-to-business products and services to help their customers innovate and grow. For example, BSA members provide tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations.

As you consider advancing a comprehensive consumer data privacy bill through your committee, BSA urges the Committee to prioritize creating privacy protections that are interoperable with other state laws.

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

I. Creating Privacy Protections That Are Interoperable

Privacy laws around the world need to be consistent enough that they are interoperable, so that consumers understand how their rights change across jurisdictions and businesses can readily map obligations imposed by a new law against their existing obligations.

Thirteen states have enacted comprehensive consumer privacy laws that create new rights for consumers, impose obligations on businesses that handle consumers' personal data, and create new mechanisms to enforce those laws.[2] Twelve of those state privacy laws share a common structural framework for protecting consumer privacy, even though they create different levels of substantive privacy protections for consumers. BSA has created a resource that highlights the similar structures of these state privacy laws and compares their substantive protections. We are attaching a copy of that document, for your reference.

We urge the Committee to adopt privacy protections for Maine that are interoperable with the structure of these existing state privacy laws. Doing so can drive strong business compliance practices that better protect consumer privacy.

We also want to highlight two substantive areas in which interoperability is particularly important:

- *Enforcement*. BSA supports strong and exclusive regulatory enforcement by the Attorney General's office, which promotes a consistent and clear approach to enforcement. State attorneys general have a track record of enforcing privacy-related laws in a manner that creates effective enforcement mechanisms while providing consistent expectations for consumers and clear obligations for companies. All state privacy laws provide state attorneys general with enforcement authority,[3] and we urge the Committee to adopt a similar approach.

- *Focus on consumers, not employees*. To the extent that legislation is designed to protect consumer privacy, we recommend focusing legislation on consumers without sweeping in employment-related data. We encourage you to adopt the approach taken in 12 state privacy laws,[4] which focus on protecting consumer privacy and therefore exclude individuals acting in a commercial or employment context in their definition of "consumer," in addition to excluding data processed or maintained in employment contexts from the scope of their application. This approach can help to ensure that privacy legislation focuses on providing strong privacy protections for individual consumers.

[2] BSA | The Software Alliance, 2023 Models of State Privacy Legislation, *available at* https://www.bsa.org/policy-filings/us-2023-models-of-state-privacy-legislation.

[3] *Id*.

[4] *Id*.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

II. Distinguishing Between Controllers and Processors Benefits Consumers.

Leading global and state privacy laws display a fundamental distinction between processors, which handle personal data on behalf of another company, and controllers, which decide when and why to collect a consumer's personal data. All thirteen states to enact a comprehensive consumer privacy law have incorporated this critical distinction. In California, the state's privacy law for several years has distinguished between these different roles, which it terms businesses and service providers, while all other state comprehensive privacy laws use the terms controllers and processors.[5] This longstanding distinction is also built into privacy and data protection laws worldwide and is foundational to leading international privacy standards and voluntary frameworks that promote cross-border data transfers.[6] BSA urges the Committee to include this distinction in consumer privacy legislation.

We believe that there are two key areas where using intentional language in legislation would significantly reduce the risk of inadvertently undermining consumers' privacy and security and create clear obligations for companies to implement.

- *Definitions*. At the outset, it is critical for any privacy law to define the different types of companies that handle consumers' personal data. Specifically, legislation should distinguish between two roles: (1) companies that decide how personal data is collected, used, shared, and stored – called "controllers" or "businesses" and (2) companies that handle personal data on behalf of those other companies – called "processors" or "service providers." Every state consumer privacy law adopts this critical distinction. Any privacy law must define both roles, so that it can impose strong – but distinct – obligations on both types of companies.

- *Role-Dependent Obligations*. Legislation should impose strong obligations on all companies to safeguard consumer's personal data – and those obligations must reflect the company's role in handling that data. For example, because controllers under all 13 comprehensive state privacy laws decide why and how to collect a consumer's personal data, those companies are obligated to provide consumers

[5] *See, e.g.*, Cal. Civil Code 1798.140(d, ag); Colorado CPA Sec. 6-1-1303(7, 19); Connecticut DPA Sec. 1(8, 21); Delaware Personal Data Privacy Act, Sec. 12D-102(9, 24); Florida Digital Bill of Rights Sec. 501.702((9)(a)(4), (24)); Indiana Senate Enrolled Act No. 5 (Chapter 2, Sec. 9, 22); Iowa Senate File 262 (715D.1(8, 21)); Montana Consumer Data Privacy Act Sec. 2(8,18); Oregon CPA Sec. 1(8, 15); Tennessee Information Protection Act 47-18-3201(8, 20); Texas Data Privacy and Security Act Sec. 541.001(8, 23); Utah CPA Sec. 13-61-101(12, 26); Virginia CDPA Sec. 59.1-575.

[6] For example, privacy laws in Hong Kong, Malaysia, and Argentina distinguish between "data users" that control the collection or use of data and companies that only process data on behalf of others. In Mexico, the Philippines, and Switzerland, privacy laws adopt the "controller" and "processor" terminology. Likewise, the APEC Cross Border Privacy Rules, which the US Department of Commerce has strongly supported and promoted, apply only to controllers and are complemented by the APEC Privacy Recognition for Processors, which helps companies that process data demonstrate adherence to privacy obligations and helps controllers identify qualified and accountable processors. In addition, the International Standards Organization in 2019 published its first data protection standard, ISO 27701, which recognizes the distinct roles of controllers and processors in handling personal data. For additional information on the longstanding distinction between controllers and processors – sometimes called businesses and service providers – BSA has published a summary available here.

with certain rights, such as the ability to access, correct, and delete information, and they have the obligation to seek a consumer's consent when required. If those obligations were instead placed on service providers, it would create security risks since consumers and service providers do not generally interact with each other – so consumers may be confused by a consent request sent by a service provider; service providers, in turn, may not know whether to honor consumer rights requests from individuals they don't know. All comprehensive state privacy laws therefore appropriately place consumer-facing obligations such as consent requirements and consumer rights obligations on businesses and controllers. All 13 comprehensive state privacy laws also create a series of obligations tailored to processors, to ensure those companies handle consumers' personal data responsibly. This approach ensures that service providers are subject to strong obligations in handling consumers' personal information and helps build consumers' trust that their personal information remains protected when it is held by service providers. We are including an appendix to this letter setting out the Virginia CDPA's service provider obligations, for your reference.

Thank you for your leadership in establishing strong consumer privacy protections, and for your consideration of our views. We welcome an opportunity to further engage with you or a member of your staff on these important issues.

Sincerely,

Matthew Lenz
Senior Director and Head of State Advocacy

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Virginia's Consumer Data Protection Act
§59.1-579. Responsibility according to role; controller and processor.

A. A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this chapter. Such assistance shall include:

1. Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to § 59.1-577.

2. Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor pursuant to § 18.2-186.6 in order to meet the controller's obligations.

3. Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to § 59.1-580.

B. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth 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. The contract shall also include requirements that the processor shall:

1. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

2. 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;

3. 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;

4. Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, 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 chapter 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; and

5. Engage any subcontractor pursuant to a written contract in accordance with subsection C that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

C. Nothing in this section shall be construed to relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as defined by this chapter.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

D. Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Charter
COMMUNICATIONS

Kate Gore
Director of State Government Affairs

3. What "data minimization" do you recommend that the Legislature adopt in consumer data privacy legislation?

We recommend following California's approach. The CCPA requires that a business' "collection, use, retention and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes."

This data minimization approach – which has been mimicked by nearly every other state to have adopted a state consumer privacy law – strikes an appropriate balance between consumer protection and business use of information. A more strict standard (e.g., collection that is "strictly necessary" or "required" for a specific purposes) handcuffs a business' ability to do routine and ordinary processing activities from fraud prevention to product improvement. Consumers generally see both internal uses as net positive activities. However, "strictly necessary" and "required" language around data minimization would arguably prohibit a business from doing these things because they are not "strictly necessary" for the purpose for which the information was first collected. But a too lenient data minimization standard (e.g., collection compatible with a privacy policy) on the other hand leaves businesses to their own devices where so long as they bury a disclosure in a privacy policy, they can collect large quantities of information.

California's approach therefore strikes a balance of allowing the use of personal information based on the context in which it is collected while requiring businesses to be proportional in their collection of data. This means, for example, that a business cannot collect personal information for one purpose and use it for another, non-disclosed purpose or purpose that would not heave reasonably been expected at the time of collection. Similarly, a business should not, under the CCPA formulation, collect more information that is reasonable for the purpose. At the same time, the CCPA language provides businesses the flexibility for internal use of data that is largely seen as beneficial not only to companies, but to consumers as well.

4. Do you believe that the Legislature should repeal the current ISP privacy law (35-A M.R.S. §9301) as part of a new, comprehensive approach to data privacy? Or, do you think the Legislature should retain the ISP Privacy law?

The legislature should repeal the current ISP privacy law as part of its adoption of a comprehensive privacy law. There is significant value in the comprehensive approach taken by all thirteen states to have adopted general consumer privacy laws. Current law in Maine does not protect Mainers from any entities' data practices except for ISPs. The Maine legislature now has an opportunity to extend privacy safeguards to all Mainers and apply a more fair and equitable compliance burden on all companies of a certain size in Maine, regardless of their line of business.

118 JOHNSON ROAD, PORTLAND ME 04102 **O** (207) 253-2545 Kate.Gore@Charter.com

Charter
COMMUNICATIONS

Kate Gore
Director of State Government Affairs

The parity principle stands for consumers being best served by consistent application of privacy protections across the entire Internet ecosystem. Consumers should be protected equally whether they are using an ISP like Charter, a search engine, an e-commerce site, a streaming service, a social network, or a mobile carrier or device. It is bad for consumers for the same data to be protected when it is held by an ISP, but left entirely unprotected when it passes through the hands of search engines, social networks, advertisers, and others on its way to its intended destination.

This is why every one of the states to have considered and enacted a comprehensive privacy law to date has aligned with the parity principle. These states recognized that data protections are only effective when consumers can be sure that everyone that touches consumer data is subject to the same requirements and oversight.

118 JOHNSON ROAD, PORTLAND ME 04102 **O** (207) 253-2545 Kate.Gore@Charter.com

CollegeBoard

December 18, 2023

The Honorable Anne Carney
Senate Chair
Joint Standing Judiciary Committee
Maine Senate

The Honorable Matt Moonen
House Chair
Joint Standing Judiciary Committee
Maine House of Representatives

Re: LD 1973 and LD 1977

Dear Chairs Carney and Moonen:

College Board writes to support the scope and applicability of LD 1973, which does not apply to 501(c)(3) nonprofit organizations or institutions of higher education. We encourage the Legislature to retain these provisions in its consumer privacy legislation.

Nonprofits often collect data in pursuit of fulfilling their missions and are misfits for governance under these broad-based consumer privacy laws. That's why the overwhelming majority of consumer privacy laws **exempt nonprofits**. Other states, such as Oregon, will delay subjecting nonprofits to its consumer privacy law because they recognize that nonprofits' collection and processing of data is not akin to the uses by for-profit entities.

About College Board

College Board is a mission-driven not-for-profit organization that connects students to college success and opportunity. Each year, College Board helps more than seven million students prepare for a successful transition to college through programs and services in college readiness and college success—including the SAT, the Advanced Placement Program, and BigFuture.

College Board must collect minors' data to connect students to colleges and scholarship opportunities. We provide transparent notice about our use of any information we collect. We don't share information without the individual's permission. In serving students, College Board engages with students during school, at home, and at weekend test centers.

College Board already complies with numerous privacy laws, such as FERPA and other state student data privacy laws, as applicable. We are committed to respecting privacy and protecting individuals' data. Our data privacy principles are focused on providing notice, choice, transparency, and security to students, parents, and educators.

Potential Impacts of LD 1973 or LD 1977

Limitations on sensitive data could impact College Board's ability to fulfill its mission to connect students to opportunities. Other nonprofits may face similar circumstances.

College Board sometimes collects sensitive information to provide additional resources and supports for certain students, such as:

- Health information to approve testing accommodations for students with disabilities under the Americans with Disabilities Act.

- Race/ethnicity information to connect students to scholarships and recognition programs for underrepresented minorities, accurately report performance across subgroups of students, and quality control assessment questions to prevent bias against any group of students.

If LD 1973 or 1977 were to apply to nonprofits, Maine students' data would fall under different rules depending on where a student was located when they provided the data. This compliance patchwork based on where data was collected could be unworkable in practice and cause problems for Maine students.

Thank you and we look forward to working together to support Maine students on their path to postsecondary success.

Sincerely,

Alexandra Dominguez
Senior Director, Government Relations

December 18, 2023

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

Re: *Invitation to Comment on Specific Privacy Bill Provisions*

Dear Chair Carney and Chair Moonen,

Consumer Reports[1] thanks the Committee for their continued work to create strong privacy protections for Maine consumers. Below, we respond to the list of questions posed by the Committee as it gathers additional information from stakeholders regarding key legislative provisions under consideration.

- The Committee asks: "*Whether the Legislature should exempt from new state consumer data privacy legislation either the data or the entities (or both) regulated by other federal laws, for example the data or entities regulated under HIPAA or the Gramm-Leach Bliley Act.*"

  Consumer Reports believes that entities that collect data covered by existing sectoral federal privacy laws, like HIPAA or GLBA, should, at a maximum, receive exemptions **only for the information already protected by those laws**. Providing an entity-level exemption opens an unacceptably large loophole in the legislation that could allow businesses that conduct a variety of far-flung data collection and processing activities to

[1] 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.

exempt themselves entirely from the law so long as one part of their business collects HIPAA or GLBA covered data.

This concern is not hypothetical. In today's digital economy, health information and financial information no longer strictly reside under the provenance of hospitals and banks. In fact, Big Tech companies (Apple, Amazon, Google, Facebook, and Microsoft) *routinely* partner with hospitals and banks to serve as service providers, affiliates, or "business associates", as they help those entities collect, share, store, and analyze health and financial records covered by HIPAA or GLBA.[2] At the same time, Big Tech companies are increasingly purchasing startups in the health and financial space that already have access to the type of regulated data they crave,[3] and are steadily reaching their tentacles closer in the direction of providing traditional healthcare or financial products, such as credit products,[4] insurance,[5] digital currency,[6] and digital wallets.[7]

Large tech companies should not be exempted from the entire bill if one arm of their business receives consumers' financial information from banks or crosses the threshold into providing traditional healthcare services. It is dubious whether these entities should be receiving any exemptions at all — HIPAA and GLBA were passed years ago and lack many of the protections being considered by the committee.[8] But at the very least, we should not provide Big Tech a get-out-of-jail-free card through gaping entity-level exemptions.

---

[2] See, e.g., Rob Copeland, "Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans", Wall Street Journal, November 11, 2019, https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790

[3] See, e.g., Steve Alder, "Amazon Completes Acquisition of OneMedical Amid Concern About Uses of Patient Data", HIPAA Journal, March 3, 2023, https://www.hipaajournal.com/amazon-completes-acquisition-of-onemedical-amid-concern-about-uses-of-patient-data/

[4] See, e.g., Apple "Introducing Apple Card, a new kind of credit card created by Apple", March 25, 2019, https://www.apple.com/newsroom/2019/03/introducing-apple-card-a-new-kind-of-credit-card-created-by-apple/

[5] See, e.g., Heather Landi, Fierce Healthcare, "Here's how Google, Amazon, Facebook and Apple are targeting the health insurance market", October 7, 2020, https://www.fiercehealthcare.com/tech/here-s-how-google-amazon-facebook-and-apple-are-making-a-play-for-health-insurance-market

[6] See, e.g., Ryan Browne, CNBC, "Here's why regulators are so worried about Facebook's digital currency", September 19, 2019, https://www.cnbc.com/2019/09/19/heres-why-regulators-are-so-worried-about-facebooks-digital-currency.html

[7] See, e.g., John Mello, Tech News World, "Big Banks and Big Tech Set To Square Off Over Digital Wallets", January 24, 2023, https://www.technewsworld.com/story/big-banks-and-big-tech-set-to-square-off-over-digital-wallets-177326.html

[8] See, e.g., Robert Gellman, IAPP, "Protect consumer privacy: Repeal GLBA's privacy provisions", July 30, 2023 https://iapp.org/news/a/protect-consumer-privacy-repeal-the-glbas-privacy-provisions/

At the same time, the Committee should be aware that hospitals and financial institutions collect a plethora of information that is not covered by existing privacy laws and thus would be left completely unprotected if those entities were to receive a broad exemption. For example, hospitals, like the Mayo Clinic, collect extremely sensitive health related information from consumers that browse their websites and look up information about their treatment or health conditions.[9] Similarly, individuals not otherwise associated with a bank may use the bank's online tools, such as a mortgage calculator, which also reveals extremely sensitive information. This type of information is not typically protected by HIPAA or GLBA and is routinely shared with third-parties, including social media websites, and has a high capacity to harm individuals if it lands in the wrong hands.[10] It should be protected by a new privacy law.

- The Committee asks: "*Whether the Legislature should exempt small businesses from new state consumer data privacy legislation and, if so, how the legislation should define a "small business"? Should the measure be whether a business has a certain amount of annual gross revenue? Or whether the business collects or processes the personal data of a certain number of Maine consumers per year? What dollar amount of gross revenue or number of Maine consumers would you propose?*"

  In general, Consumer Reports believes that privacy legislation should include coverage thresholds pegged to the amount of personal data a company processes. Company size or number of employees is often a poor proxy for an entity's capacity to collect and process large amounts of consumer data, and, by extension, create significant privacy risks.

  For example, Cambridge Analytica, which illegally harvested the personal information of 87 million people, only employed 107 people at the time of the scandal in 2018 and made around $25 million in revenue the previous year.[11] Clearview AI reportedly has less than 50 employees and makes less than $5 million in annual revenue and yet has amassed a facial recognition database that includes more than 40 billion images.[12]

---

[9] Andrew Paul, Popular Science, "Almost 99 percent of hospital websites give patient data to advertisers", April 10, 2023, https://www.popsci.com/technology/hospitals-data-privacy/
[10] Id.
[11] Peg Brickley, "Cambridge Analytica Revenue Fell as Questions About Data Tactics Surfaced," Wall Street Journal, June 1, 2018, https://www.wsj.com/articles/cambridge-analytica-revenue-fell-as-questions-about-data-tactics-surfaced-1527883000 ; Pitch Book, Cambridge Analytica Overview, (May 2018), https://pitchbook.com/profiles/company/226886-68
[12] Chris Burt, Biometric Update, Clearview AI tops 40 billion reference images in facial recognition database, November 24, 2023, https://www.biometricupdate.com/202311/clearview-ai-tops-40-billion-reference-images-in-facial-recognition-database

Data thresholds should be low enough to ensure that entities that process a significant proportion of the state's residents' personal information are covered. For example, at a 100,000 person per year threshold, a business would have to collect roughly one out of every ten Maine residents' records each year to be covered. This would likely limit coverage to only the state's very largest businesses. We've previously advocated for states with similar populations, like New Hampshire and Delaware, to set their coverage threshold at 35,000 records per year.

- The Committee asks: "*What "data minimization" do you recommend that the Legislature adopt in consumer data privacy legislation?"*

  Consumer Reports supports strong data minimization provisions, like those that are currently included in LD 1977. Section 9604 (1) prohibits businesses from collecting or processing covered information unless "reasonably necessary and proportionate to provide or maintain a specific product or service requested by the individual to whom the data pertains." In today's digital economy, consumers are often faced with an all-or-nothing proposition: they may either "choose" to consent to a company's data processing activities, or fogo the service altogether if if they do not approve of any one of a company's practices (which often allow the business to track and sell the consumer's information to nebulous third-parties or build future artificial intelligence products using their information).

  L.D. 1977 would turn this arrangement on its head by ensuring consumers' privacy by default and prevent individuals from having to take any action – either to opt-in or opt-out – in order to protect themselves. We know that measures based on a consent model (opt-in or opt-out) are destined to fail because they require consumers to contact hundreds, if not thousands, of different companies in order to fully protect their privacy. These consent processes are often so onerous that they have the effect of preventing consumers from stopping the sale of their information.[13] L.D. 1977 instead puts the burden of privacy protection on those that otherwise have every incentive to exploit consumer data for their own benefit.

  By contrast, L.D. 1973 adopts a version of data minimization that is "minimization" in name only. Under that provision, data collection is limited to any purpose listed by a company in its privacy policy — instead of what is reasonably necessary to fulfill a transaction. This means that a company can simply rely on their expansive or vague privacy policy that lets them collect data for virtually any purpose and still satisfy the

[13] Maureen Mahoney, Many Companies Are Not Taking the California Consumer Privacy Act Seriously,, Medium (January 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb.

data minimization provision. Such a framework is only likely to confuse consumers into believing they have more protections than they do.

******

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

Sincerely,

Matt Schwartz
Policy Analyst

December 18, 2023

Maine Committee on Judiciary
State House, Room 438
100 State House Station
Augusta, ME 04333

RE: Request for Comment – Maine Privacy Bills

Dear Chair Carney, Chair Moonen, and Members of the Committee,

Thank you to the committee for the opportunity to comment on the proposed Maine privacy bills that are before it. CTIA is the trade association for the wireless communications industry representing wireless providers operating in Maine, including AT&T, DISH, T-Mobile, UScellular, and Verizon.

The Maine legislature is considering a privacy law that would generally apply to all industries. This is the right approach and is the one taken in other states that have enacted comprehensive privacy legislation. We urge the Maine legislature to provide consumers with consistent protections and therefore, any privacy law enacted should be interoperable with the laws that have already passed in other states. By way of example, the general approach in other states in providing consumers with choices as it relates to the use of their non-sensitive data for certain types of processing is an opt-out approach. The Maine legislature should take a similar approach to allow for a consistent framework.

At the same time, we further urge the legislature to repeal the Maine broadband internet access service (BIAS) provider privacy law (PL 2019, c. 216, §1 and affected by §2). Such repeal is included in LD 1973. It would be prudent for the legislature to have one approach that applies to all members of the Internet ecosystem – like the approach in other states. There is no basis for unique requirements to apply to only one industry segment. Other parts of the internet ecosystem often have access to the same types of data, and the same volume. The result of both a comprehensive privacy law that applies generally, and another law that only

applies to BIAS providers will raise inconsistencies as to the treatment of data, leaving consumers with a lack of understanding as to how their data is being regulated.

Sincerely,

Jake Lestock
Director
State Legislative Affairs

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

December 18, 2023

The Honorable Anne Carney, Senate Chair
The Honorable Matt Moonen, House Chair
Maine State Legislature
Judiciary Committee
230 State Street
Augusta, Maine 04330

Dear Chair Carney, Chair Moonen, and Members of the Committee:

EPIC writes in response to the Committee's request for information on data minimization. Below, we outline how online tracking works, define what data minimization is, explain why current state laws are insufficient to protect consumers, and outline existing data minimization rules in other jurisdictions.

The Electronic Privacy Information Center (EPIC) is an independent nonprofit research organization in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.[1] EPIC has long advocated for comprehensive privacy laws at both the state and federal level.[2]

We face a data privacy crisis in the United States. Unrestricted data collection has eroded consumer privacy. Consumers are surveilled through constant monitoring, profiling, and targeting online. For two decades, online firms have been allowed to collect and commodify every bit of consumer data, depriving consumers of control over their personal information, heightening security risks, and leading to data misuse, the loss of autonomy, manipulation, and discrimination.

How does online tracking work?

Consumers are constantly tracked: every website we visit, app we open, article we read, ad we linger over, even what our friends are reading and where they are going is collected and connected to other data about us all to target us with more ads. The schemes used to track our digital

[1] EPIC, *About EPIC*, https://epic.org/about/.
[2] *See e.g.* Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: *Hearing before the Subcomm. on Consumer Protection & Comm. of the H. Comm. on Energy & Comm.*, 117th Cong. (2022) (testimony of Caitriona Fitzgerald, Deputy Director, EPIC), https://epic.org/wp-content/uploads/2022/06/Testimony_Fitzgerald_CPC_2022.06.14.pdf; Caitriona Fitzgerald, *A Proposed Compromise: the State Data Privacy and Protection Act* (Feb. 22, 2023), https://epic.org/a-proposed-compromise-the-state-data-privacy-and-protection-act/.

and physical activities across the web and across devices, are too complex and opaque for the vast majority of internet users to understand or control.

Data collection is the initial stage of commercial surveillance systems. Much of the collection of personal data happens so routinely and automatically in the online ecosystem that customers have little to no knowledge of its scope. Every website we visit or app we open is collecting data about us from the second we connect. Indeed, with the increasing proliferation of "smart" devices in homes, offices, and other locations, the collection of personal data frequently happens even when customers aren't intending to interact with an online service at all. And other activities like credit card purchases[3] and even physical movements[4] can be logged and tracked without the consumer's awareness or control. These countless data points can be combined to reveal sensitive details about consumers and put them at risk of many harms, including discrimination, stalking, harassment, and government scrutiny.[5]

Personal data is generated and collected in several different ways during the course of consumers' routine online and offline activities. First, personal data is generated and collected whenever a user loads content from a website, app, service, or connected device. Some of this data is necessary to request, route, and load content and services, but other data might be collected and stored even if it isn't necessary to complete a consumer's request. Second, data can be created and collected through interactions with and use of a website, app, service, or device. Some of this data is sent or generated by the user themself (e.g., search queries, messages, and profile updates), but other data might be collected based on what the user is doing and how they are interacting with the system (e.g., what they click on, how long they stay on a page, or even where their focus shifts). And third, data is collected and transferred to and from a broad range of sources by entities who have no direct relationship to the consumer (e.g., data brokers, surveillance firms with cameras or embedded sensors, and government agencies).[6]

Next, the data collected about us is linked to other data about us through identifiers used to track, profile, or target consumers across the online ecosystem. Data about what consumers do online can be linked to them automatically if they are browsing a site or using an app or service that already knows them through an established login or known credential (e.g., e-mail address, phone number, or username), but there are many other ways that data can be linked even by

---

[3] Jay Stanley, *Why Don't We Have More Privacy When We Use A Credit Card?*, ACLU (Aug. 13, 2019), https://www.aclu.org/news/privacy-technology/why-dont-we-have-more-privacy-when-we-use-credit-card.
[4] Michael Kwet, *In Stores, Secret Surveillance Tracks Your Every Move*, N.Y. Times (June 14, 2019), https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.
[5] Manuela López Restrepo, *Does Your Rewards Card Know if You're Pregnant? Privacy Experts Sound the Alarm*, NPR (Aug. 13, 2022), https://www.npr.org/2022/08/13/1115414467/consumer-data-abortion-roe-wade-pregnancy-test-rewards-card-target-walgreens.
[6] FTC, *Data Brokers: A Call for Transparency and Accountability* iv (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [hereinafter FTC Data Broker Report].

unknown third parties. When data is collected about activities of a consumer using a computer or mobile device, any unique identifiers associated with that device might be used to link that data with other data sets or profiles about the consumer.[7] Web browsers use small files called "cookies" to store information about a user's interactions with the sites they visit, and many firms engaged in commercial surveillance have used versions of these files commonly referred to as "third party tracking cookies" to collect information about what sites users are visiting.[8] And even when a user's browser or device is configured to block these tracking cookies or to not broadcast unique identifiers, online entities can use information about the consumer's computer configuration as a sort of "fingerprint" to link their data across apps, sites, and services.[9]

The next stage in the commercial surveillance process is the profiling, targeting, and sale of personal data or personal data analytics services. Consumers' personal data can rapidly move through many different entities and be processed or sold for myriad purposes. The data brokers and analytics companies that transit in this personal data have no relationship with the consumer, and their processing purposes typically have nothing to do with the initial purpose for which the consumers' data was collected. The scale of this profiling by data brokers is staggering. Even eight years ago, the Federal Trade Commission (FTC) found that the data brokers it studied collected and stored data "on almost every U.S. household and commercial transaction," and the FTC found that one of the largest data brokers had "information on 1.4 billion consumer transactions and over 700 billion aggregated data elements."[10]

Some of the companies operating in this space specialize in building or "enriching" consumer profiles, while others merely buy, combine, and sell data sets from many different sources. Many of these services are used by companies engaged in targeted advertising and marketing to identify audiences that fit within specified demographics or to find "look alike" audiences based on existing customer or target lists. The FTC has found that these data brokers "combine and analyze data about consumers to make inferences about them, including potentially sensitive inferences."[11] The largest companies, like Acxiom and Oracle, offer a panoply of targeting and profiling tools. And

---

[7] *See* Rebecca Smith, *What Is IDFA and Why Is This iOS Update Important?*, Mozilla (Apr. 26, 2021), https://blog.mozilla.org/en/internet-culture/mozilla-explains/turn-off-idfa-for-apps-apple-ios-14-5/.
[8] Emily Stewart, *Why Every Website Wants You to Accept Its Cookies*, Vox (Dec. 10, 2019), https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy ("There are first-party cookies that are placed by the site you visit, and then there are third-party cookies, such as those placed by advertisers to see what you're interested in and in turn serve you ads—even when you leave the original site you visited. (This is how ads follow you around the internet.)"); *see Cookies on Mobile 101*, IAB (Nov. 2013), https://www.iab.com/wp-content/uploads/2015/07/CookiesOnMobile101Final.pdf.
[9] Chris Hauk, *What Is Browser Fingerprinting? What It Is and How to Stop It.*, PixelPrivacy (Aug. 16, 2022), https://pixelprivacy.com/resources/browser-fingerprinting/ ("Browser fingerprinting is a powerful method that websites use to collect information about your browser type and version, as well as your operating system, active plugins, time zone, language, screen resolution and various other active settings.").
[10] FTC Data Broker Report, *supra* note 6, at iv.
[11] *Id*.

the advertising platforms themselves, including Facebook and Google, also offer their own audience analytics tools. These companies profit off data harvested from consumer activities and transactions in ways entirely outside the expectations of consumers in their interactions with first-party businesses.

The goal of these and other similar systems is to enable companies to track and target specific users based what they watch, what they read, what they buy, who they know, and where they go. And data brokers are continually expanding their reach deeper and deeper into the private lives of individuals, especially as connected devices, services, and even audio and visual sensors become more prevalent on streets, in stores, in offices, and in homes. For example, The Trade Desk, which runs another large targeted advertising platform, promotes its "Connected TV" advertising platform as being able to "go beyond demographics and leverage first- and third-party data to reach your most valuable audiences on every screen."[12] In this context, the consumer is forced to simply make do with the fact that their every move and reaction is being logged and used to target them with advertisements that will follow them across devices, physical spaces, and contexts.

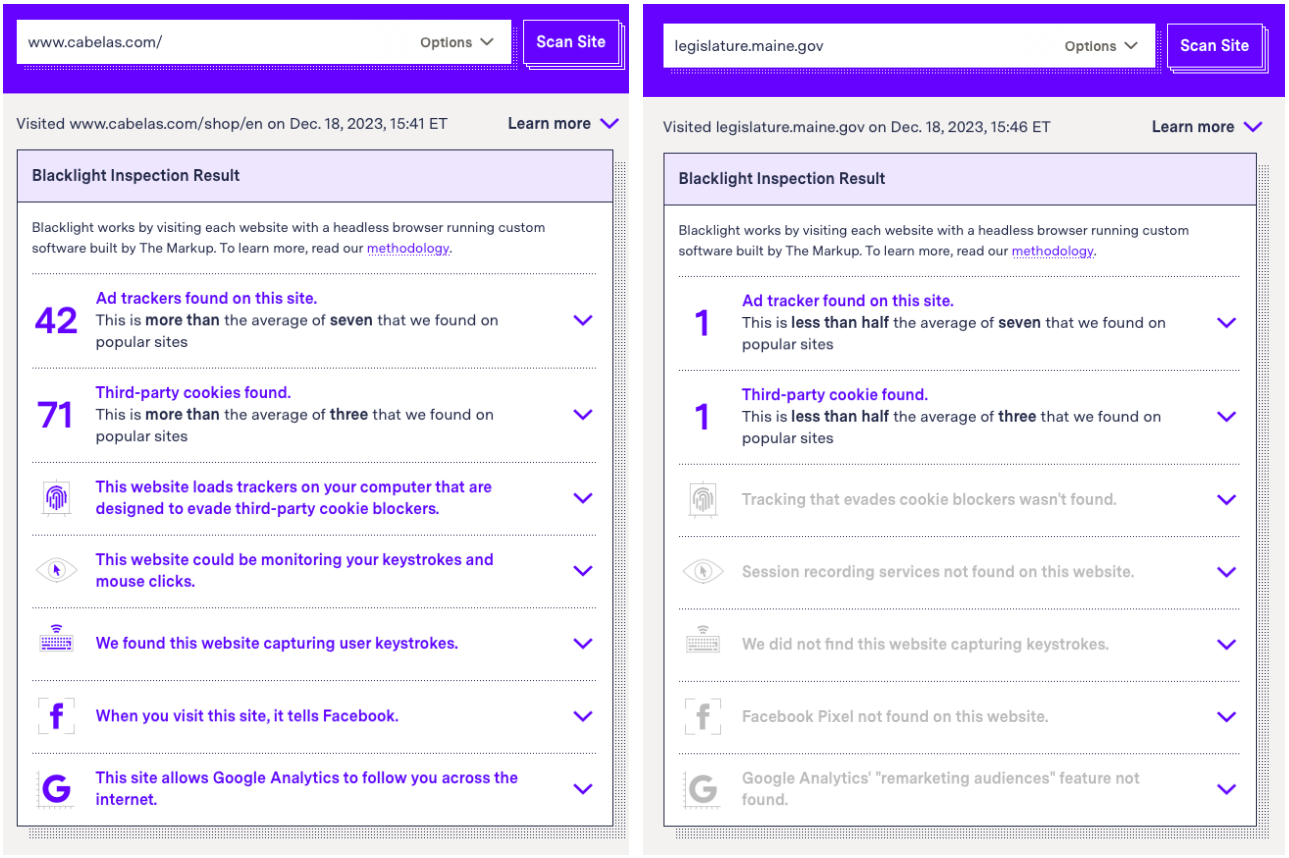
One of the largest systems of commercial surveillance, tracking, and profiling is the online advertising process known as real-time bidding (RTB).[13] This is the "process by which the digital ads we see every day are curated."[14] The IAB has explained how ubiquitous this process is: there is "not a single website publisher, mobile app, or advertising brand today that doesn't participate in real-time systems for buying or delivering personalized ads to consumers."[15] RTB systems rapidly relay information about consumers to facilitate auctions that sell digital ad space in real time. "The hundreds of participants in these auctions receive sensitive information about the potential recipient of the ad—device identifiers and cookies, location data, IP addresses, and unique demographic and biometric information such as age and gender."[16] This "bidstream" data flows to hundreds of entities (including domestic and foreign entities that have no intention of actually serving ads) and are used to "compile exhaustive dossiers about" consumers that "include their web browsing, location, and other data, which are then sold by data brokers to hedge funds, political campaigns, and even to the government without court orders."[17] Companies have used this bidstream data to violate Americans' privacy on a massive scale and have even used it to profile "participants [in] Black Lives Matter

---

[12] *Connected TV*, The Trade Desk, https://www.thetradedesk.com/us/our-platform/dsp-demand-side-platform/connected-tv (last visited Nov. 17, 2022).
[13] Jack Marshall, *WTF Is Real-time Bidding?*, Digiday (Feb. 17, 2014), https://digiday.com/media/what-is-real-time-bidding/.
[14] Letter from Sen. Ron Wyden, et al., to Chairman Joseph Simons, Fed. Trade Comm'n (July 31, 2020), https://www.wyden.senate.gov/imo/media/doc/073120%20Wyden%20Cassidy%20Led%20FTC%20Investigation%20letter.pdf.
[15] Jordan Mitchell, *The Evolution of The Internet, Identity, Privacy And Tracking – How Cookies And Tracking Exploded, And Why We Need New Standards For Consumer Privacy*, IAB Tech Lab (Sept. 4, 2019), https://iabtechlab.com/blog/evolution-of-internet-identity-privacy-tracking/.
[16] *Id*.
[17] *Id.*

protests" and to track "Americans who visited places of worship and then built religious profiles based on that information."[18]

To illustrate the problem, compare the results of the Markup's Blacklight tool[19], which reveals user-tracking technologies on websites, on the Maine Legislature's website versus the homepage for retailer Cabela's:



When a consumer visits cabelas.com, their IP address, device ID, and other information is being sent to dozens of third parties, completely outside of the consumer's view and almost always without their knowledge. Cabela's may not even be fully informed about what's happening with its customer's personal data once it is transferred to ad tech companies and other third parties. Those third parties are profiting off Cabela's customers' personal data, and most visitors to Cabela's website don't even know they exist.

[18] *Id.*
[19] https://themarkup.org/blacklight.

The harms from these privacy violations are real[20] and it is past time to correct the course. And giving Mainers the right to simply opt-out of these systems isn't enough. Mainers should have their privacy protected by default. Data minimization offers a solution.

What is data minimization?

The excessive data collection and processing that fuels commercial surveillance systems is inconsistent with the expectations of consumers, who reasonably believe that the companies they interact with will safeguard their personal information. These exploitative practices don't have to continue. The American Data Privacy and Protection Act (ADPPA) proposed in Congress last session relied on a concept that has long been a pillar of privacy protection: data minimization.

When consumers interact with a business online, they reasonably expect that their data will be collected and used for the limited purpose and duration necessary to provide the goods or services that they requested. For example, a consumer using a map application to obtain directions would not reasonably expect that their precise location data would be disclosed to third parties and combined with other data to profile them. And indeed, providing this service does not require selling, sharing, processing, or strong consumer data for an unrelated secondary purpose. Yet these business practices are widespread. Nearly every online interaction can be tracked and cataloged to build and enhance detailed profiles and retarget consumers.

The ADPPA set a baseline requirement that entities only collect, use, and transfer data that is "*reasonably necessary and proportionate*" to provide or maintain a product or service requested by the individual (or pursuant to certain enumerated purposes).[21] For sensitive data, it must be "*strictly necessary*," and may not be used for targeted advertising. This standard better aligns business practices with what consumers expect.

Data minimization is essential for both consumers and businesses. Data minimization principles provide much needed standards for data security, access, and accountability, assign responsibilities with respect to user data, and restrict data collection and use. Indeed, a data minimization rule can provide clear guidance to businesses when designing and implementing systems for data collection, storage, use, and transfer. And data security will be improved because personal data that is not collected in the first place cannot be at risk of a data breach.

The Federal Trade Commission has recognized that the overcollection and misuse of personal information is a widespread problem that harms millions of consumers every day and has

[20] Danielle Citron & Daniel Solove, *Privacy Harms*, 102 B.U.L. Rev. Online 793 (2021), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.
[21] H.R. 8152 at §101 (2022), *available at* https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

identified that data minimization is the key to addressing these unfair business practices. As it stated in a recent report:

> Data minimization measures should be inherent in any business plan—this makes sense not only from a consumer privacy perspective, but also from a business perspective because it reduces the risk of liability due to potential data exposure. Businesses should collect the data necessary to provide the service the consumer requested, and nothing more.[22]

Data minimization offers a practical solution to a broken internet ecosystem by providing clear limits on how companies can collect and use data. The ADPPA set out a model for data minimization that was subject to intense scrutiny by many parties as it moved through Congress. Maine can now take advantage of that bipartisan consensus language.

How the Connecticut Data Privacy Act fails to protect consumers

Companies should not be allowed to determine for themselves what are the permissible purposes of collecting and using consumers' personal information. Without meaningful limitations, companies can, and do, claim that they need nearly unlimited data collection, transfer, and retention periods in order to operate their businesses. Unfortunately, the limitations on data collection in the Connecticut Data Privacy Act allow companies to do just that. The CTDPA reads:

> A controller shall […] Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer.

This simply requires that businesses only collect what is reasonably necessary for the purposes they disclose to consumers in their privacy policy. This does little to change the status quo, as businesses can list any purpose they choose in their privacy policies, knowing that very few consumers will read them. This is why it is so critical that the Maine Legislature enact stronger data minimization than what was enacted in Connecticut.

Existing data minimization rules in other jurisdictions

Data minimization is not a new concept. Privacy laws dating back to the 1970s have recognized and applied this concept. The Privacy Act of 1974, a landmark privacy law regulating the personal data practices of federal agencies, requires data minimization. Each agency that collects personal data shall "maintain in its records only such information about an individual as is relevant

[22] FTC, *Bringing Dark Patterns to Light* 17–18 (2022), https://www.ftc.gov/reports/bringing-dark-patterns-light.

and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[23]

Indeed, there are already references to only disclosing data as "reasonably necessary" in Maine statute. Title 24-A, Section 2215, the Maine Insurance Code reads:

> A regulated insurance entity or insurance support organization may not disclose any personal information about a consumer collected or received in connection with an insurance transaction unless the disclosure is made with due consideration for the safety and reputation of all persons who may be affected by the disclosure, is limited to the minimum amount of personal information necessary to accomplish a lawful purpose and is disclosed:
>
> […]
>
> To a person other than a regulated insurance entity or insurance support organization, only if that disclosure is **reasonably necessary**:
>
> > (1) To enable that person to perform a business, professional or insurance function for the disclosing regulated insurance entity or insurance support organization and that person agrees not to disclose the information further without the consumer's written authorization unless the further disclosure:
> >
> > (a) Would otherwise be permitted by this section if made by a regulated insurance entity or insurance support organization; or
> >
> > (b) Is **reasonably necessary** for that person to perform its function for the disclosing regulated insurance entity or insurance support organization

The recently passed update to the California Consumer Privacy Act also includes provisions requiring a form of data minimization.[24] California regulations establish restrictions on the collection and use of personal information. The California Privacy Protection Agency explained that this "means businesses must limit the collection, use, and retention of your personal information to only those purposes that: (1) a consumer would reasonably expect, or (2) are compatible with the consumer's expectations and disclosed to the consumer, or (3) purposes that the consumer consented to, as long as consent wasn't obtained through dark patterns. For all of these purposes, the business' collection, use, and retention of the consumer's information must be reasonably necessary and proportionate to serve those purposes."

The EU's General Data Protection Regulation (GDPR) requires companies, among other things, to minimize collection of consumer data to what is "[a]dequate, relevant, and limited to what

[23] 5 U.S.C. § 552a (e)(1).
[24] Cal. Civ. Code § 1798.100(c).

is necessary in relation to the purposes for which they are processed."[25] This is layered on top of restrictions on the legal bases under which companies can process personal data. The GDPR was groundbreaking in establishing broad data protection rights online, but Maine should consider adopting a more concrete set of regulations now that difficulties with interpreting and enforcing GDPR have been revealed. Luckily a significant amount of the compliance work businesses are already doing to comply with GDPR would be applicable to ADPPA-style data minimization rules.

The key with a data minimization provision is to ensure it is tied to the specific product or service requested by the individual, not simply to whatever purpose the collecting entity decides it wants to collect data for and discloses in their privacy policy (as is the case in the Connecticut Data Privacy Act). This better aligns with consumers expectations when they use a website or app.

How would data minimization work?

Data minimization is about appropriate data flows. The biggest impact that this type of rule will have is that the entities that use our personal information in out-of-context ways, such as data brokers, will be unable to profile consumers in ways unrelated to why a consumer used an online service. The rule will limit the harmful practice of brokering, selling, or sharing personal information unrelated to the primary collection purpose and accordingly limit harmful surveillance advertising. Data minimization doesn't prevent companies from sending catalogs to their customers. It doesn't prevent them from using data they've collected about their customer's purchases to recommend products to them or e-mail them with information. Data minimization doesn't prevent advertising.

If the Committee is interested in discussing further how data minimization would work in practice, EPIC would be happy to be a resource for that discussion.

Sincerely,

Caitriona Fitzgerald

Caitriona Fitzgerald
EPIC Deputy Director

[25] Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 § 1(c).

December 15, 2023

Janet A. Stocco, Esq.
Legislative Analyst
Office of Policy and Legal Analysis
Maine State Legislature

Re: Judiciary Committee Request for Comment on Data Privacy Bills

Dear Ms. Stocco:

The Financial Industry Regulatory Authority ("FINRA") appreciates the opportunity to reiterate our earlier feedback on the data privacy bills before the Judiciary Committee, specifically regarding LD 1973 and LD 1977 – bills which would provide data privacy protections for Maine residents and place certain privacy-related obligations on a wide variety of entities. FINRA generally supports increased privacy protections but urges you to exclude regulatory data used by FINRA to oversee the brokerage industry and protect investors in Maine.

FINRA is a National Regulator of the Brokerage Industry

FINRA is a not-for-profit regulator of the securities industry that operates under authority granted to it by the Securities Exchange Act of 1934.[1] FINRA is overseen by the Securities and Exchange Commission ("SEC")[2] and works closely with the SEC and the Maine Office of Securities in executing its regulatory responsibilities. FINRA's mission is to protect investors and safeguard market integrity in a manner that facilitates vibrant capital markets. As part of this mission, FINRA examines brokerage firms, examines for and enforces compliance with FINRA rules and federal securities laws and provides information to the investing public. FINRA also works with state securities regulators nationwide to register broker-dealers and their agents and operates the electronic system through which both FINRA and state registrations flow.

FINRA's regulatory work includes oversight of the more than 600,000 financial advisors employed by the more than 3,000 broker-dealer firms within its jurisdiction. This includes the more than 150,000 persons registered to do business in Maine. FINRA also conducts cross-market oversight of trading on the nation's top exchanges and off-exchange venues for securities and options, administers a specialized arbitration forum with a focus on investor protection and administers licensing qualification examinations.[3] From 2021 to 2022, FINRA received over 25,000 investor complaints and ordered more than $70,000,000 in restitution to investors. FINRA collects and processes data for regulatory and transparency purposes only.[4]

[1] FINRA is registered with the Securities and Exchange Commission as a national securities association pursuant to the Maloney Act of 1938, 15 U.S.C. §§ 78o-3, et seq., amending the Securities Exchange Act of 1934, 15 U.S.C. §§ 73a, *et seq.* FINRA is the only entity recognized under – and the only regulator of the brokerage industry established by – this Act.
[2] SEC oversight is facilitated through the "FINRA and Securities Industry Oversight Examination Program," which conducts examinations of FINRA and the Municipal Securities Rulemaking Board.
[3] FINRA develops and administers qualifying examinations to securities industry professionals, which serve as a prerequisite to FINRA registration. FINRA also administers state law examinations on behalf of the North American Securities Administrators Association ("NASAA"), which Maine uses for state licensing purposes.
[4] FINRA is also subject to SEC's Regulation Systems Compliance and Integrity ("Reg SCI"), which regulates the technology infrastructure and security of FINRA and other critical portions of the securities industry. (17 CFR Section 242.1000.)

1735 K Street, NW
Washington, DC
20006-1506
t 202 728 8000
www.finra.org

"Sensitive Data" Should Exclude Data Collected and Processed by FINRA

The request for comments discusses the differences between the Connecticut Data Privacy Act and LD 1977, noting that the definition of "sensitive data" in LD 1977 is broader than the definition in Connecticut's bill. As noted in the December 11 hearing, this is largely because the Connecticut law is more content focused than some of the bills currently before the Judiciary Committee. In part, it is the broader definition of "sensitive data" in LD 1977 that would create significant regulatory oversight and investor protection concerns for FINRA.

For example, Sec. 9605-2 of LD 1977 prohibits a covered entity from collecting or processing sensitive data, unless it is necessary to "provide or maintain a specific product or service," or to achieve a purpose described in Sec. 9604 of the bill. Because Sec. 9604 does not contemplate regulatory oversight activities, if FINRA is considered a covered entity, it may be prohibited from:

- Collecting or processing information regarding the financial account numbers maintained or managed by regulated firms (which would be necessary to ensure compliance with applicable securities rules and laws, identify victims or wrongdoing, or ensure restitution when ordered),
- Accessing the communications of potential bad actors under investigation (or even ensuring that firms are meeting their obligations to monitor communications between employees and the investing public),
- Reviewing a potential bad actor's schedule as part of an investigation,
- Using technology (such as key card logs) to identify the location of an individual under investigation, or
- Reviewing the online activities of potential bad actors – just to highlight a few of the items.

These restrictions, among others, would significantly impact FINRA's ability to regulate broker-dealers based in Maine and financial advisors registered to do business in Maine, as well as FINRA's ability to protect Maine investors.

As discussed above and in our earlier letters, FINRA uses data for regulatory and transparency purposes only, and makes no commercial use of personal information. FINRA also shares information with law enforcement and government regulators – including the SEC and the Maine Office of Securities. The restrictions on sharing information could also negatively impact FINRA's ability to refer matters or provide information to the appropriate authorities in Maine for investigation and enforcement.

It is also important to note that, while these examples strictly focus on LD 1977, as that bill was the subject of the question in the request for comment and FINRA (the one and only national securities association registered with the Securities and Exchange Commission pursuant to the Securities Exchange Act of 1934) is currently excluded from the scope of LD 1973. Were FINRA not excluded from the scope of LD 1973, that bill too could negatively and significantly impact FINRA's ability to protect investors and regulate broker-dealers in Maine.

As such, we urge you to ensure that FINRA is excluded from the scope of any proposal that is reported from the Judiciary Committee – an exclusion which would be consistent with every state comprehensive data privacy law currently in place.[5]

A Gramm-Leach-Bliley Act Exemption Would Exclude FINRA-Regulated Entities

The request for comment also seeks information regarding whether the proposed Gramm-Leach-Bliley exemption should apply to entities or data. As your committee has heard, the Gramm-Leach-Bliley Act is a federal privacy law which, in connection with Regulation S-P, sets the current privacy standards for much of the financial services industry – including the brokerage industry that FINRA regulates.

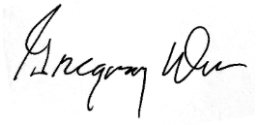
Currently, LD 1973 excludes entities and data covered by that Act. FINRA recognizes the value in this exemption. Yet, if state agencies are excluded from the scope of a bill, and Gramm-Leach-Bliley-covered entities or data are excluded from the scope of a bill, but a national securities association registered with the SEC is not, then that bill would create a situation where FINRA is subject to the restrictions on its regulatory activity while both FINRA's partner regulators and the entities it regulates are excluded from any such restrictions. This would create a significant gap in the investor protection safety net in Maine.

Requested Language

As such, FINRA respectfully requests that the Judiciary Committee ensures that any bill reported out of the committee excludes from its scope "a national securities association registered pursuant to § 15A of the Securities Exchange Act of 1934 (15 U.S.C. § 78a, et seq., as amended) and the rules and implementing regulations promulgated thereunder." This language would permit FINRA to continue protecting investors and overseeing the brokerage industry in Maine, without impacting the bill's effect on any other entities.

We thank you in advance for your time and effort and look forward to working with you on these proposals. If you have any questions, or if there is any further information we may be able to provide, please reach out to Kyle Innes at kyle.innes@finra.org or (646) 315-7367.

Sincerely,



Gregory J. Dean, Jr.
Senior Vice President
Office of Government Affairs
FINRA

[5] This includes laws in California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Tennessee, Texas, Utah and Virginia.

December 14, 2023

Maine Joint Judiciary Committee

and

Rep. Maggie O'Neil (D-129)

RE: the Data Privacy Protection Act (MDPPA) (L.D. 1977)

The Insights Association (IA), the leading nonprofit trade association for the market research and data analytics industry, offers comments on comprehensive privacy legislation before your committee, the Maine Data Privacy Protection Act (MDPPA) (L.D. 1977), on behalf of our more than 15 members in Maine, and to propose amendments.

IA's more than 7,700 overall members are the world's leading producers of intelligence, analytics and insights defining the needs, attitudes and behaviors of consumers, organizations and their employees, students and citizens. With that essential understanding, leaders can make intelligent decisions and deploy strategies and tactics to build trust, inspire innovation, realize the full potential of individuals and teams, and successfully create and promote products, services and ideas.

The Insights Association supports comprehensive federal privacy legislation that moves beyond the old-school notice-and-choice model, instead of a patchwork of conflicting state privacy laws built on those old models. A study[1] conducted by our member companies Research Narrative and Innovate MR, on behalf of Privacy for America, revealed that nearly all Americans surveyed (92 percent) believe it is important for Congress to pass new legislation to protect consumers' personal data, and a majority (62 percent) prefer federal regulation over individual state regulations. Four out of five voters (81 percent) support a national standard that outright prohibits harmful ways of collecting, using, and sharing personal data.

Congress made some progress on that front in 2022, passing the American Data Privacy and Protection Act (ADPPA) out of committee in the U.S. House -- legislation that was the basis for much of L.D. 1977 -- and we are pushing hard for a federal law even now.

However, should you and your fellow legislators decide to move forward with the MDPPA, the Insights Association wishes to highlight important points in the bill that we urge you to maintain and others we urge you to improve:

[1] New Study Shows Overwhelming Bipartisan Support for U.S. Federal Privacy Legislation. DECEMBER 1, 2021. https://www.insightsassociation.org/News-Updates/Articles/ArticleID/289/New-Study-Shows-Overwhelming-Bipartisan-Support-for-U-S-Federal-Privacy-Legislation

1. **Maintain the existing provisions on market research and audience measurement**: We appreciate the following provisions, which we urge you to maintain: In §9607 3(D), that subsection 1 could not be construed to prevent the use of incentives for research subjects in market research[2]; in the definition of "sensitive data", that clause L excludes "covered data used solely for transfers for independent video measurement"; and an exclusion from the definition of "targeted advertising" for "processing covered data strictly necessary for the sole purpose of measuring or reporting advertising or content, performance, reach or frequency, including independent measurement."
2. **Tighten the definition of "sensitive data" as it relates to common demographic data**: The current definition of "sensitive data" in the MDPPA includes relatively common demographic data, especially data revealing "An individual's race, color, ethnicity"– data so common that it is asked by the decennial census. The Insights Association urges you to avoid imperiling even the most basic of research studies by amending clause L of the definition with language at the end: "*, except to the extent such data is used solely for purposes of determining participation of an individual in market research, defined as the collection, processing, or transfer of covered data as reasonably necessary and proportionate to investigate the market for or marketing of products, services, or ideas, where the covered data is not— (A) integrated into any product or service; (B) otherwise used to contact any individual or individual's device; or (C) used to advertise or market to any individual or individual's device.".*"
3. **Tighten the definition of "sensitive covered data" as it relates to online activities data**: The definition's clause O, covering "[i]nformation identifying an individual's online activities over time and across 3rd-party websites or online services," would not allow for independent audience measurement, an essential underpinning to valuation of content and advertising (online and offline), which responsibly collects and shares covered data about individuals for the purpose of understanding groups. Advertisers, for example, pay based on the number of "impressions" for online ads, and independent measurement verifies that the number of impressions is accurate. Local Maine businesses would bear the burden of elevated costs for every impression inaccurately added to the count. Independent measurement also allows content creators to know their actual viewership/readership in relation to the marketplace, thus allowing for accurate programming and publishing decisions. Therefore, the Insights Association urges you to amend clause O of the definition of "sensitive data" by adding at the end: "*, except to the extent such data is used solely for the purpose of measuring or reporting advertising or content, performance, reach, or frequency, including independent measurement.*"[3]
4. **Centralize enforcement authority with the Attorney General, add a right to cure, and limit the private right of action**: IA encourages you to centralize enforcement authority for the

[2] D. "Prohibit a covered entity from offering a financial incentive or other consideration to an individual for participation in the collection, processing or transfer of covered data as reasonably necessary and proportionate to investigate the market for or marketing of products, services or ideas, when the covered data is not integrated into a product or service otherwise used to contact an individual or individual's device or used to advertise or market to an individual or individual's device"

[3] This clarification is based on the exceptions to the definition of targeted advertising in this same legislation.

MDPPA with the state Attorney General instead of authorizing private rights of action outright. Absent a centralized regulator and enforcer, private litigation would drive an industry of class action lawsuits for mere technical violations of a complex statute by legitimate actors, rather than deterring and punishing bad actors. Further, to improve compliance with a complex and complicated new law, we urge the inclusion of a 30-day right to cure violations (that does not sunset). Should you insist on maintenance of the private litigation, you should at least limit it to strictly injunctive relief, to assist in the push for compliance.

5. **Set guidelines to inform rulemaking power**: Given the complexity of the MDPPA and the privacy and security issues involved, the Insights Association urges adding the following clear guardrails for in the issuance of regulations or guidance in Section 19: (b) *Whenever the Attorney General is authorized to engage in rulemaking or issue guidance, the AG shall include an assessment of each of the following criteria to make a determination as to whether the costs to the privacy interests of individuals outweigh the countervailing benefits to individuals or to competition: (1) HARM TO INDIVIDUALS.—The AG must assess whether the practice has or is likely to substantially harm reasonable individuals targeted or affected by the conduct. The type of harm may be financial, physical, or reputational, or may involve substantial harassment or intrusion into private activity, but it must be real and concrete and not speculative or trivial. (2) BENEFIT TO INDIVIDUALS.—The AG must assess the benefits conferred by the practice, including the role of the practice in providing lower prices, greater availability and choice, improved functionality, and/or customer support for products or services. (3) IMPACT ON BUSINESS PRACTICES.—The AG must assess the role of the practice in enabling covered entities to compete and innovate in the marketplace or otherwise offer products and services to the public. (4) REASONABLE EXPECTATIONS OF INDIVIDUALS.—The AG must assess the context surrounding the practice from the perspective of reasonable individuals, including relevant disclosures and choices, the relationship of individuals to the practice and the persons or covered entities engaged in it, the target audience for the practice, and the sensitivity of the covered data at issue. (5) RISK MITIGATION.—The AG must assess whether the practice incorporates effective policies, practices, and/or technical measures to minimize the risk of individual harm and/or data practices contrary to reasonable individual expectations, and whether individuals can reasonably avoid such risks themselves.*"

The Insights Association and our members support strong consumer privacy protections within a regulatory framework that still allows for the pursuit of insights, as we've discussed above. We look forward to talking with you and your fellow legislators and staff further, and providing more information regarding these issues and the Maine Data Privacy and Protection Act (MDPPA) (L.D. 1977).

Howard Fienberg
Senior VP, Advocacy
Insights Association

Stocco, Janet

From: Gerrity, Bruce C. <BGerrity@preti.com>
Sent: Monday, December 18, 2023 11:51 AM
To: Stocco, Janet
Cc: Lesko, Amy P.
Subject: Response to Several Committee Questions by the Maine Automobile Dealers Association

The Maine Automobile Dealers Association ("MADA") submits the following comments regarding several of the Committee's requests:

1. Exemptions: The Legislature should exempt from new legislation the entities regulated by a variety of federal laws. This is particularly important from the automobile perspective since there are a number of rules from the Federal Trade Commission ("FTC") (for example the safeguards rule protecting privacy and the red flags rule, which require dealers to verify the identity of a buyer to make sure there is no fraud), the Bureau of Consumer Financial Protection ("BCFP") the Department of Labor, HIPAA and Gramm Leach Bliley, among others, which impact and secure privacy issues under federal law.

2. Small Business Exemption: MADA has dealers of markedly different sizes. Even though ever dealer is required to comply with privacy laws, whether they be large or small, for a small dealership the proposed legislation will be particularly onerous. Revenue is not a reasonable measuring stick as even one new unit will cost from $20,000 up to $100,000. One realistic measure would be number of employees. A reasonable number would be 25.

3. Data Minimization: Any legislation should be consistent with that in other states.

4. ISP Privacy Law Standards: The ISP privacy law standards should not be incorporated into new legislation.

Electronic Privacy Information Center Comments

1. Definition of Sensitive Data. The definition of sensitive data in LD 1977 is not only overly broad, but will also create inconsistency among different state definitions and standards. Consistency will reduce confusion and improve compliance, rather than requiring regulated entities to attempt to juggle multiple applications of law in different states. That will cause confusion and not be in the best interests of consumers.

5. Exemption for Entities under Federal Privacy Laws. Entities should be excluded. For example, the comments in the question about the GLBA privacy rights recognize that there are numerous other privacy standards regulated by other federal agencies and statutes. Parsing the data from one source of regulation to another (such as the FTC) will once again create confusion and inconsistency among state laws. The entity exclusion should apply across the general scope of federal privacy laws.

7. The Maine Unfair Trade Practices Act. The Maine Unfair Trade Practices Act has a long history of successful application both in terms of actions by the Attorney General for injunctive relief or damages as well as an independent consumer right of action. The Act balances a consumer's right to bring an individual action with the right of a business to defend itself by allowing a business to make an offer of judgment under Rule 68 of the Maine Rules of Civil Procedure which reduces litigation, allows for a higher probability of settlement, and creates an incentive for both sides to resolve their differences. A stand-alone private right of action as is currently proposed does not balance business and consumer rights in any way and will incentivize unwarranted litigation.

-- Bruce Gerrity

Bruce C. Gerrity
Partner
207.623.5300 Tel
207.650.4595 Cell
bgerrity@preti.com
Bio | LinkedIn | Twitter | preti.com

PretiFlaherty
45 Memorial Circle
P.O. Box 1058
Augusta, ME 04332-1058

Stocco, Janet

From: Josh Steirman <jsteirman@mainebankers.com>
Sent: Monday, December 18, 2023 11:33 AM
To: Stocco, Janet
Subject: RE: Requests for Comment - Privacy Bills - Due Dec. 18th
Attachments: Privacy comment letter_JUD_18 Dec 2023.pdf

Good morning Janet,

Attached is our comment on the first question, discussing the nature of a GLBA exemption. We urge the committee to adopt an entity-level exemption for financial institutions governed by GLBA.

Regarding question 5a, the example cites an industry other than banking, so I hesitate to comment. But typically the lender (who might hold the customer's financial data) is a separate legal entity from the auto dealer; the lender would be governed by an array of financial regulators, including GLBA oversight.

Please do not hesitate to reach out with questions or clarification.

Thanks and regards, Josh

Josh Steirman
Director of Government Relations
MAINE BANKERS ASSOCIATION
2 Thomas Drive | Westbrook, ME 04092

207-791-8406 office
207-239-5757 mobile
jsteirman@mainebankers.com
www.mainebankers.com

From: jud-ip-request@lists.legislature.maine.gov <jud-ip-request@lists.legislature.maine.gov> **On Behalf Of** Stocco, Janet
Sent: Monday, December 11, 2023 5:21 PM
To: jud-ip@lists.legislature.maine.gov
Subject: [jud-ip] Requests for Comment - Privacy Bills - Due Dec. 18th

Dear Judiciary Committee Interested Parties,

Invitation to comment:

MAINE BANKERS Association

December 18, 2023

To: Committee on the Judiciary, 131st Maine Legislature

Re: LD 1973 and LD 1977 – committee's request for comment regarding GLBA exemption

Senator Carney, Representative Moonen, and honorable members of the Committee:

We write today in response to the Committee's request for additional information regarding the details of an exemption from new data privacy legislation currently under consideration. 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, noting the following reasons: 1.) exemptions at the data-level would exacerbate a patchwork of laws across different states, 2.) a data-level exemption would create confusion, unnecessary government expense, and litigation, 3.) uncertainty emanating from a data-level exemption would lead to lower cyber-security standards for consumers, and 4.) banks are already thoroughly regulated, federal oversight is already robust, and this federal regulatory infrastructure for data privacy is built around entity-level supervision.

- Avoiding a patchwork of laws: of the states which have already passed similar data privacy laws, 12 out of 13 states enacted 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 small businesses.

- Minimizing government expense and preventing litigation: if Maine law utilized a data-level exemption, this would require the state to create new definitions of what is considered customer data under a wide variety of circumstances. Such a 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 being diverted to this type of unnecessary legal challenge.

- Data-level exemptions would put cyber security at risk: the 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. These systems, which customers choose to opt into at overwhelming rates, are much more secure than passwords alone. An entity-level exemption for financial institutions would provide the certainty needed to continue providing customers with the most advanced levels of technology for customer safety and data security.

- Harmonizing with federal oversight: banks are already subject to extensive regulation (including GLBA) which mandates high standards of data security and notice of data practices to consumers. 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 business laws only enforced by the threat of prosecution or litigation. Furthermore, GLBA continues to be updated by rulemaking and legislation, such as recent passage in the US House of the Data Privacy Act of 2023.

For these reasons we respectfully urge the Legislature to include an entity-level GLBA exemption in any new data privacy legislation. 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.

Thank you for your consideration, we remain ready to address any further questions from the Committee.

Respectfully Submitted,
Joshua Steirman
Maine Bankers Association

Maine Credit Union League

2 Ledgeview Drive · Westbrook, ME 04092
Mailing Address: P.O. Box 1236 · Portland, ME 04104
207-773-5671 · 1-800-442-6715
www.mainecul.org

To: Committee on Judiciary

From: Ellen Parent,
Director of Compliance

Cc: Susan Pinette, Committee Clerk
Janet Stocco, OPLA Analyst
Elias Murphy, OPLA Analyst

Date: Monday, December 18, 2023

Subject: Gramm-Leach-Bliley Privacy Exemptions

Summary:

Financial institutions, such as credit unions, are subject to the provisions of the Gramm-Leach-Bliley Act (GLBA) which contains provisions protecting the nonpublic personal data of their consumers and providing notice to their customers when their data is disclosed to nonaffiliated third parties. This law applies when the consumer interacts with the financial institution and provides nonpublic personal information in order to obtain a financial product.

In general, a financial institution may not share nonprivate personal information with unaffiliated parties. There are a few exceptions to this, but even in those cases, the recipients may not disclose the information they receive except subject to an exception, such as to law enforcement subject to an authorized subpoena, to process transactions, or at the customer's request.

Financial institutions must provide, initial, annual, and any revised privacy policy notices and must provide consumers with a notice about how to opt out of any sharing that the institution may do under one of the limited exceptions.

Data Level Exemption:

Two of the twelve states that have instituted comprehensive privacy legislation have exempted data that is subject to the provisions of GLBA, these two states are California and Oregon. Oregon exempts financial institutions who are regulated and examined regularly by the state or the federal financial services regulators. California maintains a data-only exemption for credit unions and other financial institutions. This means that financial

Maine Credit Union League

2 Ledgeview Drive · Westbrook, ME 04092
Mailing Address: P.O. Box 1236 · Portland, ME 04104
207-773-5671 · 1-800-442-6715
www.mainecul.org

institutions have to maintain two different data regimes, one for data related to financial services, and one for other types of data.

Data that is not subject to GLBA includes data relating to employees, data relating to commercial or business financial relationships, prospective customers, and any information collected through a website on a prospective consumer such as what data is clicked on.

In California, there has been a back-and-forth debate over the collection and rights of individuals whose data is collected by is not subject to GLBA exemptions, especially the information of employees. The rights of deletion remain one of the more difficult concerns as deletion rights at a financial institution might be in conflict with federal law. Financial institutions have established processes to protect their consumers, a data level exemption could lead to them to collect more information than previously to determine which data falls into each category.

Uniformity:

Uniformity across states remains a major priority for credit unions. Of those states that have adopted a comprehensive privacy legislation, only one has not exempted credit unions at an entity level. Maine's credit unions are small financial institutions who take their compliance obligations extremely seriously. The added burden of complying with a privacy law that is significantly different than other nearby states means that the costs of compliance are higher for Maine credit unions and makes it more expensive for them to operate than those who are across the border in New Hampshire or in other New England states. In addition, while states are free to adopt legislation more strict than that of the federal government, there could be a conflict in laws when determining which legislative regime affords consumers greater protection.

Examinations:

Credit unions are examined regularly. Depending on their size, a credit union is examined by the National Credit Union Administration, the Bureau of Financial Institutions, or both, on an annual or eighteen-month cycle. One of the aspects examined is the security and protection of nonpublic personal information and compliance with GLBA. Regulators have procedures in place to ensure that credit unions are treating their consumers' data with the proper care and security. In addition, credit union regulators have a number of enforcement options at the ready, including, in dire cases, closing down a credit union. Adopting a data level exemption will necessitate the creation of new examination procedures at the state level.

MAINE
STATE
CHAMBER
of
COMMERCE

The voice of Maine business

December 18, 2023

Joint Standing Committee on Judiciary
100 State House Station
Augusta, Maine 04333

RE: LD 1705, LD 1902, LD 1973, and LD 1977

Senator Carney, Representative Moonen, and members of the Judiciary Committee:

The Maine State Chamber of Commerce appreciates the opportunity to provide additional comments on the privacy legislation (LD 1705, LD 1902, LD 1973, and LD 1977) that is being considered by the Committee. First and foremost, without a federal data privacy protection law in place, the Chamber is concerned that patchwork laws will hinder the business community. Therefore, the Chamber supports the Maine Legislature passing legislation that is similar to the well-vetted framework adopted by twelve other states thus far. We believe LD 1973, *An Act to Enact the Maine Consumer Privacy Act*, is the best vehicle to accomplish that.

The Chamber also supports an entity level exemption for companies currently regulated under the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach Bliley Act (GLBA). In 1996, HIPAA established a national standard to protect the privacy of individuals' medical records and identifiable health information, and to limit the use of such information without an individual's authorization. Regulated entities include health care providers, health insurance companies, and government programs, such as Medicare and Medicaid. Shortly after, in 1999, entities such as banks, credit unions, and insurers that provide financial services and products began getting federally regulated under the GLBA. As these entities are already regulated, the Chamber believes it makes the most sense to exempt the entities themselves rather than the data they work with; this is consistent with legislation adopted by other states.

Maine has hundreds of small businesses that make up the backbone of our economy who may be negatively impacted by the privacy legislation currently being considered if some type of exemption isn't put in place for them. The Chamber believes "small business" should be defined in the law and based on the number of consumers the business collects or processes data for, rather than basing it off revenue. This would be inline with the framework of other states; for example, Oregon and Virginia have a threshold of 100,000 consumers.

Finally, the Chamber has concerns with the definition of "sensitive data" as defined in the amendment to LD 1973 that Senator Keim presented to the committee on December 11, 2023. Sensitive data most commonly refers to an individual's race and ethnicity, sexual orientation, and government-issued identifiers like a social security number. However, the definition in the amendment goes beyond that to include:

E. Online usage information derived from the consumer's use of a controller's online product or service, including but not limited to web browsing history and search data, content of communication, device and or online identifiers (e.g. MAC address, IP addresses, etc.);

The Chamber believes online search data and web browsing fall outside of "sensitive data" parameters. Therefore, the Chamber believes the definition should be amended, striking that language.

Again, the Chambers appreciates the opportunity to provide feedback on this important issue and asks that the committee adopt a framework that has been vetted and adopted by other states.

Ashley Luszczki
Government Relations Specialist
Maine State Chamber of Commerce
aluszczki@mainechamber.org

MAINE ASSOCIATION OF HEALTH PLANS

December 18, 2023

Senator Anne Carney, Senate Chair
Representative Matt Moonen, House Chair
Join Standing Committee on Judiciary
100 State House Station
Augusta, Maine 04333-0100

RE: Response to Committee Request for Comments

Dear Senator Carney, Representative Moonen, and Members of the Committee:

The Maine Association of Health Plans consists of licensed health insurance carriers operating in Maine and providing or administering coverage for approximately 600,000 Mainers. We welcome this chance to respond to the Judiciary Committee's request for comments.

Overview

Since 1996 the federal Health Insurance Portability and Accountability Act (HIPAA) has governed the privacy and security of Americans' health care data. HIPAA establishes consistent federal standards to protect individuals' medical and health plan records and other individually identifiable health information, collectively defined as "protected health information" (PHI).

HIPAA applies to "covered entities" including health plans, health care clearinghouses, and most health care providers as well as "business associates" which are contractors managing PHI for covered entities.

Like HIPAA, the Gramm-Leach-Bliley Act (GLBA) governs the privacy and security of consumer and customer information held by "financial institutions." This includes companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance.

Since consumers' personal health information or financial information can be collected by entities not covered by HIPAA and GLBA, states are seeking to create a parallel consumer data privacy infrastructure.

Support HIPAA/GLBA Exemptions at the Entity Level

Covered entities subject to HIPAA/GLBA should be exempt from new state consumer data privacy legislation. For exemptions of a HIPAA-covered entity, the following model language is recommended:

This Act shall not apply to an entity subject to and in compliance with the federal Health Insurance Portability and Accountability Act (Pub. L. 104–191, 110 Stat. 1936, enacted August 21, 1996) and the rules promulgated thereunder.

For exemptions of an entity subject to the Gramm-Leach Bliley Act (GLBA), the following model language is recommended:

This Act shall not apply to an entity subject to and in compliance with regulations promulgated pursuant to Tit. V of the federal Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801 – 6809.

De-Identified Information

Information that is de-identified in accordance with 45 CFR 164 should be exempt. The following model language is recommended:

"Personal Information" does not include information that (i) does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used, alone or in combination with other information, to identify an individual, or (ii) is anonymized using a method no less secure than methods provided for under HIPAA.

Employee Exemption

Comprehensive data privacy laws should also not apply to personal information that is collected by a business about a person in the course of the person acting as a "job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of" the business to the extent that the personal information is collected and used within the employment context.

Definitional exemptions should make clear that "consumer" does not include a natural person acting in an employment context and/or that "personal information" does not include data or employment information.

Use related exemptions should explicitly permit the processing of employment data in the context of employment and application for employment; use of emergency contact information for emergency contact purposes; and use of employment information for benefits administration.

Business-to-Business ("B2B") Exemption

Comprehensive data privacy laws should not apply to business-to-business ("B2B") communications or transactions, such as activities concerning due diligence regarding a product or service, providing a product or service, or receiving a product or service.

Such an exemption should apply to information "reflecting a written or verbal communication or a transaction" between the business and an employee or contractor of another organization (i.e., a business, non-profit, or government agency), where the communication or transaction occurs in the context of (1) the business conducting due diligence on that other organization, or (2) the business providing or receiving a product or service to or from such organization.

Definitional exemptions should make clear that "consumer" does not include a natural person acting in a commercial context and exclude commercial information such as that noted above from any definition of "personal information."

Support State Licensed Insurer Exemption

Comprehensive data privacy laws should also not apply to entities that are subject to the state's insurance licensure requirements. The Tennessee Information Protection Act, for example, exempts "an individual,

firm, association, corporation, or other entity that is licensed in this state under [title] as an insurance company and transacts insurance business."

In Maine, consumer health data is also protected by the Maine Insurance Information and Privacy Protection Act (IIPPA) and is enforced by the Superintendent of the Bureau of Insurance. In a May 22, 2023, letter to the Committee, the Bureau expressed concerns with proposed provisions that could conflict with existing Maine law and urged an exception for consumer health data covered by existing state law.[1]

Topics for Comment Requested by the Committee

- What "data minimization" do you recommend that the Legislature adopt in consumer data privacy legislation?
    - We recommend use of the HIPAA's Privacy Rule's approach to "data minimization," through its "minimum necessary" standard and implementation specifications. This approach works well and allows entities to use and disclose data necessary for permitted purposes.

Eliminate Private Right of Action (PRA)

PRA are often costly for businesses, draining resources and stifling innovation. The availability of a PRA should be eliminated. If not eliminated, the right should be at least limited to circumstances where injury can be proven, and the violation was due to willful neglect.

Any enforcement by the Attorney General should similarly be tied to the regulated entity's culpability, and a regulated entity needs to have the ability to cure certain violations (e.g., violations not due to willful neglect that are cured within a 30-day period) prior to any enforcement action.

Thank you for your consideration of these comments.

Sincerely,

Dan Demeritt
Executive Director

[1] https://legislature.maine.gov/backend/app/services/getDocument.aspx?doctype=test&documentId=10024887

Maine Hospital Association

MAINE'S LEADING
VOICE FOR HEALTHCARE

Privacy Bills

Response to Questions

December 18, 2023

Please accept these comments as Jeff Austin's response to both the questions posed at the previous work session and the questions sent in an email by Ms. Stocco.

1. [Re. Moonen]: ***Please reach out to Oregon, Colorado and Delaware, three states that do not have entity level exemptions, and ask how it is going for hospitals there.***

   MHA Response: I reached out to Oregon and Colorado as I personally know my counterparts in those states; I don't know my counterpart in Delaware.

Oregon indicated that its law goes into effect in July 2024, so there is no actual experience with the law. Colorado's just went into effect in July, 2023.

However, both Colorado and Oregon felt they were able to secure a number of exemptions that are tantamount to an entity-level exemption. We would simply argue that if so much information is exempted at the data level, why not do an entity exemption like other states do.

A few observations about Colorado and Oregon. For example, the information related to employment is exempt in both Oregon and Colorado. I did not think LD 1977 applied to the employment context, although it is unclear. Oregon and Colorado expressly exempt employment-related information. Furthermore, there are entity-level exemptions in Oregon for other entities.

The data exemptions in LD 1973 (Sen. Keim's bill) may not be as broad as in Colorado or Oregon.

Finally, I know Oregon rejected a private right of action, I'm not sure about Colorado.

If you are not inclined to grant an entity level exemption for HIPAA covered entities, as most states do, based upon the fact that Oregon and Colorado don't have entity exemptions, then please look at their other provisions such as the broad array of data exemptions and the elimination of private right of action as well.

2. [Rep. Kuhn] ***If an entity level exemption is provided to hospitals or other healthcare entities, does that spill-over to any insurance carriers with which the healthcare covered entity is related (e.g., Martin's Point and its Medicare Advantage plan)?***

   MHA Response: No. Insurance companies are covered entities themselves and would be independently exempt.

Also, many other states have entity level exemptions and so there should be some experience from other states about affiliations between covered entities and non-covered entities and you could ask the analyst to contact other states and see how this concern is addressed. I can say for hospitals that we are not seeking an entity level exemption for the purpose of exempting data of an affiliated business.

Suffice it to say, we would not oppose some clarifying language. For example, a provision that said that the covered entity exemption only applies as long as the covered entity receives the majority of its revenue from its covered entity activities (e.g., healthcare) as opposed to some affiliated business.

3. [Rep. Sheehan] ***Do hospitals collect biometric information***?

   MHA Response: The provision of healthcare itself involves a lot of biometric information, but it would be subject to HIPAA. Otherwise, I only know of its use in the employment context.

The only biometric information used (I hesitate to say collected) that I am aware of is in the employment context. For example, in order to access computers that contain HIPAA-protected information, there are many passwords etc. Clinicians often get frustrated with the amount of signing-in and signing-out that they have to do in a day. So, a HIPAA-compliant biometric system, like a fingerprint system, is much faster and easier than typing passwords and swiping access cards. Our members would not say that they collect or store the fingerprint. Nevertheless, it is used.

Keep in mind, I'm not sure LD 1977 covers the employment context. Some of the provisions in LD 1977 don't really make sense in the employment context. For example, so many sections of the law are premised on the term "consumer." Furthermore, section 9607 (prohibiting retaliation) appears to only apply to the provision of goods and services, not employment. But it is a bit ambiguous, in my opinion.

Again, if you are not inclined to grant HIPAA covered entities an entity-level exemption, we feel strongly that the bill you enact should be clear that it does not apply to employment-related information.

Questions posed in Ms. Stocco's email.

1. *Whether the Legislature should exempt from new state consumer data privacy legislation either the data or the entities (or both) regulated by other federal laws, for example the data or entities regulated under HIPAA or the Gramm-Leach Bliley Act.*

We believe Maine should follow the lead of most of the other states that have an entity level exemption. We've previously explained why in two prior memos.

4. *With respect to the question whether general consumer data privacy legislation should exclude <u>entities</u> governed by existing federal privacy laws or instead only the <u>data</u> protected under those laws:*
    a. ***GLBA**. Sometimes a business, like a car dealership, has both a financial side (covered by GLBA) and a non-financial, marketing side (not covered by GLBA). It is the committee's understanding that proposals to exempt from the scope of state consumer privacy legislation the <u>data</u> regulated by the GLBA rather than the <u>entities</u> regulated by the GLBA would ensure that such businesses would be prohibited from using information that would protected by GLBA on the financial side of the business on the non-financial marketing side of the business where the data is not protected under the GLBA. Is this true?*
    b. ***HIPAA**. **Similarly, if the state legislation includes an exemption for <u>entities</u> regulated by HIPAA, how can the committee ensure that this exception doesn't allow a HIPAA-regulated entity to use consumer data collected on the healthcare side of its business for non-healthcare purposes?***
    c. *Is there any way to address these concerns other than employing data-level exemptions to the state legislation? For example:*
        - *Would it be effective for the state legislation to include an exemption for entities governed by the GLBA or HIPAA but only to the extent that they are engaging in activities subject to the GLBA or HIPAA? **or***
        - *Would it be effective for the state legislation to define "covered data" in a way that excludes information covered by the GLBA, HIPAA (and FERPA as well as the other laws)? **or***
        - *Is there another possible approach?*

I will attempt to answer the question in bold above about HIPAA data. I'm not sure what fact pattern this question is driving at. Consumer data "collected on the healthcare side" of the hospital business is generally HIPAA protected and so its use would be governed by HIPAA.

Hospitals may have some data that is not HIPAA protected. For example, people who enroll in a nutrition class. We may have names and addresses and phone numbers of people who join a nutrition class. That data would not have been collected for healthcare treatment purposes, so it's not HIPAA data. I would argue it's not "data collected on the healthcare side of its business". If we had an entity exemption, this data would not be subject to either HIPAA or LD 1977.

We continue to believe it is the obligation of those who seek to regulate businesses to articulate the concern, preferably with specific examples of what has happened in Maine, and to tailor the regulation to that concern. This has been the posture of the Judiciary Committee in the past, on issues such as sharing cell phone location data with law enforcement.

Has anyone articulated a specific concern with hospitals collection, use and storage of nutrition class information or any other similar data that is not HIPAA protected? We don't believe so.

We prefer not to be included in a regulatory regime with myriad administrative obligations because of small, discreet pockets of data that are very much ancillary to our primary activities, primary activities which are regulated by HIPAA.

Please remember, this law will not be written in stone. In the future, if a concern does emerge with specific reference to actions being taken by hospitals or other healthcare providers in Maine, you can act then. But, conversely, to the extent that the legislature chooses to regulate as broadly as possible now the premise that it can be scaled-back later if found to create problems, please keep two things in mind. First, that rarely happens; regulatory reach tends to expand over time, not retract. Second, regulated entities have to invest in financial, IT and human resources to comply with the law in the interim. We believe it is more reasonable to being in a more focused way and expand as necessary in the future.

Thank you for accepting these comments.

THE LAW OFFICE of DANIEL J. BERNIER LLC

December 13, 2023

To The Distinguished Members of the Judiciary Committee

From Daniel J. Bernier, representing the Maine Insurance Agents Association

Re: Invitation to comment on LD 1705, LD 1902, LD 1973 and LD 1971

I represent the Maine Insurance Agents Association, an organization of insurance agents throughout the State. Not only are insurance agencies regulated under Gram Leach Bliley and HIPAA, but Maine also adopted the National Association of Insurance Commissioners Model Insurance Data Security Act which can be found in 24 M.R.S.A.§2261 et. seq. So there is already sufficient regulation of the insurance industry. While not all of the insurance industry supported the passage of the model law, the Maine Insurance Agents Association supported the Superintendent of Insurance a few years ago when he proposed the NAIC Model Act. The Model gives the Superintendent the authority to look at the size of an operation in terms of the guidelines that they issue for cyber security; the guidelines that would be necessary for a small Main Street insurance agency are different from those for a big international insurer. An insurance agency also does have some unique aspects to it as local agencies do need to interact with insurance companies for quotes on pricing, and for claims. Given that there is a specific law which addresses the insurance industry and a regulator with a staff to oversee that law, conduct audits and most importantly to be available for local insurance agencies if they have questions on what they should be doing, it does not make a lot of sense to impose yet another regulatory regime which could conflict of that with the Maine Bureau of Insurance.

The Maine Bureau of Insurance provides guidance on compliance with this law and what is particularly good is if a local insurance agency has questions on what they are supposed to be doing it is easy to have a conversation with Bureau Staff. If an agent is not following the law the Superintendent has the authority to penalize them including revoking their license. The Superintendent issues Bulletins providing guidance on the law; most recently Bulletin 468.

As a Maine resident, I do appreciate the committee looking at these issues, especially for industries where there is little regulation. However, any regulation of insurance agencies should be in title 24-A which is enforced by the Superintendent. Having multiple laws regulating insurance agencies can run into issues of conflicts between those laws and how do we resolve those conflicts. When something is outside title 24-A there can be issues of the

179 Main Street, Suite 304 * Waterville, Maine 04901 * t 207.877.8969 * dan@bernierlawoffice.com

Superintendent's ability to enforce statutes outside title 24-A or to provide guidance on those statutes. If the committee is concerned about gaps in title 24-A, the best course of action would be to write a letter to the Superintendent requesting he address those gaps through statute or rulemaking under title 24-A.

Thank you for your time.

Very truly yours,

Daniel J. Bernier

DJB/hb

179 Main Street, Suite 304 * Waterville, Maine 04901 * t 207.877.8969 * dan@bernierlawoffice.com

PIRG (Public Interest Research Group) & ConnPIRG's Comments to the Maine Judiciary Committee on the Weaknesses of Connecticut's Data Privacy Act
12/18/2023

PIRG is a consumer protection and public interest group with state chapters across the country, including our Connecticut chapter, ConnPIRG which was involved in trying to make the state's consumer privacy bill stronger. We had concerns with the bill that ultimately passed, and appreciate the opportunity to share our concerns.

There are 3 issues we wish to touch on briefly.

1) **Data minimization.** Connecticut's law put in place a harmful standard for what data companies can collect from consumers and what they can do with it. The way the law is currently drafted, it amounts to businesses being able to collect, process and use whatever data they want, as long as *the company* views the data collection as being relevant to delivering the service in question, and its collection and use practices are "disclosed to the consumer" - which often happens inside a company's privacy policy.

   It will likely come as no surprise to the Committee that disclosing what you do with data in the fine print is decidedly not a consumer-friendly practice, as these documents are long and full of hard-to-understand legalese. Instead of putting the onus on the consumer to set aside 30 minutes or more to play lawyer and parse a document full of vague and tricky language, it should be required that companies must limit upfront what data they collect to ONLY what's strictly necessary to deliver the service the consumer is expecting to get from a company. The company should also use that data only for that explicit purpose, and not for any secondary purposes. This orientation is key - it's not about what data collection a company thinks is appropriate. A real data minimization standard puts the expectations of the consumer front and center.

   For example, in order for a company to process and ship a consumer's purchase, the company needs to know what item the consumer bought, where to ship it, and what contact information they should use in order to communicate about any questions or concerns in the process of fulfilling the order. This all makes sense, and is proportionate to what a consumer is expecting to get - the item they bought delivered to their door.

   It does not make sense, however, for that company to be able to then turn around and sell or share that information with third parties. Google does not need to receive information about what I bought. Neither does Facebook, nor data brokers, nor any other party hoping to monetize my data. What I buy and how I interact with a retailer should be between me and the retailer alone. Unfortunately right now, unfettered data sales and sharing are the de facto assumption virtually anytime a consumer interacts with an online service, including a retailer's website.

   This is a problem. The more data a company collects about you, and the more it shares

that data with other companies, the more likely it becomes that your data will be exposed in a breach or a hack and end up in the wrong hands, like with scammers or identity thieves.

Implementing a real, consumer-oriented data minimization standard does not mean the end of companies being able to advertise to their customers. Retailers can still use their own customer's information to communicate with them directly about products and services they might be interested in. What changes is the number of unnecessary actors collecting data about

To protect consumers' data, what's needed is a broad prohibition on unnecessary data collection and secondary uses by companies - a real, consumer-oriented data minimization standard.

2) **Entity-level exemptions.** Connecticut's law includes entity-level exemptions for whole industries that don't have to comply with the law. This includes health insurance companies, hospitals and doctor's offices covered by the Health Insurance Portability and Accountability (HIPAA), and financial institutions as covered by the Gramm-Leach-Bliley Act (GLBA).

   Both HIPAA and GLBA were passed in the 90s. Technology has advanced by leaps and bounds since then, making these laws inadequate for the threats consumers face now. Entity-level exemptions based on these outdated laws serve to give the companies we trust our most sensitive information with broad leeway. These institutions take advantage of this loophole.

   According to a 2020 study by the U.S. Government Accountability Office (GAO), banks and credit unions gather a lot more data about people than is really necessary, including social media and web browsing activity. These institutions share information like people's financial information like income with a variety of third parties, vaguely called "affiliates", for whom getting detailed information about is nearly impossible.

   For protecting consumers, it's much better to enact exemptions on the data or purpose level (i.e. prohibitions on the collection of certain classes of data, or on specific uses of data) than give certain types of companies carte blanche - especially when it comes to health and financial data, which most people consider to be extremely personal information.

3) **A private right of action for individuals.** Connecticut's law does not include the right for individual consumers to take companies to court for misuse of personal data. This is a problem. Especially when it comes to under-resourced enforcement agencies, such as state AG offices, the ability for individuals to sue is one of the absolute best deterrents to corporate abuse. Maine could follow what Illinois has done, where aggrieved individuals

can seek damages under the state's Biometric Information Privacy Act (BIPA). The Illinois State Supreme Court has upheld this right during judicial reviews of the law.

If there is anything ConnPIRG and PIRG can do to be of assistance as Maine considers putting stronger protections on the books, please do not hesitate to reach out to us.

R.J. Cross
rj@pirg.org

Written comments on LD 1705, LD 1902, LD 1973 & LD 1977

Submitted by Lisa Margulies, Vice President of Public Affairs, Maine, on behalf of Planned Parenthood of Northern New England, and George Hill, President/CEO, on behalf of Maine Family Planning

1. *Whether the Legislature should exempt from new state consumer data privacy legislation either the data or the entities (or both) regulated by other federal laws, for example the data or entities regulated under HIPAA or the Gramm-Leach Bliley Act.*

Planned Parenthood and Maine Family Planning support policies that protect individuals' right to privacy and control over their personal health-related 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 health data is essential in safeguarding health care access. In light of this, Planned Parenthood and Maine Family Planning support the legislature's interest in increasing data privacy protections in the state.

However, it is essential that bills addressing consumer data do not conflate consumer's sensitive health-related data with patient information protected under HIPAA and related state laws. Subjecting HIPAA covered entities to two different, and sometimes conflicting, data maintenance regimes would create significant compliance concerns for health care providers and entities covered by HIPAA.

Failing to provide a clear carve-out for information and entities already subject to HIPAA would create confusion and compliance concerns for health care providers, who already must comply with a broad range of privacy protections and limitations on disclosures. Asking health care providers to navigate these dueling frameworks would create significant administrative and financial burdens for these essential providers, including non-profit organizations like ours, which are already pressed to meet funding demands in a drastically altered post-Covid healthcare landscape while continuing to provide free or significantly discounted care throughout the state for anyone who needs it.

As providers of comprehensive reproductive and sexual health care in this state, we urge the Committee to ensure that these consumer data privacy bills do not unintentionally adversely impact health care providers and adopt an exemption for data and/or entities regulated by HIPAA. To best ensure workable protections, these bills must be sufficiently tailored to address personal data and entities not otherwise subject to HIPAA and related state medical records laws through, at a minimum, a clear functional carve-out for PHI and intermingled information held by entities subject to HIPAA.

Restore the Fourth:
Statement on LD 1973 amendments

Restore the Fourth is a nonpartisan 501c(3) advocacy group based in Boston, MA with members in Maine and chapters in many US states. RT4's name refers to the Fourth Amendment to the United States Constitution, and its core mission is advocacy for better privacy protections for US persons and a decrease in unconstitutional mass surveillance through better legislation.

Restore the Fourth generally supports consumer privacy legislation modeled after the high standards already passed in many foreign jurisdictions such as the European Union, Canada and elsewhere, with appropriate adaptations to the US context including, for example First Amendment considerations for freedom of the press, open government, right to protest, etc.

In our opinion, the Connecticut-model bill, already adopted by or under consideration in at least a dozen states, does not protect privacy as strongly as ADPPA-style bills like Representative O'Neil's LD 1977. However, in the interest of improving Senator Keim's LD 1973, we would like to provide our recommendations and some background to the committee regarding three specific points that the committee discussed in their prior working session:

1. Applicability Threshold

To effectively address common privacy concerns, and provide adequate protection of political, ethnic, sexual or other minorities, the threshold should not reflect the typical volume of consumer data a company routinely handles in their normal course of business.

Instead, the number should fall *just under* the number of Mainers who comprise minority groups whose rights are frequently at risk from privacy violations. From this human and civil rights angle, balanced with the interests of the small business community, we recommend a value of 35,000 for a state with a population between 1 and 1.5 million, as has also been negotiated in Delaware and New Hampshire.

Within the state of Maine, minorities may utilize services or online applications that provide community-specific resources. Consider the real-world implications of a threshold of 100,000 consumers placed on applications or online platforms operating in Maine, targeted toward minority populations such as the gay community, immigrants seeking legal assistance, law-abiding gun owners, Christian minority groups, African Americans reporting instances of police brutality, or Jewish individuals seeking kosher food options. Using a threshold of 100,000 would affect vulnerable groups of individuals residing within the state of Maine regardless of political persuasion and affect their exercise of constitutionally

protected rights and freedoms at very least through self-censorship, based on the knowledge that their activities are being recorded and exchanged for valuable gain, and can end up in the hands of government or other parties capable of coercive force or other injury.

In the current draft of Senator Keim's LD 1973, "consumer" is defined as only state residents, and the threshold of 100,000 consumers comes from Connecticut, a state which has a population of 3.6 million. Companies operating in Maine will naturally encounter a smaller volume of consumers and their data. In contrast, a state like Delaware with a population of 1.0 million sits closer to Maine's population of 1.4 million. Delaware's privacy law applies a threshold number of consumers at 35,000, which is a more appropriate and reasonable threshold, and the same 35,000 has been negotiated in New Hampshire's recent SB 255. Montana's recently passed law uses a threshold of 50,000.

2. Guidance on data minimization: necessary for protecting rights

What is data minimization?

Data minimization is limiting the *collection, processing, transfer and storage/retention* of personal information - to *only* that which is directly relevant and necessary to accomplish a specified purpose.

However, note that there are at least two standards of necessity in this regard in existing law. We refer you to EPIC and PIRG's testimonies for the distinction between the legal terms of art "strictly necessary" and "reasonably necessary."

Instead, here we would like to present you with examples of why data minimization is necessary for the protection of fundamental rights, as well as what it means in various stages of the data processing lifecycle.

Why do we need data minimization?

> **Without Data Minimization:** Consent fatigue where the consumer has to predict how their data could be used, and individually opt in or out to every single potential data type or use case, inevitably failing to control the spread of their data. Imagine a woman seeking an abortion in Maine, or a gun owner seeking information on firearm maintenance, or a religious minority seeking information on religious services - finding themselves having to determine the list of companies whose software runs on their phone and collects excessive data, and analyze and opt out of every single one in order to defend their rights.

With Data Minimization: Data subjects/consumers can have the expectation that the use of their data is appropriate. This approach places the role of limiting data spread squarely on the data controller, who is best positioned to know how their systems work and why data is needed, and has the resources to implement the controls. Proactively protects everyone in the population, including the most vulnerable.

Herd immunity: Data protection produces a collective immunity of the population from certain kinds of intrusions that can affect not only individual freedom and privacy, but also freedom from coercion and the exercise of democratic rights. Data minimization ensures that everyone is protected, rather than the few who have the resources, time, interest and technical and legal expertise to assert rights one by one with every data processor affecting Mainers.

Stages of data flow affected by data minimization, with examples

Collection: Let's say a company asks you for your social security number. They might need it later, but for now there's no reason they do. They could provide you a different, internal ID number, or for example for HR software they could use your employer ID. However, if you refuse to provide your SSN, they can refuse you service. This is pretty unique to the US, and one of the reasons our social security numbers are hacked so often from so many different sources. This would be different with Data Minimization: You would only need to provide information that was actually needed, and could not be denied service if you refused irrelevant data.

Processing: Your data was legitimately needed to provide you with a service you requested, and it was also processed to provide you what you asked for! However, it was also used in another way. For example, in combination with other data, it was used to try to predict the likelihood that you are pregnant or seeking an abortion. This would in some cases not be permitted with data minimization. [need a better example here] This is also known as a prohibition against "secondary purposes."

Transfer: Your data was needed to provide you with a service you requested, and was internally processed by the data collector - as well as correctly transferred to their contractors for billing and shipping, so you can receive an item you ordered in the mail after paying for it! However, your data is then also transferred to a third party who might use it for a different purpose or exchange it onwards, for example a data broker. This would not be permitted with data minimization.

Storage/retention:

(Limited storage) After placing an order, your shipping information needs to be stored at least until you receive the package, and some additional information associated with both billing and shipping may need to be held for some years for tax auditing purposes, disputes, legal liability, etc. In other words, many times it makes sense to store data. However, after some time has passed, the data is not relevant anymore. With data minimization it could no longer be stored once no legitimate business purpose, in line with original purposes of collection and processing, remained.

(No storage) There are also cases where data does not need to be stored at all: for example, when it needs to be momentarily processed to return a result. This might apply to decision making on an autonomous vehicle based on camera input, placing a call or sending a message by an instant messaging application, processing verbal commands, or performing automatic translation of text.

(Purpose of retention limits) This measure reduces the likelihood that data is hacked after the fact, subject to law enforcement proceedings, or repurposed by industry in violation of the data subject's rights.

Isn't this burdensome or controversial?

The first country in Europe to introduce such strong laws was actually Germany, one of the strongest economies in the world, in 1970-1977. Data minimization has been law in parts of Europe since shortly afterward, and eventually the whole EU by 1995 - partially as a counterreaction to excessive government collection of personal data in WWII, something we in the US frequently cite as a distinction between authoritarian and stably less authoritarian governments. Data minimization is the standard in GDPR, the comprehensive EU Regulation that went into effect in 2018, and improved upon the earlier directive from 1995. Data minimization is also standard in PIPEDA, Canada's data protection law since 2002, as well as similar legislation in other economically advanced countries including South Korea, New Zealand, Argentina, Israel, Switzerland, Norway, and Japan.

3. Entity-Level Exemptions

Finally, Restore the Fourth would like to caution the committee about the risks inherent in granting entity-level exemptions in privacy laws, and how they provide a large window for companies to violate legislative intent.

With entity-level exemptions, any entity in any line of business can choose to exempt all of its activities from the law by dedicating an insignificantly small portion of its business to an exempt class. The three main types of entity-level exemptions we have found under consideration during hearings in state legislatures, so far, have related to financial institutions (typically governed by GLBA), healthcare companies (governed by HIPAA), or companies providing data relevant to consumer credit reporting (presumably - but often not - covered by FCRA).

1. The present bill does provide an entity-level exemption for GLBA-covered entities. As such, a company which uses 1% of its net worth to purchase a small payments or banking app, will not have to comply with LD 1973 for any of their data collection, processing or transfer activities. This would not seem to accord with your legislative intent, if RT4 is reading it correctly. RT4 recommends limiting the exemption to data in that business unit or data derived from it, similarly to the HIPAA exemptions.
2. The present bill attempts to provide a data-level (that is, *not* entity-level) exemption within entities processing HIPAA data. This is difficult to do, and the approach is not perfect. However, RT4, in principle, supports the attempt embodied in the current draft wording. This wording seems to make it impossible for an entity to exempt unrelated activities merely through the acquisition or founding of a small healthcare branch of the business as an end run around LD 1973.
3. FCRA entity-level exemptions would render the law largely useless, and we are grateful that the present wording does not *prima facie* produce such an entity-level exemption. However, the wording is overbroad, and includes data types that RT4 is concerned may disproportionately impact the exercise of constitutionally protected activities or the treatment of constitutionally protected classes. These include broad categories like “mode of living,” “character,” etc. RT4 recommends making the types of data and the threshold level of importance (e.g. as percentage of revenue) of data transfers to FCRA-covered entities, required for an exemption, to be clarified in the wording.

The reason we say FCRA exemptions are the most dangerous to the enforceability of the legislation is precisely because of the broadness of the notion of credit reporting-relevant data. Whereas to exploit the GLBA entity-level exemption, a company not involved in financial services would need to go to considerable expense (even if 1% or less of its net value) to acquire or develop a financial services branch, with FCRA this is not necessary.

Data brokers are companies in the US that concentrate on collecting, aggregating, and selling personal information about individuals from a variety of sources, often without their consent. Their role typically involves packaging collected data to sell to other businesses or the government, a common method the federal government uses to avoid the evidentiary and warrant requirements of the Fourth Amendment. Most individuals are unaware of the information collected, purchased, or sold, which can present significant harm to the individual. Please consider the Congressional Oversight and Investigations Subcommittee Hearing held in April of this year for more information.

If a company wishes to become exempt under a (hypothetical) FCRA entity-level exemption, it would merely need to annually transfer a nominal amount of personal data about a nominal set of persons, to some data broker. This could cost a company less than $10 per year, and allow any company to avoid being subject to LD 1973 for this low cost, without changing any of their other business practices from the *status quo ante.*

In other words, FCRA or other entity-level exemptions being included in a privacy law can actually create incentives for companies to systematically violate the privacy of their consumers.

For these reasons, RT4 advises and promotes use of data-level exemptions whenever they can be articulated with clear, unambiguous wording. Data-level exemptions are based on the type of data collected or processed, regardless of the type of company handling it. This option creates a level of consistency and clarity that helps eliminate loopholes and uphold legislative intent.

Thank you to the committee for reviewing our submission.

Restore the Fourth
Legislative Analysts:
David M
Christina D

Maine Grocers &
Food Producers
Association
PO Box 5234
Augusta, ME 04332
207.622.4461
info@mgfpa.org

Retail Association of Maine
45 Melville Street, Suite 1
Augusta, ME 04330
Tel: 207.623.1149 | Mobile:
207.240.7377
curtis@retailmaine.org
www.retailmaine.org

December 18, 2023

Senator Anne Carney, Chair
Representative Matthew Moonen, Chair
And Members of the Judiciary Committee

RE: Information Requested Following the December 11, 2023 Work Session on Consumer Privacy Legislation and Topics for Comment.

Dear Senator Carney, Representative Moonen and Members of the Judiciary Committee:

Thank you for the opportunity to provide additional input as the committee considers consumer privacy legislation. As I discussed on mic during the December 11, 2023 Work Session, we feel it is critically important for Maine to enact consumer privacy legislation that is in line with what has been enacted in other states. We are open to some modest changes to things that may be Maine-specific needs. However, we would have significant concerns if Maine ultimately enacts legislation that is out of step with other states. We need a law that is laser-focused on giving consumers and the regulated community alike the ability to predict what is expected and required.

To specifically answer the questions provided by the Committee:

Q. Whether the Legislature should exempt from new state consumer data privacy legislation either the data or the entities (or both) regulated by other federal laws, for example the data or entities regulated under HIPAA or the Gramm-Leach Bliley Act.

A. We think it is important to note that HIPPA and GLBA are different even though they are essentially federal preemptions. Although we are not experts in the details of HIPPA and GLBA, it does seem like HIPPA provides more robust and consistent privacy protections for consumers. These protections are more widely known and understood by consumers. With GLBA, however, it is not clear how this exemption provides consumer privacy protections at the same level that HIPPA does or how it will offer similar protections to consumers as what is being considered with state-level consumer privacy protections.

Kennebec Savings Bank's privacy page explains what information is shared or not, and whether or not a consumer can limit that sharing (https://www.kennebecsavings.bank/privacy-policy). For joint marketing with other financial institutions, they disclose that they do share personal information, but the consumer is unable

to limit that sharing. If the banks are given an entity level exemption, this practice would be allowed to continue. We think the committee should discuss further the ramifications of a GLBA entity-level or data-level exemption, and what that would be like in practice.

Q. Whether the Legislature should exempt small businesses from new state consumer data privacy legislation and, if so, how the legislation should define a "small business"? Should the measure be whether a business has a certain amount of annual gross revenue? Or whether the business collects or processes the personal data of a certain number of Maine consumers per year? What dollar amount of gross revenue or number of Maine consumers would you propose?

A. Yes! There absolutely should be a threshold as this is one of the more complex pieces of legislation we encountered in many years. Burdening small businesses like hair dressers, and candy stores with the costly compliance of this legislation would be devastating to small businesses.

As we have noted before, the Connecticut law is emerging as the de facto state-level privacy legislation, and that legislation defines small business exemptions as less than 100,000 consumers. Delaware veered away from that level, and enacted 50,000 consumers. Tennessee increased this threshold to 175,000 consumers. We prefer 100,000 to keep in line with the majority of other states. The number of consumers is derived more from the type of business, and not population size. Some advocates have tried to make the argument that a smaller population justifies a smaller number of consumers. We disagree. As we stated at the Work Session, a convenience store in Maine likely does the same number of transactions as a convenience store in another state. Their transactions are not tied to population size.

While you could consider some level of sales threshold, consumers may be a more accurate, relevant, and understandable threshold for businesses that may interact with consumers but don't do as many direct sales.

Q. What "data minimization" do you recommend that the Legislature adopt in consumer data privacy legislation?

A. 1977 limits collection, processing, and transferring to provide a product requested by the consumer or maintain a service requested by the consumer. It includes a specific list of allowable uses with no catch all. As examples - It would not allow businesses to do analysis of marketing operations. It would not allow businesses to pay for the targeted ad that someone clicked on. It would not allow businesses to operate.

This concept is important and has been consistent across states in the new legislation passed in 2023. LD 1973 gets this right. LD 1977 would introduce restrictions that would reduce new solutions to consumers that save them time and provide convenience. Innovation on behalf of consumers in the management of their data should not be overly restrictive.

Language like this has been proposed, and we could support this language:
Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

We are comfortable with the concept of data minimization, but the regulations need to be in line with how other states have addressed this issue. The goal of privacy legislation is to bring common sense protections to consumers while also preserving innovations that will serve them well.

Q. Do you believe that the Legislature should repeal the current ISP privacy law (35-A M.R.S. §9301) as part of a new, comprehensive approach to data privacy? Or, do you think the Legislature should retain the ISP Privacy law?

A. At first, the concept of everyone playing by the same rulebook seemed to make sense, but we agree with the Maine AG's office when they emphasized that ISP's are the only entity that knows everything someone does online. They know how long you spend online; what websites are visited; and other data. Consumers pay for access to the internet, and they are the primary on-ramp to everything (social media, e-commerce, gaming, news, etc). So, the rules that apply to them probably should be different.

Responses to the questions posed to EPIC:

1. The definition of "sensitive data" under LD 1977 is much broader than the definition of "sensitive data" in the CTDPA. Can you please provide a brief explanation why the definition in LD 1977 deviates from the definition in the CTDPA: perhaps a paragraph or two explaining why each additional category of data appears in LD 1977 and how characterizing that additional category of data as "sensitive" would benefit consumers? (For reference, please see the bulleted lists of items included in each definition that appear on the first page of the comparison chart posted here https://legislature.maine.gov/doc/10392 - the chart starts on page 12 of the PDF)

A. Nearly every state uses nearly the exact same SPI definition. LD 1977 goes far beyond that and is just not workable.

Here are some examples:
CO:
(24) "SENSITIVE DATA" MEANS:
(a) PERSONAL DATA REVEALING RACIAL OR ETHNIC ORIGIN,
RELIGIOUS BELIEFS, A MENTAL OR PHYSICAL HEALTH CONDITION OR
DIAGNOSIS, SEX LIFE OR SEXUAL ORIENTATION, OR CITIZENSHIP OR
CITIZENSHIP STATUS;
(b) GENETIC OR BIOMETRIC DATA THAT MAY BE PROCESSED FOR THE
PURPOSE OF UNIQUELY IDENTIFYING AN INDIVIDUAL; OR
(c) PERSONAL DATA FROM A KNOWN CHILD.

VA:
"Sensitive data" means a category of personal data that includes:
1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
3. The personal data collected from a known child; or
4. Precise geolocation data.

UT:
(32) (a) "Sensitive data" means:
206 (i) personal data that reveals:
207 (A) an individual's racial or ethnic origin;
208 (B) an individual's religious beliefs;
209 (C) an individual's sexual orientation;
210 (D) an individual's citizenship or immigration status; or
211 (E) information regarding an individual's medical history, mental or physical health
212 condition, or medical treatment or diagnosis by a health care professional;
213 (ii) the processing of genetic personal data or biometric data, if the processing is for the
214 purpose of identifying a specific individual; or
215 (iii) specific geolocation data.

Additionally, LD 1977 expansion of "sensitive data" is not needed given the elements are specifically protected under various federal laws and in some cases, ME law. Adding additional layers of regulation on top of these well understood laws creates conflicting and non-sensical treatment of such data. Additionally, the definition of "sensitive data" in the LD 1973 original draft requires that information to use the higher threshold of opt-in protections.

2. Can you please explain, with examples if possible, the differences in the types of entities considered a "covered entity" under LD 1977 versus a "controller" under the CTPDA as well as the types of entities considered a "service provider" under LD 1977 versus a "processor" under the CTPDA? Can you explain the benefits to consumers from the LD 1977 approach as opposed to the CTDPA approach? Relatedly, why does LD 1977 use a different name to describe these entities?

A. Our understanding is that there are no real differences. Since LD 1977 was somewhat pulled from the federal ADPPA proposal, it brought in those terms which essentially mean the same thing. Retailers would be considered "controllers" in LD 1973, and "covered entity" under LD 1977. We would urge the committee to use the terminology in LD 1973 for consistency with other states.

3. The CTDPA (as amended by Conn. Public Act No. 23-56) exempts air carriers regulated under the Federal Aviation Act of 1958 and the Airline Deregulation Act of 1978 as well as personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in those two federal acts. Can you please briefly explain what types of data / information are protected by the Federal Aviation Act of 1958 and federal Airline Deregulation Act of 1978 and how the industry is and is not allowed to use this information? (Senator Carney is not requesting a detailed summary, just a brief understanding of these laws' data protections would be helpful.)

A. This issue is not relevant to the retail industry. We have no comment.

4. With respect to the question whether general consumer data privacy legislation should exclude entities governed by existing federal privacy laws or instead only the data protected under those laws:

> ***a. GLBA. Sometimes a business, like a car dealership, has both a financial side (covered by GLBA) and a non-financial, marketing side (not covered by GLBA). It is the committee's understanding that***

proposals to exempt from the scope of state consumer privacy legislation the data regulated by the GLBA rather than the entities regulated by the GLBA would ensure that such businesses would be prohibited from using information that would be protected by GLBA on the financial side of the business on the non-financial marketing side of the business where the data is not protected under the GLBA. Is this true?

b. HIPAA. Similarly, if the state legislation includes an exemption for entities regulated by HIPAA, how can the committee ensure that this exception doesn't allow a HIPAA-regulated entity to use consumer data collected on the healthcare side of its business for non-healthcare purposes?

c. Is there any way to address these concerns other than employing data-level exemptions to the state legislation? For example:

Would it be effective for the state legislation to include an exemption for entities governed by the GLBA or HIPAA but only to the extent that they are engaging in activities subject to the GLBA or HIPAA? Or

Would it be effective for the state legislation to define "covered data" in a way that excludes information covered by the GLBA, HIPAA (and FERPA as well as the other laws)? Or

Is there another possible approach?

A. These are good questions to be asking. As noted above, we believe the committee should continue to examine these issues to determine what exemption, if any, is reasonable to include in a comprehensive privacy bill.

5. The CTDPA and other states' general consumer privacy laws exempt from their scope certain defined activities by controllers and processers (see, for example, page 3 of the LD 1973, LD 1977 and CTDPA comparison chart). By contrast, LD 1977 establishes a specific list of allowed purposes for collection, processing and transferring covered data. Why does LD 1977 take this alternative approach and what additional protections do consumers gain as a result of this approach?

A. LD 1977 would be overly prohibitive, restricting any future uses of data in certain areas that could have positive uses for consumers. No other state has restricted uses in this way. See verbiage above about innovation on behalf of consumers.

6. With respect to the private right of action: Please comment on the effectiveness of using the remedies available under the Maine Unfair Trade Practices Act (Title 5, Chapter 10 of the Maine Revised Statutes, described in the bill analysis beginning on the bottom of PDF page 5 of the committee's Oct. 17 meeting materials posted here) as opposed to creating a standalone private right of action in the comprehensive consumer privacy legislation itself.

A. We are opposed to a private right of action, especially as much of the bill hinges on specific timeframes or possible ticky-tack violations that may be easily fixable. These are extremely broad bills regulating in at a level that will significantly impact nearly every ME business. The point is to protect consumers, not to punish well-meaning businesses for whom data use is necessary. PRAs have been shown to be a disproportionate response (E.G IL BIPA lawsuits) and no other state has a comprehensive PRA for privacy.

Although we are not attorneys, our experience with Maine's Unfair Trade Practices Act shows that it is a solid enforcement tool for the State, and we feel would provide adequate protection to Maine consumers.

In closing, we appreciate the Committee's diligent work on this issue. We know this is not an easy task, but we hope that the input and data that we have provided throughout this process has been helpful, and clear in communicating the impacts of various issues to Maine's retailers, grocers and small businesses.

Thank you for the consideration of our input.

Respectfully,

Curtis Picard, President & CEO,
Retail Association of Maine
45 Melville St., Augusta, ME 04330
curtis@retailmaine.org | 207-623-1149

Christine Cummings, Executive Director,
Maine Grocers & Food Producers Association
PO Box 5234, Augusta, ME 04332
christine@mgfpa.org | 207-622-4461

December 17, 2023

The Honorable Anne Carney
Senate Chair of the Committee on Judiciary
c/o Legislative Information Office
100 State House Station
Augusta, ME 04333

The Honorable Matt Moonen
House Chair of the Committee on Judiciary
c/o Legislative Information Office
100 State House Station
Augusta, ME 04333

RE: Response to Invitation to Comment on Data Privacy Legislation

Dear Chair Carney, Chair Moonen, and Members of the Committee on Judiciary,

On behalf of the Securities Industry and Financial Markets Association (SIFMA),[1] we thank you for the opportunity to provide comments on the questions posed by the Maine Committee on the Judiciary regarding data privacy. SIFMA brings together the shared interests of hundreds of securities firms, banks and asset managers located across the country. There are more than 25,400 people employed by the financial services industry, more than 900 financial advisors, and 19 broker-dealers who call Maine home.[2] SIFMA's mission is to support a strong financial services industry, investor opportunity, capital formation, job creation, and economic growth.

SIFMA commends the Committee for its dedication to protecting the privacy of Maine residents and for hosting numerous hearings to listen to stakeholders experiences with complying with existing state comprehensive data privacy laws and how it is important to harmonize any new legislation with existing state and federal laws. Financial institutions have been and remain committed to adhering to specific, effective and reasonable privacy laws and regulations for decades. SIFMA specifically will be responding to questions regarding why it is important to exempt entities regulated by the Gramm Leach Bliley Act (GLBA) and the need for exclusive enforcement authority by the Maine Attorney General.

[1] SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. For more information, visit http://www.sifma.org.

[2] US Department of Labor - Bureau of Economic Analysis

1. **The Legislature Should Exempt Financial Institutions regulated by the Gramm Leach Bliley Act**

SIFMA requests that any comprehensive data privacy bill include an exemption for financial institutions and their affiliates regulated by GLBA, to prevent regulatory conflict and limit consumer confusion. An entity and affiliate level GLBA exemption provides the clearest solution for both regulated entities and consumers.

Enacted in 1999, the GLBA established comprehensive federal law that, among other things, governs financial institutions' privacy and data protection controls, including disclosure of privacy practices to customers, cybersecurity controls, and restrictions on the unauthorized sharing of non-public consumer financial information with significant oversight and enforcement by financial regulators. As a result, financial institutions covered by GLBA already have comprehensive, mature privacy programs in place, thus making required compliance any state law duplicative, conflicting, and confusing for customers. An exemption for GLBA-regulated entities would help to alleviate that confusion.

Because financial institutions are regulated under GLBA, adding conflicting overlapping state law could be very confusing for consumers. An exemption for GLBA-regulated entities would help to alleviate that confusion. Most data collected by financial institutions is subject to GLBA, but there are some categories of information that are not collected pursuant to GLBA, such as prospective customer information and some account beneficiary data. Financial institutions do not generally treat data differently based on how or why they collect it. Once they have data, they generally treat it in the same way as information collected under the GLBA for cybersecurity and data protection purposes as described above. Requiring the information to be dissected into categories governed by different laws would impose a significant burden on financial institutions and would far outweigh any perceived increase in consumer protection.

In addition, consumers are unlikely to know or care which data is collected under GLBA and which is not, but they do know when they are dealing with their financial institution (bank, brokerage firm, investment adviser, etc.). The differences will not matter to consumers, but when the consumer requests to have their data disclosed, corrected, or deleted, the company would have to parse which portions of that data is subject to state law (because it was not collected under GLBA). After the firm determines what data is not exempt from the state law, the consumer may still be told that, for example, that data may not be able to be corrected or deleted due to federal recordkeeping requirements which will apply regardless of whether such data was collected under GLBA. If the law includes an entity-level exemption, there is no confusion for consumers because while all of their data held by a financial institution is exempt from the state law, it is thoroughly protected under federal law.

As such, a financial institution and their affiliates exemption is the best, most comprehensive way to protect Maine consumer's data, as the entities are subject to GLBA and therefore must have the policies and procedures in place to protect such information, as required by federal law. This exemption language would allow the financial services industry to provide consumers with meaningful privacy control in an efficient and effective manner and fully aligned with Federal law.

In total, 13 states have enacted comprehensive consumer data privacy laws aimed at providing consumers with additional rights over their personal information. In fact, Colorado, Connecticut,

Delaware, Florida, Indiana, Iowa, Montana, Tennessee, Texas, Utah and Virginia have exempted entities subject to GLBA and only two states - California and Oregon, only exempt data from their comprehensive data privacy law.

2. **Privacy laws should be enforced by the Attorney General and not by plaintiffs' attorneys through private rights of action.**

We also request that any bill give exclusive enforcement authority to the Maine Attorney General (AG). The Maine AG's office is the most familiar with industry standards and best practices. Consumer protection is a prime duty of the Maine AG, and they are very active in bringing lawsuits and enforcement actions against companies that violate state laws.

The AG's office is also well-suited to work with a business to identify, remedy and monitor issues before imposing a penalty, thus creating incentives for businesses to work collaboratively with the AG for better consumer protection. Private Right of Actions (PRAs) weaken the ability of state agencies to enforce privacy laws because it allows plaintiffs' lawyers to shape state policy through the courts, rather than allowing legislators and regulators to shape balanced policies and protections. Such precedents may stray from the original intent of the law by creating unintended results which will unnecessarily burden all Maine businesses.

In fact, PRAs benefit the plaintiffs' bar to the detriment of consumers, since plaintiffs' attorneys often seek millions of dollars in attorney's fees, while the actual victims may receive vouchers, or recover pennies on the dollar, or nothing at all, and are also bound by the class action settlement with no further legal remedies available to them.[3] If the AG has the sole authority to enforce the case, the office works on behalf of the victims and ensures that the victim is made whole.

Plaintiff's attorneys may also initiate class action lawsuits for minor violations where class members did not experience concrete harm, thus allowing for damages disproportionate to the harm incurred by the consumer. Many times, when faced with lengthy and expensive private litigation, businesses settle because it will cost less than the legal fees incurred to fight a frivolous lawsuit.

In short, while we applaud your work to protect Maine residents' data privacy, we would like to work with the sponsors and the committee to better align the proposal with federal law and existing robust financial services data protection policies and practices before any legislation advances in the process. We appreciate your willingness to consider our concerns. If you have any questions, please contact me, Stephanie Klarer, at sklarer@sifma.org or (212) 313-1211.

Sincerely,

/s/
Stephanie Klarer
Assistant Vice President
State Government Affairs
SIFMA

[3] Ill-suited: rights of action and privacy claims. Institute for Legal Reform. (September 29, 2021) (available at https://instituteforlegalreform.com/research/ill-suited-private-rights-of-action-and-privacy-claims/).

U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

December 18, 2023

The Honorable Anne Carney
Senate Chair
Joint Standing Judiciary Committee
Maine Senate

The Honorable Matt Moonen
House Chair
Joint Standing Judiciary Committee
Maine House of Representatives

Re: LD 1973 and LD 1977

Dear Chairs Carney and Moonen:

The U.S. Chamber of Commerce ("Chamber") appreciates the opportunity to provide comment on LD 1973, the "Maine Consumer Privacy Act," and LD 1977, "the Data Privacy and Protection Act." In today's digital economy, it is critical that individual privacy protections enable continued innovation by which businesses can offer the products and services that consumers enjoy. LD1977 fails to meet these goals and would lead to an unworkable and anti-consumer patchwork of state laws. In addition, we also offer proposed suggestions to improve LD 1973 and proposed language to amend it.

Data privacy laws have a significant impact on small businesses. According to a recent Chamber report, *Empowering Small Business*, **75 percent** of small businesses stated that technology platforms, such as payments apps, digital advertising, and delivery, help them compete with larger companies.[1] **73 percent** of small businesses also say that limiting access to data will harm their business operations.[2] One small business owner of a coffee shop described the problems caused by blocking data usage[3]:

> *This is very unfortunate as it would essentially be another "pandemic" for us.* Not having customer data means that we would go back to the early 1980's where we would market our products to a generic list, which in turn would be extremely costly and not a good customer experience. Having customer data helps us customize our marketing so the end result is more meaningful to the customer.

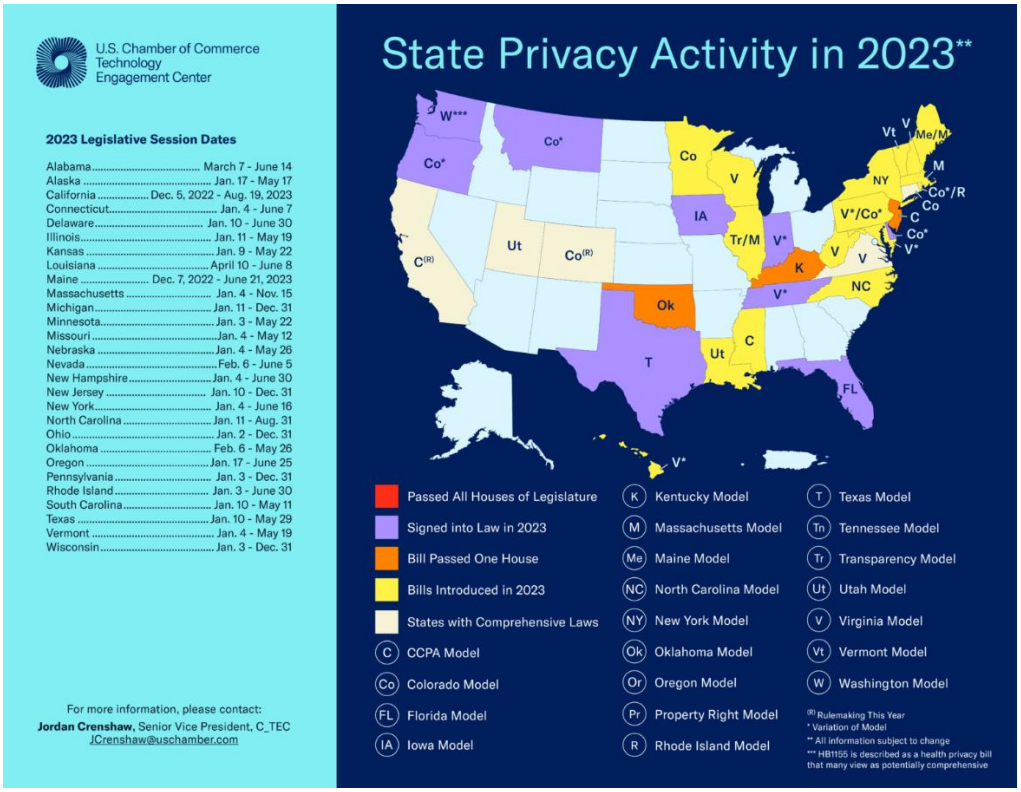
[1] https://americaninnovators.com/wp-content/uploads/2023/09/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf.
[2] *Id*.
[3] https://www.uschamber.com/technology/small-business-owners-credit-technology-platforms-as-a-lifeline-for-their-business (emphasis added).

Consistency, uniformity, and workability are critical to ensuring small businesses are not disproportionately harmed by data protection laws.

I. LD 1977

A. LD 1977 Exacerbates a State Patchwork

LD1977 would significantly harm innovation and lead to an unworkable patchwork of state laws. Thirteen states have passed comprehensive privacy legislation since 2018. Fortunately, twelve of these states, with legislatures controlled by both Democrats and Republicans, such as Virginia, Oregon, Texas, and Colorado have passed similar laws using a "Consensus Framework" that provides strong consumer protections and enables innovation.[4] LD 1977 significantly departs from this Consensus Framework that has emerged across the nation, imposing prohibitions that limit sensitive data collection to what is "strictly necessary," AI risk assessments, and utilizing private rights of action as an enforcement mechanism.



Absent a federal privacy law, it is critically important that states adopt harmonized and uniform standards for privacy. A recent report from ITI highlighted that a national patchwork of privacy laws would cost the United States economy $1 trillion and disproportionately impact small businesses with a $200 billion economic

[4] https://americaninnovators.com/2023-data-privacy/.

burden.[5] As stated in *Empowering Small Business*, a majority of small businesses are concerned that a patchwork of laws will increase both their compliance and litigation costs.[6]

B. LD 1977 Has Conflicting Requirements

Section 9615 requires covered entities to conduct impact assessments of algorithms. These impact assessments would require companies to examine "disparate impact on the basis of an individuals' race, color religion, national origin, sex, or disability status." Section 9605 though, bars the collection or processing of "sensitive data, except when the collection or processing is strictly necessary to provide or maintain a specific product or service..." Under LD 1977, race, color, ethnicity, and religion are considered "sensitive data." Given then definition of "sensitive data," covered entities could be faced with the choice of violating the bill to either comply with the bill's data minimization or impact assessment requirements.

C. Private Rights of Action

Maine should harmonize its legislation with the thirteen other states that have rejected private rights of action for privacy violations. Privacy legislation should be enforced by state attorneys general and not empower the private trial bar at the expense of business innovation and viability. Frivolous, non-harm-based litigation, in particular, has been used in the past to extract costly settlements from companies, even small businesses, based on privacy law provisions granting a private right of action. Private rights of action are ill-suited in privacy laws because:[7]

- Private rights of action undermine appropriate agency enforcement and allow plaintiffs' lawyers to set policy nationwide, rather than allowing expert regulators to shape and balance policy and protections. By contrast, statutes enforced exclusively by agencies are appropriately guided by experts in the field who can be expected to understand the complexities of encouraging compliance and innovation while preventing and remediating harms.

- They can also lead to a series of inconsistent and dramatically varied, district-by-district court rulings. Agency enforcement can provide constructive, consistent decisions that shape privacy protections for all

[5] https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/.
[6] *Supra* n. 1.
[7] https://instituteforlegalreform.com/wp-content/uploads/2020/10/Ill-Suited_-_Private_RIghts_of_Action_and_Privacy_Claims_Report.pdf

American consumers and provide structure for companies aiming to align their practices with existing and developing law.

- Combined with the power handed to the plaintiffs' bar in Federal Rule of Civil Procedure 23, private rights of action are routinely abused by plaintiffs' attorneys, leading to grossly expensive litigation and staggeringly high settlements that disproportionally benefit plaintiffs' lawyers rather than individuals whose privacy interests may have been infringed.

- They also hinder innovation and consumer choice by threatening companies with frivolous, excessive, and expensive litigation, particularly if those companies are at the forefront of transformative new technologies.

Private rights of action would be devastating for business because individual judicial district precedent could also create further confusion and conflict.

II. LD 1973

The Chamber recognizes that LD 1973 more closely resembles the bipartisan Consensus Framework that has already passed in twelve states. We have listed below commentary on how proposed changes to LD 1973 would depart from state Consensus Framework and how that could limit innovation and the products and services consumers enjoy.

- **Definition of Sensitive Data.** It has been proposed that the definition of "Sensitive Data" include "Online usage information derived from the consumer's use of a controller's online product or service, including but not limited to web browsing history and search data, content of communication, device and or online identifiers (e.g. MAC address, IP addresses, etc.)." This would significantly impact e-commerce in Maine, as basic internet functionality and advertising would be subject to strict opt-in requirements.

- **Opt-In.** Like the 14-state consensus laws, consumers should have the right to opt-out of targeted advertising, profiling, and data sales. A differing requirement that companies obtain consent before engaging in these types of activities could be harmful to societally beneficial uses of data and small business. **65 percent** of small businesses have stated that losing the ability to conduct targeted advertising would harm their

business.[8] Additionally, an opt-in regime will subject consumers to notice fatigue as was experienced during the implementation of Europe's General Data Protection Regulation.

- **"Strictly Necessary" Data Minimization Standard.** The 14-state consensus approach does not limit data usage and collection to what is "strictly necessary." Such an approach would significantly inhibit innovation as covered entities may have new societally and consumer-friendly business uses for data throughout different times of product and service development.

- **Applicability to Small Business.** All states that have adopted comprehensive privacy legislation have attempted to reduce burdens on small businesses by limiting their laws applicability to covered entities to collect or use the data of a certain number of individuals. As discussed previously, small businesses will bear a disproportionate burden. We suggest that states adopt a threshold like California and Virginia's laws of 100,000 individuals. It is also important to note that even if the smallest businesses are not directly covered by legislation, tools they use to compete would still be subject to state regulations and a patchwork.

- **Automatic Deletion.** LD 1973 would require companies to delete data used for targeted advertising, sales or transfers unless they have obtained consent. Such an automatic deletion requirement is not a provision in the 14-state consensus model that has been adopted. Such a requirement would once again subject consumers to notice fatigue as companies would be required to obtain consent to retain the data previously collected.

- **Industry neutrality.** Every state that has adopted a comprehensive privacy law has recognized the importance of ensuring that the same data is subject to the same protections regardless of where it exists and is processed in the internet ecosystem. Current Maine law does not reflect industry neutrality due to its disparate treatment of internet service providers (ISPs). As introduced, LD 1973 repeals the ISP privacy law and comprehensively applies the same requirements to every industry sector.[9] We support this approach and ask you to align consumer protections in LD 1973 with those in the Consensus Framework.

[8] *Supra* n. 1.
[9] Title 35-A M.R.S. § 9301.

- **Enforcement.** LD 1973 as introduced strikes the right balance by vesting enforcement authority with the Attorney General. For the reasons stated above, we would oppose inclusion of a private right of action. We also believe that in order to encourage collaborative compliance, privacy legislation should provide for a 30-day cure period.

We once again thank you for the opportunity to comment. For the reasons stated above to protect privacy, encourage innovation, and prevent an unworkable state patchwork, we oppose LD 1977 and encourage you to focus on passing LD 1973 and harmonize it with existing state privacy laws.

Sincerely,

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce

Stocco, Janet

From: Hayes, Danna <Danna.Hayes@maine.gov>
Sent: Tuesday, December 19, 2023 1:24 PM
To: Stocco, Janet
Subject: Responses for committee
Attachments: AG Testimony 1973.pdf; Remedies for violations SBS.docx

Hi Janet,
Here are the Office's responses to the questions posed in the last Judiciary Committee work session.

1. **What are options for identifying a violation for purposes of remedies?**

We have looked at a handful of other state privacy laws (and the federal bill) as models and determined that most broadly authorize the Attorney General to bring an action when there is a violation of any of the substantive requirements or prohibitions. The Oregon Consumer Privacy Act is unique in authorizing the Attorney General to seek a specific civil penalty of $7,500 for each violation. But again, what constitutes a single violation is not defined (e.g. each day the company fails to do something versus the first time). Without such specificity, the law would rely on the interpretation of the enforcer in the first instance, and ultimately a court to determine what is reasonable and intended. This is similar to Maine's Unfair Trade Practices Act which, in both sections 209 and 213, broadly refers to a "a method, act or practice declared unlawful " or a "violation". Since this is such a rapidly evolving area, and we have no basis in Maine to anticipate the landscape, the Attorney General is in favor of broad language similar to that found in other states. A comparison chart showing multiple states' remedy for violations provisions is attached. Alternatively, if the Committee is inclined to endorse something more granular as to what constitutes a violation, we would need more time to research reasonable and viable options.

2. **What is the AG's position relative to the repeal of the ISP law?**

The Attorney General is opposed to the repeal of the ISP law (35-A M.R.S. sec. 9301), consistent with the attached testimony. Because ISPs are essentially the onramps to the Internet, they are in a unique position to collect vast amounts of information regarding their customers' online activity. Recognizing that position, the Maine Legislature wisely enacted the ISP law with very strong protections for consumers online information. In addition to justifying the existing protections, the unique position of ISPs also complicates the applicability of those protections to the rest of the online world. While the Attorney General is willing to take a close look at the transferability of some of those safeguards into a comprehensive privacy bill, it is not a straightforward exercise because of the uniqueness of ISPs, and our primary goal with regard to ISPs is to preserve the existing protections of Maine's ISP law.

Thanks,
Danna

DANNA HAYES, J.D. | SPECIAL ASSISTANT TO THE AG
OFFICE OF THE MAINE ATTORNEY GENERAL
6 STATE HOUSE STATION | AUGUSTA, ME 04333
(207) 626-8887 (DIRECT DIAL) | (207) 626-8800 (MAIN OFFICE)
danna.hayes@maine.gov | www.maine.gov/ag

AARON M. FREY
ATTORNEY GENERAL

TEL: (207) 626-8800
TTY USERS CALL MAINE RELAY 711

STATE OF MAINE
OFFICE OF THE ATTORNEY GENERAL
6 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0006

REGIONAL OFFICES
84 HARLOW ST. 2ND FLOOR
BANGOR, MAINE 04401
TEL: (207) 941-3070
FAX: (207) 941-3075

125 PRESUMPSCOT ST., SUITE 26
PORTLAND, MAINE 04103
TEL: (207) 822-0260
FAX: (207) 822-0259

14 ACCESS HIGHWAY, STE. 1
CARIBOU, MAINE 04736
TEL: (207) 496-3792
FAX: (207) 496-3291

Testimony in Opposition to L.D. 1973, *An Act to Enact the Maine Consumer Privacy Act*

Senator Carney, Representative Moonen, and distinguished members of the Judiciary Committee, my name is Aaron Frey, and I have the privilege of serving as Maine's Attorney General. I am here today to speak in opposition to L.D. 1973, which would roll back significant privacy protections enacted by the 129th Legislature and successfully defended in federal court by my office.

In 2019, the Legislature enacted L.D. 946, "An Act to Protect the Privacy of Online Customer Information," codified at 35-A M.R.S. § 9301. This first in the nation law restricted the extent to which Internet Service Providers ("ISPs") may use, disclose, or sell their customers' personal information, such as their web browsing history, their location, the content of their communications, and their financial and health information. As the Federal Trade Commission recognized, because ISPs are essentially the onramps to the Internet, they can collect vast amounts of information regarding their customers' online activity. Maine's Legislature protected Maine residents by restricting the disclosure of what is likely some of their most private and personal information. The nation's largest telecommunication providers promptly sued the State, and my office vigorously litigated the case for two years. After we achieved initial victories in court, the industry chose to drop their lawsuit. The 2019 law remains in effect and continues to protect the private information of Maine consumers.

Late last week, L.D. 1973 was printed. It is a lengthy and complicated bill, and my office has not had time to thoroughly review it. One thing that stands out, though, is that it would repeal the 2019 ISP privacy law. That would be a mistake. The Legislature was wise in safeguarding Mainers' online information, and it should not now retreat from its zealous protection of our residents' privacy.

Moreover, based on the limited review we were able to undertake between the printing of L.D. 1973 and this hearing, we have concerns:

- The bill applies only to businesses that either control or process the personal data of at least 100,000 consumers or control or process the personal data of at least 25,000 consumers and derive more than 25 percent of their gross revenue from the sale of personal data. This means that many, if not most, businesses in Maine will not be subject to the law.

- The bill has 21 other categorical exemptions. While some of these exemptions may make sense, we are concerned that others may be inappropriate. The exemptions could also make the law vulnerable to constitutional challenge.
- The bill allows a controller to sell a consumer's personal data to an "affiliate" of the controller, thus creating what could be a significant loophole.
- The definition of "targeted advertising" is too narrow. For example, it exempts advertisements "based on activities within a controller's own publicly accessible websites or online applications."
- By authorizing "loyalty and rewards programs," the bill appears to permit controllers to essentially offer financial incentives to consumers to waive privacy rights, thus creating class-based differences where only the more affluent can afford full protection.
- The bill seems to permit controllers and processors to disclose personal information in order to comply with laws of another state, creating the possibility that actions taken in other states could undermine the privacy protections of Maine residents.
- The bill precludes the Attorney General from promulgating interpretative rules. Given the complexity of the bill, rules clarifying certain provisions could be useful, and it is not clear why the Attorney General should be prohibited from that.
- While L.D. 1973 declares that violations constitute violations of the Maine Unfair Trade Practices Act ("MUTPA"), it states that only the Attorney General may bring enforcement actions. The MUTPA generally authorizes actions by both the Attorney General and consumers, and it is not clear why this bill would exclude private enforcement. The availability of a private cause of action is important because it allows for enforcement even when my office might not have the necessary resources, and the potential for private enforcement has a significant deterrent effect.
- The Attorney General must give a controller a "right to cure" a violation and cannot bring an enforcement action if the controller ceases the violation within 30 days. This undermines the bill's deterrence, since controllers know that they can violate the law with impunity so long as if they are caught, they stop the violation.

At a time when our privacy is increasingly under attack, now is not the time to roll back hard-fought gains. While there may be worthwhile elements of this complex bill, it warrants a thorough vetting by all interested stakeholders that may not be possible this late in the legislative session. I urge the Committee to vote ought not to pass.

Comparison of LD 1973, LD 1977 and Others as to Remedies for Violations

LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
❖ **Attorney General** may bring action under Unfair Trade Practices Act (UTPA) against a controller or processer: • Must first provide notice of violation and **30-day right to cure**; may not initiate action if controller or processor asserts in writing the alleged violations have been cured and no future violations will occur	❖ **CT Attorney General** may bring action under CT Unfair Trade Practices Act to enforce the provisions of the CTDPA • Before Dec. 31, 2024: must first provide notice and a **60-day right to cure**; if controller fails to cure the violation in that time, AG may bring an action • Beginning Jan. 1, 2025: AG has **discretion** whether to give controller or processor an **opportunity to cure**, depending on: number of violations; size and complexity of defendant and nature of its processing activities; likelihood of injury to public, safety of persons or property; whether violation was caused by human or technical error; and sensitivity of the data	❖ **Attorney General, DA or Municipal Counsel** may bring an action on behalf of Maine residents against a covered entity or service provider for: • Injunctive relief to enforce compliance with law/rules • Damages, civil penalties, restitution or other compensation; and • Reasonable attorney's fees and litigation costs ❖ **Private action** by individual injured by violation of law/rules against entity committing violation (**except small business**) for: • At least a $5,000 civil penalty per individual, per violation or actual damages, whichever is greater • Punitive damages (no limit/amount stated) • Injunctive and declaratory relief • Reasonable attorney's fees and litigation costs ❖ Pre-dispute **arbitration agreements** are unenforceable
Oregon Consumer Privacy Act (Senate Bill 619)	**Colorado Privacy Act**	**Illinois Data Privacy and Protection Act**
❖ **Section 9(4)(a)** The Attorney General may bring an action to seek a civil penalty of not more than $7,500 for each violation of sections 1 to 9 of this 2023 Act or to enjoin a violation or obtain other equitable relief. [sections 1-9 impose various requirements and prohibitions, e.g. notices, consumer info, data security]	❖ **6-1-105** **6-1-105. Unfair or deceptive trade practices.** (1) A person engages in a deceptive trade practice when, in the course of the person's business, vocation, or occupation, the person: (nnn) VIOLATES ANY PROVISION OF PART 13 OF THIS ARTICLE 1 AS SPECIFIED IN SECTION 6-1-1311 (1)(c). ❖ **6-1-110**	❖ **AG or municipal enforcement (Sec. 75)** may bring a civil action in the name of the State, or as parens patriae on behalf of the residents of the State, against any covered entity or service provider that violated this Act to:(1) enjoin such act or practice;(2) enforce compliance with this Act or such regulation;(3) obtain damages, civil penalties, restitution, or other compensation on behalf of the residents of such State; or(4) obtain reasonable attorneys' fees and otherlitigation costs reasonably incurred. ❖ **Enforcement by persons (Sec. 80)** (a) Any person or class of persons subject to a violation of this Act or a regulation promulgated under this Act by a covered entity or service provider may bring a civil actionagainst such entity in any court of competent jurisdiction. (b) In a civil action brought under paragraph (a) in which a plaintiff prevails, the court may award the plaintiff: (1) an amount equal to the sum of any compensatory, liquidated, or

Comparison of LD 1973, LD 1977 and Others as to Remedies for Violations

	6-1-110. Restraining orders - injunctions - assurances of discontinuance. (1) Whenever the attorney general or a district attorney has cause to believe that a person has engaged in or is engaging in any deceptive trade practice listed in section 6-1-105 or part 7 OR 13 of this ~~article~~ ARTICLE 1, the attorney general or district attorney may apply for and obtain, in an action in the appropriate district court of this state, a temporary restraining order or injunction, or both, pursuant to the Colorado rules of civil procedure, prohibiting ~~such~~ THE person from continuing ~~such~~ THE practices, or engaging therein, or doing any act in furtherance thereof. The court may make such orders or judgments as may be necessary to prevent the use or employment by ~~such~~ THE person of any such deceptive trade practice or ~~which~~ THAT may be necessary to completely compensate or restore to the original position of any person injured by means of any such practice or to prevent any unjust enrichment by any person through the use or employment of any deceptive trade practice.	punitive damages; (2) injunctive relief; (3) declaratory relief; and (4) reasonable attorney's fees and litigation costs. (c) This Section shall not apply to any claim against a small business.
American Data Privacy and Protection Act (ADPPA) [federal bill - not enacted]	**Delaware Personal Data Privacy Act**	
❖ **SEC. 402. ENFORCEMENT BY STATES.** (a) CIVIL ACTION.—In any case in which the attorney general or State Privacy Authority of a State has reason to believe that an interest of the residents of that State has been, may be, or is adversely affected by a violation of this Act or a regulation promulgated under this Act by a covered entity or service provider, the attorney general or State Privacy Authority may bring a civil action in the name of the State, or as parens patriae on behalf of the residents of the State. Any such action shall be brought exclusively in an appropriate Federal district court of the United States to— (1) enjoin such act or practice; (2) enforce compliance with this Act or such regulation; (3) obtain damages, civil penalties, restitution, or other compensation on behalf of the residents of such State; or	❖ **Sec. 12D-111 Enforcement** (e) A violation of this chapter shall be deemed an unlawful practice under § 2513 of Chapter 25 of this title [Prohibted Trade Practices] and a violation of Subchapter II of Chapter 25 of this title, and shall be enforced solely by the Department of Justice [Attorney General].	❖

(4) obtain reasonable attorneys' fees and other litigation costs reasonably incurred. **SEC. 403. ENFORCEMENT BY PERSONS.** (a) ENFORCEMENT BY PERSONS.— (1) IN GENERAL.—Beginning on the date that is 2 years after the date on which this Act takes effect, any person or class of persons for a violation of this Act or a regulation promulgated under this Act by a covered entity or service provider may bring a civil action against such entity in any Federal court of competent jurisdiction. (2) RELIEF.—In a civil action brought under paragraph (1) in which a plaintiff prevails, the court may award the plaintiff— (A) an amount equal to the sum of any compensatory damages; (B) injunctive relief; (C) declaratory relief; and (D) reasonable attorney's fees and litigation costs.		

December 19, 2023

To: Members, Committee on the Judiciary

From: David R. Clough – Maine State Director

Re: Data Privacy Legislation

These comments are on behalf of small business owners who are members of NFIB and would be affected by decisions made on the data privacy issue. By way of background, NFIB has thousands of small business owners in Maine who are members. Our members can be found in 185 legislative districts and are typically very small enterprises, with the average member being smaller than the size of a legislative committee, but the membership also includes small businesses that employ dozens of people in Maine.

Small business owners care deeply about the privacy of their customers as well as their own personal privacy as consumers. We urge committee members to be mindful that the vast majority of small businesses in Maine have limited resources and would find it extremely difficult to comply with complicated privacy mandates. Unlike large businesses, small business owners do not have a compliance department or team of attorneys to help them deal with complicated new laws and regulations. Most owners handle new paperwork and compliance burdens themselves.

Our comments today are limited to the question of a small business exemption and threshold for such an exemption.

Exemption – Yes, there should be a small business exemption.

Threshold – We do not have an exact numerical threshold in mind but urge committee members to think in terms of level of revenue derived from selling person data and level of personal data processed.

Consumer – The most commonly used metric in state data privacy laws is the processing of personal data of 100,000 or more consumers during a calendar year.

Sales – States typically set a threshold of at least 50% for the level of revenue derived from selling personal data.

Customers – States also typically set a threshold of at least 25,000 customers.

Again, we urge committee members to be mindful that small businesses can be disproportionately affected by laws and regulations due to the constraints inherent to the entity (sometimes referred to as “mom and pop” businesses).