Joint Standing Committee on Judiciary

MEETING AGENDA
Tuesday, October 17, 2023
Maine State House, Room 438 (JUD Committee Room)
The meeting will be livestreamed at the following link: https://legislature.maine.gov/Audio/#438

10:00 a.m. **Public Hearing**

LD 1977, An Act to Create the Data Privacy and Protection Act (Rep. O'Neil)

11:00 a.m. **Work Session**

LD 1705, An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data (Rep. O'Neil)
LD 1902, An Act to Protect Personal Health Data (Rep. O'Neil)
LD 1973, An Act to Enact the Maine Consumer Privacy Act (Sen. Keim)
LD 1977, An Act to Create the Data Privacy and Protection Act (Rep. O'Neil)

- **Information from Legislative Analyst**
- **Updates from bill sponsors**
- **Comments from organizations that registered to speak on the following questions**:

(1) What are the benefits and drawbacks of including a private right of action in consumer data privacy legislation?

(2) Should the Legislature enact standalone bills addressing biometric identifiers and health data in addition to enacting a comprehensive data privacy bill or should the Legislature address all types of consumer personal data in a single bill? Why?

(3) How does the choice between an opt-in or an opt-out model for consumer consent to the collection, sharing and sale of personal data impact consumers?

(4) Are there particular approaches to consumer data privacy in other states that you consider particularly valuable or problematic?

(5) What existing federal laws protect consumer personal data in your industry (or the industry of concern to you) – what types of data do those laws protect (or not protect) and what types of companies do they regulate (or not regulate)?

(6) Are there any pending Congressional proposals regarding consumer data privacy of which the Maine Legislature should be aware?

Please see list of registered commenters on the back of the page

After WS **Discussion of Next Steps**

- Next Meeting: Wed. Nov. 8th at 10:00 a.m. (privacy bills work session)
- Additional Work Sessions on privacy bills?
  - First: Tues. Nov. 28th or Wed. Nov. 29th
  - Second: Mon. Dec. 11th or Fri. Dec. 15th
- Potential meeting about tribal issues?
  - Tentative Date: Tues. Dec. 12th

Joint Standing Committee on Judiciary

Organizations that Registered to Comment during the Work Session on LD 1705, LD 1902, LD 1973 and LD 1977

ACLU of Maine	**Meagan Sway,** Policy Director	In person
Anthem	**Diane Johanson**	In person
AvaMed	**Roxy Kozyckyj,** Director, State Government and Regional Affairs	Via Zoom
Cato Institute	**Jennifer Huddleston,** Technology Policy Research Fellow	Via Zoom
Computer & Communications Industry Association	**Alexander Spyropoulos,** Regional State Policy Manager – Northeast	Via Zoom
Charter Communications	**Scott Cowperthwait,** VP - Privacy & Cybersecurity	In person
Consumer Reports	**Matt Schwartz**, Policy Analyst	Via Zoom
Electronic Privacy Information Center	**Caitriona Fitzgerald,** Deputy Director	Via Zoom
Findhelp	**Toby Landau,** Regional Director, Government Relations	Via Zoom
Hospitality Maine	**Nate Cloutier,** Director of Government Affairs	Via Zoom
L.L. Bean	**Christiana van Voorhees,** Senior Associate Counsel	In person
Maine Auto Dealers Association	**Anne E. Sedlack**	In person
Maine Bankers Association	**Josh Steirman**, Director of Government Relations **Andy Grover**, Executive VP, Bangor Savings Bank **Craig Garofalo**, Executive VP, Kennebec Sav. Bank	In person
Maine Broadband Coalition	**Myles Smith**, Executive Director	In person
Maine Credit Union League	**Ellen Parent**, Director of Compliance	In person
Maine Hospital Association	**Jeff Austin,** VP Government Affairs and Communications	Possibly Zoom
MaineHealth	**Sarah Calder**, Senior Government Affairs Director	In person
Maine State Chamber of Commerce	**Ashley Luszczki**, Government Relations Specialist	In person
National Retail Federation	**Paul Martino**, VP and Senior Policy Council	Via Zoom
Office of the Attorney General	**Brendan O'Neil**, Assistant Attorney General	In person
Planned Parenthood of Northern New England	**Lisa Margulies**, VP of Public Affairs, Maine	Via Zoom
Retail Association of Maine	**Curtis Picard**, President & CEO	In person
State Privacy and Security Coalition	**Andrew Kingman**	In person
Technet	**Christopher Gilrein**, Executive Director Massachusetts and the Northeast	In person
Wex Inc.	**Katie Hawkins**, Legal Director of Regulatory Affairs	In person

Maine State Legislature
OFFICE OF POLICY AND LEGAL ANALYSIS
www.mainelegislature.gov/opla
13 State House Station, Augusta, Maine 04333-0013
(207) 287-1670

BILL ANALYSIS

TO: Joint Standing Committee on Judiciary

FROM: Janet Stocco, Legislative Analyst

DATE: October 17, 2023

RE: LD 1705, An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data (Rep. O'Neil)

LD 1902, An Act to Protect Personal Health Data (Rep. O'Neil)

LD 1973, An Act to Enact the Maine Consumer Privacy Act (Sen. Keim)

LD 1977, An Act to Create the Data Privacy and Protection Act (Rep. O'Neil)

SUMMARIES

LD 1705 – Biometric Identifiers – *effective January 1, 2025.*

LD 1705 proposes to regulate the collection and use by private entities of "biometric identifiers" (BIs)—information generated by measuring an individual's unique biological characteristics that can be used to identify the individual such as fingerprints or iris scans.

LD 1705 would generally require private entities:
- To obtain written or electronic consent before collecting, purchasing, receiving, storing, using, or sharing BIs;
- To provide specific information for free, on request, about the BIs it possesses for the requesting individual;
- To adhere to a publicly available BI-retention and destruction policy requiring destruction of BIs one year after a individual's interaction with the entity and within 30 days of an individuals' deletion request; and
- To store and transmit BIs consistent with the industry standard of care in a way that prevents their disclosure.

LD 1705 also proposes generally to prohibit private entities and the entities they contract with (processors) from:
- Selling, leasing or trading BIs; and
- Discriminating against customers who do not consent to the collection of their BIs.

Remedies: Either an individual or the Attorney General may bring a civil action against a private entity for violations of the bill to recover either actual damages or specified civil penalties as well as reasonable attorney's fees, court costs and equitable relief. A violation is also prima facie evidence a violation of the Maine UTPA.

LD 1902 – "My Health My Data Act" – *regular effective date*

State and federal laws currently protect the privacy of health data *held by health plans, health care providers and their business associates*. LD 1902 proposes to regulate the collection, use and disclosure *by private entities* of "consumer health data" (CHD)—including biometric data.

LD 1902 would generally require a private entity:
- To obtain separate written or electronic consent for collection and for sharing of CHD, unless collection or sharing is necessary to provide a product or service requested by the consumer;

- To confirm its collection or sharing of CHD on request and to comply with both a consumer's withdrawal of consent for the private entity to collect or share CHD and the consumer's request to delete their CHD;
- To adhere to a CHD privacy policy made available on its webpage and establish and adhere to a data retention and destruction policy; and
- To adopt and follow security practices that limit access to CHD consistent with the industry standard of care.

LD 1902 also proposes generally to prohibit:
- Any person from selling CHD;
- Any person from creating a geofence to identify, target or track a health care facility's customers; and
- A regulated entity from discriminating against customers who do not consent to collection or sharing of CHD.

Remedies: Identical to LD 1902.

LD 1973 – Maine Consumer Privacy Act – *regular effective date*

LD 1973 proposes to regulate private entities' collection, use and disclosure of "personal data"—non-public data reasonably linkable to an identified individual, with heightened protections applicable to "sensitive data"—personal data of children under 13 years of age and other, specifically listed types of data like biometric data. The bill's requirements apply to non-government entities not regulated by other specific federal or state privacy laws and except when the private entities are complying with their legal obligations under other laws or court orders.

LD 1973 would generally require a private entity that operates in Maine:
- To obtain affirmative consent (opt-in) before processing sensitive data for any purpose, processing personal data for targeted advertising or profiling or selling personal data for any purpose; or
- To, for free at least once per year on receipt of a request, provide consumers with access to personal data it processes, correct inaccuracies in that data, delete the data, and provide a portable copy of the data;
- Provide consumers with a privacy notice explaining what it does with personal data and consumer rights; and
- To implement reasonable data security and integrity practices and conduct data protection assessments for its activities involving processing of personal data that poses a heightened risk of harm to consumers.

LD 1973 also proposes generally to prohibit a private entity that operates in Maine from:
- Collecting, processing or transferring personal data unless reasonably necessary and compatible with the purposes disclosed to the consumer
- Collecting or processing personal data of certain minors for targeted advertising purposes;
- Processing personal data in a way that violates state and federal laws prohibiting unlawful discrimination; and
- Discriminating against consumers who exercise their rights, except may offer consumer loyalty programs.

Remedies: The Attorney General may bring an action under the Maine Unfair Trade Practices Act (UTPA) to enforce violations after first providing notice of the violation and a 30-day opportunity to cure the violation.

Repeal: The bill also repeals 35 M.R.S. §9301, a 2020 state law generally requiring Internet Service Providers (ISPs) to obtain consent before using, disclosing or selling a Maine customer's personally identifying information.

LD 1977 – Data Privacy and Protection Act – ***effective 180 days after adjournment (or later as specified)***

Like LD 1973, LD 1977 proposes to regulate private entities' collection, use and disclosure of "covered data"—non-public data reasonably linkable to an identified individual, with heightened protections applicable to "sensitive data"—personal data of minors and other, specifically listed types of data like biometric data.

Unlike LD 1973, LD 1977 establishes as a general rule that covered data may only be collected, processed or transferred by private entities for specific allowed purposes, for example, providing requested products or services or to comply with obligations under other state, federal, tribal or local laws. It also does not exempt private entities that are operating under specific federal laws (ex: HIPAA or Gramm-Leach-Bliley) from its purview.

LD 1977 would generally require a covered entity:

- To obtain affirmative consent (opt-in) before transferring sensitive data, including all data of a minor, to an unaffiliated entity (3rd party), or transferring data about an individual's selected video services to a 3rd party;
- To provide individuals the option to conset (opt-out) of targeted advertising and any transfer of non-sensitive covered data to a 3rd party for a purpose that is not on the specific list of generally allowed purposes;
- To, for free at least twice per year on receipt of a request, provide consumers with access to personal data it processed in the past 24 months; information on the sources of that data and the categories of 3rd parties to which it transferred the data and why; correct verified and substantial inaccuracies in that data; request deletion of the data by the covered entity and all transferees; and provide a portable copy of the data;
- To make publicly available a dated privacy policy explaining what it does with covered data and consumer rights and provide affected individuals advance notice of material changes to the privacy policy;
- To implement reasonable data security practices, prevent and mitigate reasonable risks, train employees with access to covered data, name privacy and security officers and conduct data protection assessments every other year for each of its activities that pose a substantial privacy risk to individuals; and
- Conduct pre-deployment design evaluations and annual impact assessments on certain algorithms it uses.

LD 1973 also proposes generally to prohibit:

- Collecting, processing or transferring *non-sensitive* covered data unless *reasonably necessary* and *sensitive data* unless *strictly necessary* for a generally allowed purpose;
- Collecting or processing sensitive data of adults for targeted advertising; engaging in targeted advertising to persons known to be minors; or processing or transferring SSNs for other than a few limited reasons;
- Discriminating based on race, color, religion, national origin, sex or disability in covered data activities; and
- Retaliating against consumers who exercise their rights, except may offer limited consumer loyalty programs.

Private entity types: The bill is not limited to businesses that operate in Maine or that target Maine residents. Fewer requirements apply to businesses that meet the bill's definition of a "small business" while additional requirements apply to businesses that meet the bill's definition of a "covered high-impact social media company," "data broker" or "large data holder."

Remedies: The Attorney General, a district attorney or a municipal attorney may bring a civil action for violations of the bill to recover injunctive relief, obtain damages, civil penalties (not specified in amount), restitution or other compensation on behalf of Maine residents as well as reasonable attorney's fees and litigation costs. An individual (not just Maine resident) may bring an action for violations involving the individual's covered data to recover damages of a least $5,000 per violation, punitive damages, injunctive and declaratory relief and reasonable attorney's fees and litigation costs. In addition, pre-dispute arbitration agreements are unenforceable.

ADDITIONAL INFORMATION

1. **Appendices:**
   a) Detailed comparison of LD 1705 (biometric identifiers, BIs) and LD 1902 (consumer health data, CHD)
   b) Detailed comparison of LD 1973 and LD 1977 (general consumer privacy bills).
   c) Other state information on regulation of biometric identifiers and consumer health data. *For other state information on general consumer privacy bills, please pose specific questions for the next WS.*

2. **Maine Unfair Trade Practices Act**: The Maine UTPA prohibits "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce"—certain statutes and rules adopted by the Attorney General declare certain actions to be prima facie violations of the UTPA. Under the UTPA:

   a) The **Attorney General** may bring an action to enjoin a person from violating the UTPA if that action is in the public interest. Any person who violates such an injunction may be ordered to pay a $10,000 civil penalty per violation and to restitution-type relief for individuals harmed by the violation of the injunction. The AG may also seek civil penalties for intentional violations of the UTPA.

b) A **private individual** who purchases goods or services for family or household purposes may bring an action seeking actual damages, restitution, and equitable relief for UTPA violations. Plaintiff must give the defendant 30-days' notice of the action. If defendant offers to settle the case and the final judgment is not more favorable to plaintiff than the offer, plaintiff may not recover attorney's fees and costs.

3. **Competing biometric information definitions**:

LD 1705	LD 1902	LD 1973 and LD 1977
2. Biometric identifier. "Biometric identifier" means information generated by measurements of an individual's unique biological characteristics, including a voiceprint or imagery of the iris, retina, fingerprint, face or hand, that can be used to identify that individual. "Biometric identifier" **does not include**: A. A writing sample or written signature; B. A photograph or video, except for measurable biological characteristics that can be generated or captured from a photograph or video; C. A biological sample used for valid scientific testing or screening; D. Demographic information; E. A tattoo description or a physical description, such as height, weight, hair color or eye color; F. A donated organ, tissue or other body part, blood or serum stored on behalf of a recipient or potential recipient of a living or cadaveric transplant and obtained or stored by a federally designated organ procurement organization; G. Health care information, as defined in Title 22, section 1711-C, subsection 1, paragraph E, obtained for health care, as defined in Title 22, section 1711-C, subsection 1, paragraph C; H. An x-ray, computed tomography, magnetic resonance imaging, positron emission tomography, mammography or other image or film of the human anatomy used to diagnose or treat an illness or other medical condition or to further validate scientific testing or screening; or I. Information collected, used or disclosed for human subject research.	**3. Biometric data.** "Biometric data" means data generated from the measurement or technological processing of an individual's physiological, biological or behavioral characteristics that can be used individually or in combination with other data to identify a consumer. "Biometric data" **includes**, but is not limited to: A. Imagery of the iris, retina, fingerprint, face, hand, palm and vein patterns and voice recordings, from which an identifier template can be extracted; or B. Keystroke patterns or rhythms, gait patterns or rhythms and sleep, health or exercise data that contain identifying information. **Notes:** (1) To be regulated as "consumer health data" under LD 1902, biometric data must**:** • Be information that describes or reveals the physical health, mental health, disability, diagnosis or health condition of a consumer; and • Must relate to the consumer's conditions, diagnoses, treatments, medications, bodily functions, efforts to research or obtain health care services and supplies, gender-affirming care or reproductive or sexual health information. (2) The info. excluded in ¶G & ¶I of the definition of "biometric identifier" in LD 1705 are also excluded from regulation under §1350-X(1) & (3) of LD 1902.	**LD 1973**: • Does not define "biometric data" • Treats "The processing of . . . biometric data for the purpose of uniquely identifying an individual" as "sensitive data." **LD 1977:** **2. Biometric information.** "Biometric information" means covered data generated from the technological processing of an individual's unique biological, physical or physiological characteristics that is linked or reasonably linkable to an individual. "Biometric information" **includes** fingerprints; voice prints; iris or retina scans; facial or hand mapping, geometry or templates; or gait or other unique body movements. "Biometric information" **does not include** a digital or physical photograph; an audio or video recording; or data generated from a digital or physical photograph or an audio or video recording, that cannot be used, alone or in combination with other information, to identify an individual. **Note**: • "Biometric information" is treated as "sensitive data."

ISSUES FOR CONSIDERATION [1]

1. **BI definition**: Are the differences in the definitions of "biometric identifier," "biometric data" and "biometric information" intentional? Is LD 1705 intended to include behavioral BIs (ex: gait), not just physical BIs?

2. **Overlapping Regulation:**

   a) Unlike LD 1905, LD 1705 appears generally designed to regulate BIs held by private entities for non-health-care purposes. However, it may be possible for a private entity to collect BIs for a non-health-related reason, yet those BIs may at some future point qualify as CHD under LD 1902. For example, if an entity uses a retina scan to confirm a customer's identity, it is possible future technology will allow that scan to "reveal" eye diseases?

   b) The general consumer data privacy bills, LD 1973 and LD 1977, regulate a broad category of personally identifying data. Both treat biometric data that can identify a unique individual as "sensitive data" subject to more protections than other personal data, while LD 1977 also treats CHD as "sensitive data" subject to heightened protection. However, the bills differ from LD 1705 and LD 1902 as well as from each other on whether consent is required to collect, process and transfer such data, and under what circumstances.

   Thus, the committee may wish to consider regulating BIs, CHD and other personal data through separate legislation (exempting the narrower categories of data from any omnibus legislation) or regulating all personal data (with different levels of protection for different data) through one omnibus piece of legislation.

3. **Maine connection**: While LD 1902 and LD 1973 are directed only at non-government entities that conduct business in Maine or that target the provisions of goods or services to Maine residents, LD 1705 and LD 1977 are not so limited, raising potential dormant commerce clause concerns.

4. **Other states & complexity:** Representatives from multiple industries highlighted the need for regulatory consistency across states, regarding, for example, consent mechanisms, required privacy policies, definitions of "consent," "sensitive data," "targeted advertising," etc. In addition, several industry representatives emphasized that complex regulatory schemes are anti-competitive in that it is much more difficult for small businesses to comply with complex regulations than large businesses.

5. **Opt-in:**

   a) Industry representatives expressed concern that requiring affirmative consent (opt-in) for collection, processing and transfer of personal data could overwhelm consumers (lead to "consent fatigue") and they urge the committee to follow the opt-out consent model adopted by several other states. They also note that opt-in consent requirements significantly raise the cost of advertising for small businesses. Consumer advocates counter that opt-out mechanisms can be so onerous they are simply unworkable for consumers.

   b) More specific to BIs, industry advocates urge that requiring opt-in for collection and processing of BIs could harm consumers who do not opt in, because BIs provide stronger protection, for financial records and transactions for example, than passwords. By contrast, Representative O'Neil and consumer advocates support an opt-in approach that provides more control for consumers in part because: a person cannot change a BI once it has been divulged in a data breach or stolen by an identity thief; BIs less accurately identify minorities, women, the elderly and children, not only undermining their security of BI-authenticated transactions but also rendering them vulnerable to misidentification; and political protesters, domestic violence survivors and others may wish to limit their vulnerability to tracking using their BIs.

[1] This bill analysis does not attempt to summarize policy arguments presented in testimony related to reasons to vote for or against a bill as written. Instead, this analysis summarizes only those issues that the analyst reasonably believes may lead a committee member to consider proposing an amendment to the bill.

6. **Remedies:**

   a) Industry representatives cautioned against **private rights of action** generally as well as the specific wording of the provisions in LD 1702, LD 1905 and LD 1977 allowing set monetary penalties to accrue for "each violation" or "per violation" of the law. Similar language in the Illinois Biometric Privacy Information Act Law has been interpreted to permit the recovery of liquidated damages each time a company scans or transmits a person's BI without consent, leading to enormous damages awards. Such enormous financial risk can hinder innovation and consumer choice in affected states. By contrast, consumer advocates argue that private rights of action are essential enforcement mechanisms typically employed by consumer protection laws, especially when government agencies lack sufficient resources to bring enforcement actions. Private rights of action, they argue, are the only meaningful mechanisms to deter violations of these laws and to make harmed individuals whole.

   b) Consumer advocates object both generally and to the specific language of the **30-day right to cure** provision in LD 1973, which they interpret as prohibiting the Attorney General from bringing a lawsuit if the defendant promises in writing not to continue violating the law—even if violations of the law continue. Industry advocates argue, by contrast, that cure periods allow industry members that are acting in good faith to correct inadvertent or technical violations, focusing lawsuits on the truly nefarious actors.

7. **Effective date**: Industry advocates recommend delaying the effective date of consumer privacy legislation to afford companies an opportunity to understand the law's provisions and adjust their practices to comply with those provisions. As currently drafted, only LD 1705 provides more than a year delay before it takes effect, although LD 1977 provides a 6-month period for industry to comply with most of its provisions and an additional one to two years for compliance with specific, more burdensome requirements.

8. **Recent legislative history**: Representative O'Neil introduced LD 1945, *An Act to Regulate the Use of Biometric Identifiers*, in the 130th Legislature.

   a) Six members of the Judiciary Committee voted in favor of amending the bill to establish a legislative study comprised of seven legislators to make recommendations for legislation that could be reported out by the Judiciary Committee in the 131st Legislature concerning the collection, storage, use, sale security and destruction of biometric identifiers. The Senate adopted this committee amendment to LD 1945.

   b) Six different members of the Judiciary Committee voted in favor of an amended version of LD 1945 that included both language similar to that set forth in LD 1705 and the legislative study language. The House voted in favor of this committee amendment to LD 1945 and, thus, the bill died in nonconcurrence.

   c) There are several differences between the substantive portion of the latter committee amendment to LD 1945 and LD 1705, including that LD 1705:
      - Exempts from regulation facial surveillance information governed by Title 25, chapter 701;
      - Authorizes an individual to request deletion of the individual's BI through a representative and only requires the deletion of BIs in response to a request that can be verified by the private entity;
      - Includes a new section, §9604, establishing additional requirements for "affirmative written consent";
      - Imposes data-security requirements on processors and not just private entities;
      - Extends the requirement for consent to collect, use or disclose BIs to require consent for storing BIs;
      - Removes language from LD 1945 prohibiting a private entity from "otherwise profiting from" BIs (instead the relevant provision in LD 1705 only prohibits the sale, lease or trade of BIs);
      - Extends the prohibition against providing a different quality of goods or service to an individual who does not consent to collection of a BI to all individuals who exercise their rights under the law;
      - Authorizes any "individual alleging a violation" to bring a civil action against an offending private entity (LD 1945 allowed actions only by an "individual *whose [BI] is the subject of a violation*"); and
      - Removes unallocated language from LD 1945 providing that the bill may not be construed as legislative intent regarding the definition of "personal information" in any other state law.

9. **Applicability Exceptions**: The committee should carefully consider what types of information and what types of entities (or both) that are subject to regulation under other federal or state privacy laws should be exempted from the scope of these bills. Each bill takes a different approach to this issue.

10. **Specific proposed amendments (from testimony)**

a) All bills:

- *Maine State Police*: clarify all entities regulated by these bills must share information with law enforcement pursuant to subpoenas or search warrants validly obtained under federal or state law.

b) LD 1705 (Biometric identifiers)

- *AvaMed*: More clearly exclude information subject to federal laws, federal regulations and state laws governing access to health care information. *See* language proposed in testimony.
- *CCIA:* (a) eliminate the private right of action; (b) add a 30-day right to cure; (c) amend definition of "BIs" to include only data generated by automated measurements of a consumer's biological characteristics and to exclude all photographs or videos without qualification; and to exclude publicly available and de-identified information; (d) amend definition of "personal information" to exclude publicly available and de-identified data; and (e) amend definition of "consent" to include electronic consent (Analyst Note: electronic consent already included). *See* proposed language in testimony.
- *Center for Progress*: (a) clarify the prohibition of discrimination based on failure to allow collection, processing or transfer of BIs, unless use of the BI is "strictly necessary" to the sale of goods or provision of the service. What if the use of BIs makes the service convenient and efficient and less risky to the entity? What if different family members have different choices but one smart device?
- *Maine Credit Union League and Maine Bankers Association*: exempt financial institutions subject to the Gramm-Leach-Bliley Act.
- *Professor Scott Bloomberg (Maine Law):* consider amending the definition of BI to include biometric data—for example, about facial characteristics like smiling, eye movements—even when it is not used to identify a specific individual, as these involuntary movements reveal consumer preferences.

c) LD 1902 (Consumer Health Data)

- *AvaMed*: More clearly exclude information subject to federal laws, federal regulations and state laws governing access to health care information. *See* language proposed in testimony.
- *Anthem & Maine Auto Dealers Association*: Exempt the insurance industry, which is already subject to extensive regulation, from the provisions of the bill.
- *CCIA*: (a) more narrowly define CHD by removing "efforts to research health care services or supplies," information related to "bodily functions" and (within definition of "gender-affirming care services") "products that . . . affirm an individual's gender identity" to avoid situations where data about purchases of feminine care products, toilet paper or undergarments is considered CHD; (b) narrow the definition of "location information" to focus not on whether that data could be used to indicate a consumer's attempt to receive health care services or supplies but instead to focus on whether the company is collecting or processing the data for that purpose—e.g., allow a directions app to collect location information for purposes of providing directions even for patients at a clinic; (c) eliminate private right of action and (d) include at least a 30-day right to cure period.

- *Consumer reports*: define the "discrimination" prohibited when a consumer chooses not to consent to collection or sharing of CHD—*i.e.* denying goods or services, charging different prices and providing a different level or quality of service. *See* language proposed in testimony dated Oct. 11, 2023.
- *EPIC:* Limit the collection of CHD to instances where it is "strictly necessary" to provide a product or service requested by the consumer—*i.e.*, eliminate the option for a consumer to consent to the collection of CHD and strengthen the "necessary" standard for collecting CHD without consent.
- *findhelp:* Broaden the definition of CHD to include "social care information"—which would include that relates to the need for, payment for, or provision of social care including day care, housing, transportation, employment, etc. *See* language proposed in testimony dated Oct. 11, 2023.
- *Maine Bureau of Insurance*: Exempt from the bill CHD covered by the Insurance Information and Privacy Protection Act (Title 24-A, Chapter 24 of the Maine Revised Statutes), which governs the collection, use and disclosure of information gathered in connection with insurance transactions in the State or by insurance organizations of Maine residents and is currently enforced by the bureau.
- *TechNet*: (a) exempt entities subject to regulation by HIPAA, not just the "protected health information" that is subject to regulation by HIPAA; (b) narrow the definition of CHD to exclude information "derived" or "extrapolated" from CHD, which if included could have unintended consequences, (c) define the types of "medication" purchases included in the definition, to avoid situations where data on purchases of toilet paper or feminine hygiene products is considered CHD.

d) LD 1973 (general consumer privacy; Keim)

- *ACLU of Maine, Maine Attorney General and Maine Broadband Coalition*: oppose LD 1973, specifically the provision repealing Maine's ISP privacy law (35-A M.R.S. 9301).
- *CCIA*: (a) limit requirement for opt-in consent to processing or sale of sensitive data, otherwise apply an opt-out consent approach for sale and processing of non-sensitive consumer data; (b) amend the definition of "consent" to remove the affirmative act requirement and not exclude acceptance of terms of use agreement or hovering over, muting, pausing or closing a given piece of content; (c) amend the definition of "processor" to include not just persons but also legal entities that process data on behalf of a controller (*analyst note:* under 1 M.R.S. §72(15) when "person" is used in Maine statute it "may include a body corporate); (d) amend definition of "sale" of personal data to include only sales for monetary consideration not sales for "other valuable consideration"; (e) expand the provisions of §9603(1)(A) and (D), which exempt controllers from confirming that they process personal data or to providing a portable copy of that personal data to consumer's if doing so would reveal a "trade secret" to also exclude instances where the disclosure would reveal "sensitive business information"; and (e) provide a delayed effective date of no earlier than January 1, 2025 to provide businesses with adequate time to comply with the law.
- *Maine Attorney General*: (a) do not limit the bill's applicability to entities that control or process the data of ≥100,000 Maine residents or of ≥ 25,000 Maine residents and derive > 25% of their gross revenue from selling personal data—because most Maine businesses do not reach these thresholds and would be exempt from the bill; (b) narrow the list of categorical exemptions from the bill, some of which may be inappropriate and the inclusion of which render the bill vulnerable to constitutional challenge; (c) do not exempt sale of data to an "affiliate" from the prohibition on selling data without consent; (d) expand the definition of "targeted advertising" to include targeted advertising within the controller's own websites and applications; (e) do not prohibit the AG's office from promulgating interpretive rules; (f) allow private rights of action; (g) do not require 30-day right to cure; (h) do not allow companies to offer financial incentives to disclose data through consumer loyalty programs; and (i) do not allow actions in compliance with other state's laws if they violate this legislation.

- *Multiple industry representatives*: support enactment of LD 1973 if the opt-in consent requirement is amended to require only opt-out consent to match approach of most if not all states with privacy laws.
- *Maine Chamber of Commerce*: supports LD 1973 if the opt-in consent requirement is limited to the processing of sensitive data only.
- *Retail Association of Maine*: (a) due to seasonal sales volumes, use a July 1st rather than a January 1st effective date; (b) delay the effective date by at least 2 years, to allow Maine businesses to comply; and (c) provide reduced regulation for small businesses, for example those that employ less than 50 employees.

e) LD 1977 (general consumer privacy; O'Neil)

- There has been insufficient time to review the testimony from today's public hearing for proposed amendments to LD 1977.

REQUESTS FOR INFORMATION

1. **Maine State Chamber of Commerce:** Examples of how Maine businesses use BIs currently.

2. **Maine Credit Union League:** Available data on security breaches in Maine credit unions caused by guessed passwords (as opposed to use of biometric identifiers to confirm account holder's identity).

3. **Representative O'Neil**: Information on how geofencing works and why LD 1902, which is based on a Washington state law, does not limit the use of consumer health data by government agencies.

4. **Retail Association of Maine:** Source of its assertion that there have been a lot of cases brought against small businesses under the private right of action in the Illinois Biometric Information Privacy Act.

DRAFTING ISSUES

1. Technical drafting issues: Each bill has multiple technical drafting issues, including ambiguous language, internal inconsistencies, and technical violations of state drafting standards. The committee may wish to authorize the analyst to work with the relevant bill sponsor or a specific committee member(s) to work through these issues after a substantive vote to move forward with a bill has been taken**.**

2. More substantive issues

a) LD 1705: (a) Limit applicability to private entities conducting business in Maine?

(b) Clarify when the bill's provisions apply to "processors" and not just private entities?

(c) Amend the definition of "private entity" to more clearly exclude all government actors, including federal government actors, and only when acting in a government capacity?

(d) What info. must a private entity disclose under §9606(2) for the 12 months *before it collects* a BI?

(e) Clarify who has standing to bring a private right of action alleging a violation of the bill's provisions?

b) LD 1902: (a) What is the relationship between "biometric data" as described in the definitions of "consumer health data" and "personal information" in the bill?

(b) Is opt-in consent required for processing CHD, or does opt-in consent for collection cover processing?

(c) What types of discrimination are prohibited by §1350-Q(4) and for exercising what rights?

(d) What are the remedies for the bill's prohibitions against "any person" selling CHD or creating a geofence around a health care facility?

c) LD 1973: (a) Is consent sufficient to permit targeted advertising to minors and sale of minor's personal data and, if so, for what ages of minors?

(b) How must a controller provide the privacy notice to consumers?

(c) What are the difference between "consent" and "opt-in" in the bill? Are these the same? Relatedly, are the opt-in mechanism requirements in §9605(7) applicable to all consents? Even before July 1, 2025?

(d) Is the "reasonably necessary and compatible" standard in §9605(2)(E) clear?

(e) How often must data protection assessments be conducted by controllers? What if the processing changes, must a new data protection assessment be conducted?

★ (f) §9607(3) creates a new public records exception for data protection assessments shared with the Attorney General. If a majority of the committee approves of this new public records exception, a review of the new exception is required under the Freedom of Access Act.

(g) Does §9609(1)(E), as written, allow consumers to waive the requirements of this law via contract?

d) LD 1977: (a) Limit applicability to private entities conducting business in Maine?

(b) What is the relationship between the requirements for "affirmative consent" and "opt out" consent in §9609(5) and §9610(1)?

(c) Is the "reasonably necessary and proportionate" standard in §9604(1) and (2) clear?

(d) What counts as "data previously collected in accordance with this chapter" in §9604(2)(B), given the vastly different types of allowed purposes for collecting, processing and transferring this data?

(e) Under §9604(2)(G) and §9605(3)(B), may a covered entity and service provider comply with court orders, subpoenas and warrants? And may they release location information to law enforcement under all of the exigent circumstance exceptions to the warrant requirement in current 16 M.R.S. §650?

(f) How do the required data policies in §9606 and required data security practices in §9616 relate?

(g) What does the prohibition on unlawful pricing in §9607 mean? Is it limited to the bill's topics?

(h) Does the authority to charge different prices in §9607(3)(E) swallow the anti-retaliation rule?

(i) How and where must a privacy notice be made publicly available?

(j) When may a covered entity transfer non-sensitive covered data of an adult – conflict between §9609(5) and §9619(1) – and for a minor – does §9609(5) prevent transfers for purposes allowed in §9604(2)?

(k) Should §9614(1) be amended to prohibit discrimination on the basis of all MHRA protected classes?

(l) The bill refers to rules but has no rulemaking authority. Is the intent to include rulemaking authority for the Attorney General or a cross-reference to the Maine UTPA (and thus to AG rulemaking authority)?

(m) What amount of civil penalties, in addition to or instead of damages, may the Attorney General, district attorney or municipal counsel recover in an enforcement action?

FISCAL INFORMATION

Not yet determined by OFPR for any of the bills (as of October 16, 2023).

Attachment A: **Detailed comparison of LD 1705 & LD 1902**

	LD 1705 – Biometric Identifiers (BIs)	LD 1902 – Consumer health data (CHD)
Protected Data	❖ **Biometric identifiers (BIs)**- information that can be used to identify an individual generated by measuring the individual's unique biological characteristics—*e.g.*: • a fingerprint, handprint or faceprint • a voiceprint • a retina or iris scan, etc. <u>Excludes:</u> ○ writing sample or signature ○ photo or video (except for characteristics captured from it) ○ biological sample for testing or screening ○ demographic information ○ tattoo or physical description ○ donated blood, organ or body part ○ scan of human anatomy for diagnosis or treatment ○ information for regulated human subject research	❖ **Consumer health data (CHD) –** personal info. (reasonably capable of being linked to a consumer) describing or revealing the consumer's physical or mental health, disability, diagnosis or health condition—including information related to: • health conditions, diagnoses, testing, treatments, medication uses or purchases, symptoms, research of health care services or supplies • "Gender-affirming care information" • "Reproductive or sexual health information" • "Genetic data" or "**biometric data**" related to items listed above • Location information indicating attempt to acquire health care • Info. akin to the above derived by machines from non-health info. <u>Excludes:</u> ○ information in federal, state, local government public records ○ deidentified data ○ information used to engage in regulated human subject research
Covered entities	❖ **Private entity:** individual acting in commercial capacity or a business ❖ **Processor:** private entity that collects, processes, stores or otherwise uses BIs for another private entity <u>Excludes (for both definitions above):</u> ○ State or local government agency or ○ State judicial officer or clerk of court	❖ **Regulated entity:** person that conducts business in Maine or targets Maine consumers <u>and</u> collects, shares, sells or directs processing of CHD <u>Excludes:</u> ○ A government agency ❖ **Service provider** – person that processes CHD for regulated entity
Applicability	❖ **Information <u>not</u> affected:** • "Health care information" "obtained for health care" under 22 M.R.S. §1711-C (state analog to HIPAA) • Health information "subject to" federal HIPAA and its regulations • Personal information collected, processed, sold or disclosed by financial institutions under federal Gramm-Leach-Bliley Act • Facial surveillance data regulated by state Title 25, chapter 701 ❖ **Activities <u>not</u> affected:** • Does not affect admissibility/discoverability of evidence • Consent not required when disclosing BIs for the following reasons: ○ To complete a financial transaction requested by the individual ○ As required by federal or state law, a warrant or a subpoena	❖ **Information <u>not</u> affected:** • Health care information "collected, used or disclosed in accordance with" 22 M.R.S. §1711-C (state analog to HIPAA) • Health information "collected, used or disclosed in accordance with" federal HIPAA and its regulations • Patient identifying info. "collected, used or disclosed in accordance with" federal regulations for substance use disorder patient records ❖ **Activities <u>not</u> affected:** • Information of individuals acting in an employment context

Attachment A: **Detailed comparison of LD 1705 & LD 1902**

	LD 1705 – Biometric Identifiers (BIs)	LD 1902 – Consumer health data (CHD)
Requirements related to protected data	❖ Activities permitted only with individual's **consent (opt-in)** • Collect BI • Purchase/receive/obtain BI • Use BI • Store BI • Transfer/disseminate BI	❖ Activities permitted only (a) with consumer **consent (opt-in) <u>or</u>** (b) if **necessary** to provide a product or service requested by consumer • Collect CHD • Purchase/receive/acquire CHD • Retain CHD • Share CHD (*i.e.,* license or disclose CHD) <u>Exceptions:</u> may share without additional consent (a) to service provider consistent with purpose for collecting CHD; (b) to 3rd party with direct relationship to regulated entity to provide a requested product or service or (b) to a successor in interest
	❖**Prohibited** activities: • Sell/lease/trade BI	❖ **Prohibited** activities: • Sell CHD <u>Exceptions:</u> may sell (a) to service provider consistent with purpose for collecting CHD; (b) to a successor in interest via merger or bankruptcy; (c) individual may sell own CHD
Processor / Service Provider Restrictions	❖ **Processors** may not: • Sell/lease/trade BI • Collect, store, process, use or disclose BIs unless authorized by contract with the private entity	❖ **Service providers** may not: • Process CHD unless authorized by contract with the regulated entity (otherwise it assumes all responsibilities of a regulated entity) • Retain CHD after end of contracted services unless required by law • Fail to assist regulated entity in fulfilling its obligations under the law
Requirements to obtain consent	• Must be written (includes electronic), specific and unambiguous • Consenting individual may not be under duress or undue influence	• Must be written (includes electronic), specific and unambiguous • Must be voluntary & may not be based on material misrepresentations or misleadingly designed user interface
		• Separate consent required for collection & sharing of CHD
	• Must be after having been informed o That a BI is being collected, obtained, stored, etc. and for what purpose and what length of time	• Must be after receiving a request to use CHD that: o Is made through primary means used to offer a product/service o In language in which product or service is provided o Reasonably accessible to consumer with a disability o That clearly describes categories of CHD to be collected, processed or transferred and for what purpose o Explains option to refuse consent, which must be as prominent and may not take more steps than granting consent
	• Consent may **<u>not</u>** be: o Based on execution of a general release form or user agreement o If electronic consent – user interface may not influence toward consent and not giving consent must be the default setting	• Consent may **<u>not</u>** be based on: o Acceptance of general terms of use agreement o Hovering over, muting, pausing or closing a piece of content

Attachment A: **Detailed comparison of LD 1705 & LD 1902**

	LD 1705 – Biometric Identifiers (BIs)	LD 1902 – Consumer health data (CHD)
Discrimination prohibited	❖ **Private entities** may not: • Condition sale of goods or service on collection or use of BI – unless strictly necessary to provide the goods or service • Charge different price or give different quality of goods or service to customer who exercises rights (including right not to consent)	❖ **Regulated entities** may not discriminate (not defined) against consumers who choose not to consent to collection or sharing of CHD
Geofence restriction	n/a	**No person** may create geofence around health care facility to (a) ID, (b) track, (c) collect data from or (d) send notices to customers therein.
Required privacy policy	❖ **Private entity** must make written policy available to the public with: • Guidelines for retention/permanent destruction of BIs ❖ **Private entity** must adhere to its written retention/destruction policy o <u>Except</u> may comply with state or federal law, subpoena, court order or warrant in manner that deviates from the policy	❖ **Regulated entity** must post on its homepage a policy disclosing: • Types of CHD collected, why and how it will be used • Sources from which CHD is collected • What CHD is shared & with whom (and give their contact info.) • How long each category of CHD is retained • How consumer can exercise their rights under LD 1902 ❖ **Regulated entity** may not: • Collect, use or share any category of CHD not in its policy • Collect, use or share CHD for any purpose not in its policy • Ask service provider to act in manner inconsistent with its policy
Required disclosure	❖ **Private entity**, on request, must disclose the following for the 12 months prior to BI collection through the date of disclosure: • Types of BIs associated with requester • Personal information related to the BIs • Sources of BIs and personal information linked to the BIs • Uses of BIs and personal information linked to the BIs • Types of 3rd parties to whom BIs were disclosed and types of linked personal information that was disclosed ❖ **Cost**: May not charge for disclosure	❖ **Regulated entity**, on request, must confirm to a consumer: • Whether it collects consumer's CHD and give access to that CHD • Who it shares consumer's CHD with and give contact info. (email) • It has not sold the consumer's CHD ❖ Other information regulated entity must provide in response: • Consumer may withdraw consent for CHD collection or sharing • Consumer has right to have CHD deleted and how to do so ❖ Request mechanics: • consumer may make request at any time • method must be secure and request must be authenticated
Deletion of protected data	❖ **Private Entities** • **By request:** Within 30 days of authenticated request, **private entity**: o Must permanently destroy requestor's BIs	❖ **Regulated entities** • **By request:** Within 30 days (and without unreasonable delay) of receiving authenticated request, **regulated entity** must: o Delete requester's CHD from its records/systems; and o Notify service providers & 3rd-party transferees of request

Attachment A: **Detailed comparison of LD 1705 & LD 1902**

	LD 1705 – Biometric Identifiers (BIs)	LD 1902 – Consumer health data (CHD)
	• **Generally:** must permanently destroy BI at earliest of: o Date initial purpose for obtaining BI is satisfied, o 1-year after last interaction with the individual, or o 30 days after individual's verified request to destroy BI	• **Generally:** must permanently destroy CHD o When deletion of CHD is required by law o When CHD no longer necessary for purpose for which consent was given <u>unless</u> regulated entity is required to retain CHD by law or the consumer consents to retention ❖ **Service providers and 3rd parties** that receive CHD: • Must "honor" deletion requests when notified by regulated entity • Must delete CHD at end of providing service to regulated entity <u>unless</u> required to retain CHD by law
Data Security	❖ **Private entity** and **processor** must: • Store and transmit BIs: o Consistent with industry reasonable standard of care o In as protective as its manner for storing and transmitting other "confidential and sensitive information" (ex: SSNs)	❖ **Regulated entity** shall: • Protect confidentiality and integrity of CHD o Consistent with industry reasonable standard of care applicable to the volume and nature of the information • Restrict access to CHD by employees or others – only allow if strictly necessary to provide product or service customer requested
Special provisions for private entities as employers	❖ **Consent required** — in the form of a release signed by employee as a condition of employment — to use employees' BIs to: • Provide access to secure locations and/or computers • Record start and end of work day and meal or rest breaks ❖ **Prohibited** use of employees' BIs: • Use of BIs for employee tracking ❖ **Policy** governing use of employees' BIs need not be made public	n/a ("consumer" does not include individual in employment context)
Remedies for violations *Identical remedies for these bills*	❖ **Individual or Attorney General may bring a civil action** against a private entity and is entitled to recover: • The larger of: actual damages or civil penalties of ≥ $1,000 per negligent violation or ≥ $5,000 per reckless or intentional violation; • Reasonable attorney's fees and court costs (including expert witness fees); and • Any other relief, including equitable relief. ❖ An action may also be brought under the **Maine Unfair Trade Practices Act (UTPA)**	
Effective Date	**January 1, 2025**	Not specified (90 days after adjournment)

Attachment B: **Detailed comparison of LD 1973 and LD 1977**

	LD 1973 (Keim)	LD 1977 (O'Neil)
Protected Data	❖ **"Personal data":** • Non-public information • Linked or reasonably linkable to an identified individual ❖ "**Sensitive data":** subset of personal data including: • Data revealing race, ethnicity, religion, mental or physical health, sexual orientation, citizenship or immigration status • Processing of biometric or genetic data to uniquely ID a person • Precise geolocation data (within 1,750 feet) • Personal data of a child <13 years of age Exception (both types of data above): • "Consumer" is defined for purposes of the bill to exclude an employee, contractor, etc. interacting with a controller solely in an employment context	❖ "**Covered data**": • Non-public information, including derived data • Linked or reasonably linkable, alone or in combination with other information, to an identifiable individual ❖ "**Sensitive data":** subset of covered data including: • Data revealing race, ethnicity, religion, mental or physical health, disability, diagnosis, sexual behavior, employment history, union membership or family or social relationships • Biometric and genetic information • Location information (within 1,850 feet) • Information of person known to be a minor <18 years of age • Social security, passport or driver's license number • Account or device log-in credentials or access codes • Private communications (email, text, DM, voicemail, mail) and information about the transmission of those communications • Calendar and address book information, phone or text logs, photos, audio recordings, and videos if those are for private use, whether on the individual's device or remotely stored • Photo or video images of naked or undergarment-clad genitals • Information about video content requested by an individual and an individual's online activities over time
Size and Maine connection requirements for regulation	❖ **Law applies to** persons: • Conducting business in Maine or targeting Maine residents • That processed or directed processing of, in last calendar year: o ≥100,000 Maine residents (except payment transactions) **or** o ≥25,000 Maine residents and derived > 25% of gross revenue from the sale of personal data	❖ **Law applicable to** persons that for any of the prior 3 years: • Collect or process data of >75,000 individuals per year (other than solely for purpose of billing for requested product/service) • Have average annual gross revenue >$20,000,000 **or** • Receive any revenue for transferring covered data *Note: no Maine connection required*
Types of covered entities	❖ **Controller:** person that determines purpose and means of processing personal data ❖ **Processor:** person that processes personal data for a controller	❖ **Covered entity**: alone or jointly determines purposes and means of collecting, processing or transferring covered data ❖ **Service provider**: collects, processes or transfers covered data for a covered entity or federal, state, tribal or local government
Exceptions to applicability	❖ **Law not applicable to (types of entities / types of data)**: • State or its political subdivisions or boards or agencies, • Certain tax-exempt organizations • Higher education institutions and data regulated by FERPA	❖ **Law not applicable to:** • Government entities • Service providers that exclusively and solely process information provided by government entities (except as specified below)

Attachment B: **Detailed comparison of LD 1973 and LD 1977**

	LD 1973 (Keim)	LD 1977 (O'Neil)

Note:
for LD 1973, see lists on pp. 4-6 and 12-14
	• Financial institutions or data subject to Gramm-Leach-Bliley Act
	• National securities ass'ns under Securities Exchange Act of 1934
	• Entities and protected health information regulated by HIPAA and intermingled/indistinguishable info. held by those entities
	• Info. that has been de-identified in accordance with HIPAA
	• Info. for public health activities as authorized by HIPAA
	• Identifying info. related to substance-use disorder treatment
	• Identifiable information collected as part of human subject research conducted under federal law or international guidelines
	• Info. collected, processed, sold or disclosed in compliance with:
	  o federal Health Care Quality Improvement Act of 1986
	  o federal Fair Credit Reporting Act
	  o federal Driver's Privacy Protection Act of 1994
	  o federal Farm Credit Act of 1971
	  o federal Airline Deregulation Act of 1978
	• Information of those applying to or employed by a controller, processor or third party or to administer benefits to employees
	• Disclosures that violate an evidentiary privilege under state law
	• Disclosures that violate freedom of speech or press
	
	❖ **Controller / Processor activities <u>not</u> affected by bill**:
	• Complying with federal, state or local laws, investigations, subpoenas or summonses & defending legal claims
	• Providing product or service requested by the consumer, including performing contracted services (ex: warranty)
	• Taking immediate steps to protect an interest essential for the life or physical safety of a consumer or other individual
	• Preventing or responding to security incidents, identity theft, fraud, harassment or illegal activity or report those incidents
	• Engaging in scientific or statistical research that adheres to all other ethics and privacy laws and is overseen by an IRB
	• Assisting another controller or processer with its compliance
	• Process personal data for public health purposes subject to confidentiality obligations of federal or state laws
	• Collection, use or retention of data for internal use, including R&D, product recalls, identifying and repairing technical errors
	• Processing of personal data by person for own household use
		Note: LD 1977 does not similarly include a comprehensive list of activities unaffected by the requirements/prohibitions in the bill.
		
		Instead, it generally limits collection, processing and transferring of covered data to specific allowed purposes listed on pp. 6-7:
		• Complying with obligations under local, state, tribal or federal laws & defending legal claims
		• Completing transaction for a requested product or service
		• Fulfilling a product or service warranty
		• Preventing harm if have a good faith believe individual at risk of death, serious physical injury or other serious health risk
		• Preventing or responding to security incident (network security or physical security, including trespass, medical alert, fire alarm)
		• Preventing or responding to fraud, harassment or illegal activity targeted at or involving the controller or service provider
		• Conducting scientific, historical or statistical research that adheres to all relevant laws and regulations
		• Authenticating users of product or service
		• Carrying out a product recall under state or federal law
		• Delivering non-advertisement communication to an individual that is reasonably anticipated by their interaction with the entity
		• Delivering commination at direction of an individual
		• Ensuring security and integrity of covered data
		• Support individuals' participation in civil engagement, including voting, petitioning, unionizing, providing indigent legal services
		• Transferring assets to successor in interest after notice to affected individuals and reasonable opportunity to withdraw consent or request deletion of covered data
		• **Previously collected data** – distinct purposes allowed, including for targeted advertising (see page 6, lines 5-24)

Attachment B: **Detailed comparison of LD 1973 and LD 1977**

	LD 1973 (Keim)	LD 1977 (O'Neil)
Requirements related to protected data	❖ All collection, processing, transfer and sale of **personal data** must be: • **Reasonably necessary & compatible** with the purpose disclosed to the consumer (unless obtain consent)	❖ All collection, processing and transferring of **covered data** must be: • For an **allowed purpose** (See list above) • **Reasonably necessary & proportionate** to that purpose ❖ All collection or processing of **sensitive data** must be: • **Strictly necessary** to achieve an **allowed purpose** (other than promoting civic engagement)
	❖ Activities permitted **without consent** • Processing (includes collecting, processing and disclosing but not selling) of non-sensitive personal data for any purpose except targeted advertising	❖ Activities permitted **without consent** • Collecting, processing or *transferring to a service provider* any covered data for an allowed purpose (see list above) • Transfer *adult's* covered data to 3rd party for allowed purpose
	❖ Activities permitted only **with consent (opt-in)** • Processing **sensitive data** for **any purpose** • Processing personal data for **targeted advertising** • **Selling** personal data Exceptions: "sale" defined to exclude sharing personal data with (a) processor; (b) 3rd party for purpose of providing requested product or service; (c) affiliate or (d) successor in interest after merger, bankruptcy or other transaction. • Process personal data for "**profiling**"- *i.e.,* "solely automated decisions that produce legal or similarly significant effects"	❖ Activities permitted only **with consent (opt-in)** • Transfer any **covered data of minor** to 3rd party Exception: Cybertip about child victims to NCMEC • Transfer **sensitive data** to a 3rd party Exceptions: may transfer (a) to comply with law; (b) to prevent imminent injury; (c) to a successor in interest; (d) to transfer password to identify reused passwords; (e) to transfer genetic info. for medical diagnosis or treatment • Transfer info on selected **video content or services** to 3rd party Exceptions: same as (a) to (e) above
		❖ Activities permitted only with **choice to opt-out** (*opt-out consent appears to be the intent of §9609(5) and §9610(1))* • **Transfer** non-sensitive covered data to 3rd party for **other than** one of the **allowed purposes** (See list above *but see §9619(1)*) • **Targeted advertising** to person (unless known to be a minor)
	❖ Other **prohibited** activities (regardless of consent): • Collect or process personal data of **minors known to be ages 13-15 for targeted advertising** (*it is not 100% clear from the text of the bill if this activity is intended to be prohibited, even with consent*)	❖ Other **prohibited** activities (regardless of consent) • Process or transfer **SSNs** (except for limited reasons—*e.g.*, for credit extension, authentication, collection or payment of taxes, enforce a contract, prevent fraud/crime or as required by law) • Process **sensitive data** for **targeted advertising** • **Targeted advertising** to person known to be a **minor** (stricter requirements for high-impact social media companies and data holders described below)

Attachment B: **Detailed comparison of LD 1973 and LD 1977**

	LD 1973 (Keim)	LD 1977 (O'Neil)
Processor and Third-party activity restrictions	❖ **Processor:** • May not process personal data beyond directions in contract with controller (otherwise, it assumes the responsibilities of a controller under LD 1973, including being subject to remedies) • May not collect, process or transfer personal data if has knowledge covered entity violated law with respect to that data	❖ **Service Provider** (including those serving only government entities): • May not collect, process or transfer covered data except pursuant to contract with covered entity (otherwise, it assumes all of the responsibilities of a covered entity under LD 1977) • May not assist covered entity with known violation of the law ❖ **Third party** (see definition page 5): • May not process covered data and sensitive data Exceptions: may process: ▪ *Covered data and sensitive data*: (a) to complete a transaction for a requested product or service; (b) to authenticate a user; or (d) to prevent or detect a security incident (intrusion, medical alert, trespass or fire alarm) ▪ *Non-sensitive data*: for purpose disclosed in privacy notice (recall this transfer has an opt-out requirement) ▪ *Sensitive data*: for purpose for which consumer gave opt-in consent to transfer
Requirements for consent	❖ **Consent** requirements: • Written or electronic statement that is specific and unambiguous • Freely given (user interface may not impair decision-making) • By (a) consumer, (b) designated agent, guardian or conservator; or (c) parent or legal guardian of minor < 13 years old	❖ **Consent (opt-in)** requirements: *Note: opt-out consent not defined* • Affirmative act that is specific and unambiguous • Freely given (not based on material misrepresentations and user interface may not be designed to impair decision-making) • By (a) individual or (b) parent or legal guardian of a minor
	• *(Not explicit)* presumably consumer must be informed of the purposes for which personal data is processed (perhaps the privacy notice is sufficient for this purpose?)	• After receiving standalone request from covered entity that: ▪ Is made via primary medium to offer product/service ▪ Is in each covered language (top 10 per US Census) used to sell the product/service ▪ Is reasonably accessible to individuals with disabilities ▪ Clearly explains, with prominent headings, categories of covered data collected, processed or transferred and why ▪ Clearly explains individual's rights related to consent
	• **Mechanism to opt-in:** (a) must be easy to use; (c) may not have opt-in as a default setting and (c) must enable controller to verify the Maine residency of the consumer & legitimacy of opt-in request • **Mechanism to revoke** must be at least as easy as to consent	• **Option to refuse** consent must be as prominent as and may not take more steps than granting consent • **Mechanism to withdraw consent** must be clear and conspicuous and as easy to execute as providing consent

Attachment B: **Detailed comparison of LD 1973 and LD 1977**

	LD 1973 (Keim)	LD 1977 (O'Neil)
	❖ Consent may **not** be based on: • Accepting a terms of use agreement (must be standalone) • Hovering over, muting, pausing or closing a piece of content	❖ Consent may **not** be based on: • Individual's inaction • Individual's mere continued use of service or product
Discrimination and retaliation prohibitions	❖ **Controller** may not process (includes collect and disclose) personal data in manner that violates state and federal laws against discrimination ❖ **Controller** may not discriminate against consumer for exercising a right under this law, including by: • Denying or charging different prices for goods or services • Providing different level or quality of goods or services Exception: • Need not offer product or service w/out **required** personal data • May offer different price, quality or selection of goods or services via a **voluntary consumer loyalty program**	❖ **Covered entity and service provider** may not collect, process or transfer covered data in manner that discriminates based on race, color, religion, national origin, sex or disability Exceptions: (a) self-testing to prevent discrimination; (b) diversifying applicant or customer pool; (c) private clubs not open to the public ❖ **Covered entity** may not retaliate against consumer for exercising a right under this law, including by: • Denying or charging different prices for goods or services • Providing different level or quality of goods or services Exceptions: • Need not offer product or service w/o **strictly necessary** data • May offer different price, quality or selection of goods or services via a **voluntary consumer loyalty program** only if: ▪ Only necessary covered data is transferred to 3rd parties as part of the program, data transfers are disclosed to program members and transferred covered data is not retained for any other purpose by 3rd party. • May condition price or level of service on provision of financial information **for billing purposes** • May offer financial incentives to participate in **marketing studies** (with certain limitations on the top of p. 10)
Consumer / individual rights	❖ A **consumer has a right**, upon making authenticated request, to: • **Confirm** whether controller processes personal data • **Access** data processed by controller • **Correct inaccuracies** in personal data • **Delete** personal data about the consumer • Obtain **portable copy** of own personal data from a controller Exceptions: • Controller need not disclose info that reveals a trade secret • Controller need not disclose de-identified data or data the controller is not reason. capable of associating w/the consumer	❖ A **consumer has a right**, upon making authenticated request, to: • **Download** non-archived covered data collected, processed or transferred by the covered entity within previous **24 months** • Be told categories of **3rd party transferees** of covered data and for what purposes, with an option to request 3rd party names • Be told the **sources** from which covered data was collected • **Correct verified substantial inaccuracies/incomplete info**. with reasonable efforts to notify 3rd parties & service providers • **Delete** covered data with reasonable efforts to notify 3rd parties • If technically feasible, obtain **portable copy** for self or another entity of processed covered data not including derived data

Attachment B: **Detailed comparison of LD 1973 and LD 1977**

	LD 1973 (Keim)	LD 1977 (O'Neil)
	• Controller may retain data deletion request & minimum data necessary to ensure data remains deleted in its system	Exceptions: • The exceptions in LD 1973 all apply (except may protect "privileged & confidential business info." not just trade secrets) • Need not respond if request furthers fraud, criminal activity, a security threat, breach of contract or unfair/deceptive practice • Need not comply if would violate state or federal law or the federal constitutional rights of another individual • Need not comply if action would require access to or correction of another individual's sensitive data • Need not delete data for reasons on p. 15 (described below)
	❖ **Request / appeal process**: • Each consumer generally may make one free request per year • Request process must be secure, reliable and verify requester ID • Controller may charge a reasonable fee or decline to act on technically infeasible, excessive or repetitive requests • Controller must notify consumer of unauthenticated request • Controller must act / decline to act within 45 days of request • Consumer may appeal controller's inaction within a reasonable time and decision (with reasoning) required within 60 days • If appeal denied, must provide mechanism to complain to AG	❖ **Request process**: • Each individual may make two free requests per year • Request process must not be materially misleading or use an interface designed to impair individual's reasonable choice • Covered entity may deny demonstrably impracticable or prohibitively costly requests, with explanation to requester • Covered entity must notify individual of unauthenticated request and request additional info. for verification purposes only • Covered entity must act/decline to act within 60 days of request - may extend once by 60 days if reasonably necessary
Required privacy notice / privacy policy	❖ **Controller** must provide accessible and clear privacy notice of: • Controller's contact information (e-mail or other) • Categories and purposes of personal data it processes • How consumers may exercise their rights • What categories of personal data are shared with what categories of 3rd parties	❖ **Covered entity and service provider** must provide accessible and clear privacy policy in each covered language it uses, stating: • Name and contact info. of covered entity/service provider and entities within corporate structure to which it transfers data • Categories and purposes of covered data it collects or processes • How long it intends to retain each category of covered data • Prominent description of how to exercise individual's rights • What categories of covered data are shared with what categories of 3rd parties and for what purposes • General description of its data security practices • Effective date of the policy ❖ **Material change to privacy policy** – a **covered entity** must, before implementing a new policy for prospectively collected covered data: • Take reasonable measures to notify each affected individual • Provide reasonable opportunity for withdrawal of any consents

Attachment B: **Detailed comparison of LD 1973 and LD 1977**

	LD 1973 (Keim)	LD 1977 (O'Neil)
Deletion of protected data	❖ **By request**: as is explained above, controller must delete protected data within 45 days of authenticated consumer request Exceptions: • may retain data deletion request & minimum data necessary to ensure data remains deleted in its system • may decline a technically infeasible, excessive or repetitive request, subject to the appeal procedures stated above	❖ **By request**, as is explained above, covered entity must delete covered data within 60 days of authenticated consumer request (may extend 1x) Exceptions: need not comply with deletion request that: • unreasonably interferes with providing product/service to another person the covered entity currently serves • requires deletion of data of public figure or official and the requester has no expectation of privacy in that data • involves data necessary to perform contract with requester • involves data that must be retained for professional ethics • involves data reasonably believed to be evidence of unlawful activity or abuse of covered entity's products or services • for private schools, requires deletion of data that would unreasonably interfere with providing education services ❖ **In general**, covered entity and service provider must delete covered data no longer necessary for purpose of collection, processing or transfer Exceptions • If have affirmative consent (opt-in) to retain data • If required to retain data by law
Previously collected data	❖ **Controller** must, by July 1, 2025, delete consumer's personal data that it has for purposes of sale or targeted advertising unless consumer opts-in to the sale or targeted advertising	❖ **Covered entity** may process and transfer previously collected covered data for the specific purposes set forth on p. 6, lines 5-2 (includes targeted advertising, for example)
Data Security (and Data Security Officers)	❖ **Controller** must: • Establish & implement reasonable data security and integrity practices appropriate to the volume and nature of the data • Process covered data of a child <13 years old in accordance with federal Children's Online Privacy Protection Act of 1988	❖ **Covered entity** and **service provider** must • Establish & implement reasonable data security practices to protect against unauthorized access appropriate to volume and nature of the data, size and complexity of entity, sensitivity of the data, current state-of-the art safeguards and costs • Identify and assess internal and external risks to the system • Prevent and mitigate reasonably foreseeable risks/vulnerabilities • Train employees with access to covered data • Implement procedures to detect/respond to security breaches • Designate a **privacy officer** and a **data security officer** ▪ To implement data security policies & ▪ To facilitate compliance with this law

Attachment B: **Detailed comparison of LD 1973 and LD 1977**

	LD 1973 (Keim)	LD 1977 (O'Neil)
Data Protection / Privacy Impact Assessments	❖ **Controller** must: (*timeframe not specified*) • Conduct and document a **data protection assessment(s)**—weighing benefits to controller, consumer and public of processing the data against the risks to consumers specific to • ***Scope:*** All activities presenting a heightened risk to consumers: ▪ Processing personal data for targeted advertising ▪ Sale of personal data ▪ Processing of personal data for profiling that presents a foreseeable risk of unfair treatment of consumers or physical or financial injury to consumers ▪ Processing of sensitive data • Provide copy to AG on request (if relevant to an investigation)	❖ **Covered entity** must, **every other year**: • Conduct written **privacy impact assessment** that is reasonable and appropriate in scope given nature, volume and potential risks to privacy of the data collected, processed or transferred ▪ Weighing benefits of entity's use of data against potential material adverse consequences to individual privacy ▪ Include additional information required by AG • ***Scope***: All activities that may cause a substantial privacy risk (which activities qualify is not further defined) • Make a summary of the assessment publicly accessible • Provide summary of the assessment to AG on request
Algorithm Impact Assessments	n/a	❖ **Covered entity** that uses a **covered algorithm** (defined p.1) "in a manner that poses a consequential risk of harm" must**:** • Conduct **annual impact assessment**—see p. 18-19—including describing steps taken to mitigate: harm to minors; use of algorithm to determine access to or restrictions on housing, education, employment, healthcare, insurance, credit, or public accommodations; and disparate impacts based on race, color, religion, national origin, sex, disability or political party status • Conduct pre-deployment **design evaluation** to reduce harm • Report results of assessments & evals. to AG within 30 days • Make summary of assessments & evaluations publicly available
Processor/ Service Provider duties	❖ **Processor** must: • Assist controller with responding to consumer requests • Assist controller with meeting data-security obligations • Notify controller of any security breach in processor's system • Assist controller with data protection assessments • Act only pursuant to contract with controller that requires it to: ▪ Keep confidential personal data it processes ▪ Delete or return personal data at end of services ▪ Cooperate with or conduct assessments of own services ▪ Require all subcontractors (if any) via written contract to comply with processor's obligations related to personal data	❖ **Service Provider** must (even if only working for government entity): • Assist covered entity with responding to individual requests • Assist covered entity with privacy impact/algorithm assessments • Allow other assessments by covered entity or indep. assessor • Act only pursuant to contract with covered entity detailing: ▪ Types of covered data and instructions and purposes for collecting, processing or transferring that data ▪ Duration of processing ▪ Prohibition on comingling data unless specifically allowed • Not collect, process or transfer data for covered entity if have actual knowledge covered entity violated law w/r/t that data • Delete or return covered data at end of services • Notify covered entity of any subcontractors and require, via written contract, them to comply with all obligations above

Attachment B: **Detailed comparison of LD 1973 and LD 1977**

	LD 1973 (Keim)	LD 1977 (O'Neil)
Third party requirements	n/a	❖ **Third party** may only process data it obtained from covered entity for allowed purposes and/or with required consents outlined above • Covered entity must enter contract with third party that: ▪ Specifies purpose(s) for which covered data may be processed by 3rd party and not permit any other processing ▪ Requires 3rd party to adhere to data security requirements ▪ Requires 3rd party to adhere to this law's requirements
Regulation of de-identified data	❖ **Controller** in possession of **de-identified data** must: • Take reasonable measures to prevent re-identifying the data and publicly commit to not attempting to re-identify the data • Contractually obligate recipients of the data to comply with law and monitor compliance with those contractual commitments	n/a
Special rules for special business types	n/a	❖ **Small Business**—annual revenue <$41,000,000 and process covered data <200,0000 individuals per year (beyond billing) in past 3 years: • May delete data in response to data-correction request • Relaxed requirements to respond to request for portable data • Need not conduct privacy impact or algorithm assessments • Need not train all employees with access to covered data • Need not designate data security & privacy officers • May not be sued by a private individual ❖ **Data broker**—has >50% revenue from processing data it doesn't collect or process/transfer data it doesn't collect of >5,000,000 ppl/year • Must notify public of status as data broker on website / apps • Must annually register with AG and disclose name of broker and contact person, mailing address, email address, website, and categories of covered data it processes and transfers o Penalty: $100/day civil penalty (max. $10,000/year) • AG must make searchable online registry of registered brokers ❖ **Large data holder**—has ≥ $250,000,000 annual gross revenue and collects/processes/transfers data of >5,000,000 ppl/year (except billing) • Must comply with consumer requests within 45 (not 60) days • Must prepare a plan to receive and investigate unsolicited reports of vulnerabilities in its data security systems • Must publish last 10 years' privacy policies on public website, clearly describe each material change to them, and, if also a

Attachment B: **Detailed comparison of LD 1973 and LD 1977**

	LD 1973 (Keim)	LD 1977 (O'Neil)
		covered entity, provide accessible short (<500 words) notice of its data privacy practices and individual's rights • **Annual statistics** must be disclosed by July 1st each year on its website from link to privacy policy: # verified requests to access or delete data; # requests to opt-out of data transfers or targeted advertising; # requests complied with; average days to comply • **Certify to AG** annually its good faith compliance w/law (p.17) • Designate **privacy protection officer** (who reports to CEO) to periodically review privacy and security practices; conduct biennial comprehensive audits accessible to AG; develop training program for employees; and be contact for enforcement • **Targeted advertising:** may not engage in targeted advertising in willful disregard of fact individual targeted is a minor ❖ **High-impact social media company**—has ≥$3 billion annual revenue and ≥300 million monthly active users in 3 of 12 prior months • **Targeted advertising**: may not engage in targeted advertising (a) if should have known or (b) in willful disregard of – fact individual targeted is a minor
Remedies for violations	❖ **Attorney General** may bring action under Unfair Trade Practices Act against a controller: • Must first provide notice of violation and **30-day right to cure**; may not initiate action if controller or processor asserts in writing violations are cured and no future violations will occur <u>Exceptions</u>: • No AG power under UTPA to make rules interpreting LD 1973 • No private right of action available under UPTA • Controller not liable if processor violates LD 1973 absent knowledge that processor would violate the law • Processor not liable for controller's violations	❖ **Attorney General, DA or Municipal Counsel** may bring action o/b/o Maine residents against covered entity or service provider for: • Injunctive relief to enforce compliance with law and 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 or rules against entity committing violation (except small business) for: • Actual damages or ≥ $5,000 civil penalty, whichever is greater • Punitive damages, injunctive & declaratory relief • Reasonable attorney's fees and litigation costs <u>Exceptions to liability (both public and private enforcement actions)</u>: • Covered entity transferring data not liable if service provider violates LD 1977 absent actual knowledge it would violate law • Entity receiving data not liable for transferring entity's violation ❖ Pre-dispute **arbitration agreements** are unenforceable

Attachment B: **Detailed comparison of LD 1973 and LD 1977**

	LD 1973 (Keim)	LD 1977 (O'Neil)
Repeal of other laws	❖ **Repeals 35-A M.R.S. §9301**, which generally requires Internet Service Providers (ISPs) to obtain consent before using, disclosing or selling a customer's personally identifying info. **See handout*	n/a
Definition of targeted advertising	**21. Targeted advertising.** "Targeted advertising" means displaying advertisements to a consumer when the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated publicly accessible websites or online applications to predict that consumer's preferences or interests. "Targeted advertising" **does not include**: A. Advertisements based on activities within a controller's own publicly accessible websites or online applications; B. Advertisements based on the context of a consumer's current search query, visit to a publicly accessible website or online application; C. Advertisements directed to a consumer in response to the consumer's request for information or feedback; or D. Processing personal data solely to measure or report advertising frequency, performance or reach.	**18. Targeted advertising.** "Targeted advertising" means presenting to an individual or device identified by a unique identifier, or groups of individuals or devices identified by unique identifiers, an online advertisement that is selected based on known or predicted preferences, characteristics or interests associated with the individual or a device identified by a unique identifier. "Targeted advertising" **does not include** advertising or marketing to an individual or an individual's device in response to the individual's specific request for information or feedback; an advertisement displayed based on the content or nature of the publicly accessible website or service in which the advertisement appears and does not vary based on who is viewing the advertisement; or processing covered data strictly necessary for the sole purpose of measuring or reporting advertising or content, performance, reach or frequency, including independent measurement.
Effective Date	Not specified (90 days after adjournment) - except • By July 1, 2025, consumer must opt-in to use of previously collected data for targeted advertising or for sale	Most of bill effective: 180 days after adjournment - except • 1 year later: privacy impact assessment and large data holder certification requirements take effect • 2 years later: algorithm assessment requirement takes effect

Attachment C: **other state laws related to LD 1705 (biometrics) and LD 1902 (health data)**

Research reveals that at least the following states have enacted laws specifically regulating private entities' collection, use and sharing of biometric identifiers and consumer health data. (This list may not be complete.)

a) Biometric Identifiers:

- The **Illinois** Biometric Information Privacy Act (BIPA), which is similar to LD 1705, regulates both "biometric identifiers" and "biometric information" derived from BIs. Under BIPA, a private entity generally (a) must establish a publicly available written retention policy requiring destruction of BIs when the initial purpose for their collection has been satisfied or within 3 years of the subject's last interaction with the entity; (b) may not collect, capture, purchase or otherwise obtain BIs unless it obtains the subject's written consent after providing written notice that the BI is being collected or stored and why; (c) may not disclose or share a BI unless the subject consents or disclosure is required to complete a financial transaction or to comply with a law, subpoena or search warrant; (d) may not sell, lease, or trade a BI; and (e) must store and transmit BIs in a manner consistent with the industry standard of care and that is at least as protective as the manner in which it stores and transmits other sensitive information. BIPA establishes a private right of action, through which an aggrieved person may recover actual or liquidated damages (in the same amounts as in LD 1705), reasonable attorney's fees, costs and equitable relief for each violation. BIPAA does **not**: affect the admissibility of evidence in court; apply to financial institutions subject to the Gramm-Leach-Bliley Act; or apply in a way that conflicts with federal HIPAA or its regulations. *See* 740 ILCS 14.

- **Texas** generally: (a) prohibits a person from capturing a biometric identifier for a commercial purpose unless the person informs the individual before capturing the BI and obtains the individual's consent; (b) prohibits the sale, lease or disclosure of a BI by any person unless the individual consents to the disclosure for identification if the individual disappears or dies, the disclosure is required to complete a financial transaction requested by the individual, or the disclosure is authorized by law or a search warrant; (c) requires BIs to be stored in a manner consistent with the industry standard of care and that is at least as protective as the manner in which it stores and transmits other confidential information; and (d) requires the destruction of BIs within a reasonable time not later than the first anniversary of the date the purpose of collecting the BI expires or the date that another law requires the instrument or document associated with the BI to be maintained. The state attorney general may bring an action for civil penalties of up to $25,000 per violation of this law. The law does not apply to voiceprint data retained by financial institutions or their affiliates. *See* Tex. Bus. & Com. Code §503.001.

- Unless a BI is collected to prevent fraud or theft or to protect the security of accounts, **Washington** law generally: (a) prohibits a non-government individual or entity from capturing and storing BI for a commercial purpose without first providing notice, obtaining consent or providing a mechanism by which a consumer can prevent subsequent use of the BI; (b) prohibits the sale, lease or disclosure of a BI for a commercial purpose absent consent of the individual unless the sale, lease or disclosure is necessary to provide a requested product or service, is required by law or a court order, is made to prepare for litigation or is to a third party that contractually agrees to protect the information; and (c) requires individuals and entities that possess BIs for a commercial purpose to retain BIs no longer than is necessary and to take reasonable care to prevent unauthorized access to the BIs. Violations of the Washington Law are considered unfair or deceptive acts and unfair competition and are enforceable solely by the state attorney general. The law does not apply to activities subject to federal HIPAA and its regulations *See* R.C.W. ch. 19.375.

b) **Consumer Health Data**

- The **Connecticut** Data Privacy Act (CTDPA), a general consumer privacy law, was amended shortly before it took effect on July 1, 2023 to include protections for "consumer health data"— non-public personal data used "to identify a consumer's physical or mental health condition or diagnosis" to the extent the CHD is not subject to regulation by HIPAA. The CTDPA applies to "controllers," which are generally non-governmental (defined also as non-tribal governmental) individuals and entities that conduct business in or target products or services to the state and that control or process the personal data of at least 100,000 consumers or of at least 25,000 consumers and more than 25% of their revenue derives from the sale of personal data. The CTDPA treats CHD as "sensitive data" and generally: (a) requires a controller to limit the collection of CHD to what is reasonably necessary and disclosed to the consumer; (b) prohibits a controller from processing or selling CHD without the consumer's consent or processing CHD for purposes of targeted advertising; (c) requires a controller to provide a mechanism for a consumer to revoke consent that is "at least as easy" as the mechanism to consent and to comply with the revocation request within 15 days; (d) requires a controller to maintain data security practices appropriate to the volume and nature of the personal data at issue; (e) prohibits a controller from discriminating against a consumer that exercises its rights under the CTDPA; (f) requires a controller to provide consumers with a clear privacy notice explaining the categories of data it processes, and why, and what categories it shares with third parties as well as how consumers may exercise their rights; (g) requires a controller to regulate the activities of processors via contract; and (h) prohibits any person from establishing a geofence within 1,750 feet of a mental health or reproductive or sexual health facility for purposes of identifying, tracking, collecting data from or sending notices to consumers regarding the consumer's CHD. Violations of the CTDPA are enforceable by the Attorney General under the unfair trade practices act, except that prior to December 31, 2024, the Attorney General must issue a notice of violation and provide controllers a 60-day period to cure the violation. *See* Conn. Gen. Stat. §§ 42-515 to -525 as amended by Public Act No. 23-56.

- The **Washington** My Health My Data Act, which is similar to LD 1902, regulates "consumer health data"—non-public personal information "reasonably linkable to a consumer" that identifies the consumer's physical or mental health status (with examples, like biometric data or location information related to an attempt to obtain health care, that mirror the definition in LD 1902) to the extent it is not regulated by federal HIPAA. The Washington law applies to "regulated entities," which are non-governmental (including non-tribal governmental) entities that conduct business in or target products or services to consumers in the state. **Like LD 1902**, the Washington law generally (a) requires a regulated entity to obtain separate consent for collection and for sharing of CHD, unless collection or sharing is necessary to provide a product or service requested by the consumer; (b) requires a regulated entity, on receipt of an authenticated request, to confirm collection or sharing (or selling) of CHD, to comply with a consumer's withdrawal of consent for collection or sharing (or selling) of CHD, and to comply with the consumer's request to delete their CHD and notify transferees of the deletion request;[1] (c) requires a regulated entity to establish and adhere to a CHD privacy policy posted on its homepage and adopt and follow security practices that limit access to CHD consistent with the industry standard of care; (d) prohibits any regulated entity from discriminating against a consumer for exercising any rights under the law; (e) limits processors to the activities authorized by contract with a regulated entity; and (f) prohibits any person from implementing a geofence to identify a health care facility's customers, except that **unlike LD 1902** the geofence restrictions are limited to the area within 2,000 feet of the facility and the geofence prohibition applies to the collection ***only of CHD*** from customers or the targeting of customers only with messages ***related to their CHD or health care services***. Also unlike LD 1902, the Washington law generally (a) allows the sale of CHD with consent of the consumer, which

[1] Unlike LD 1902, Washington law provides that, if the CHD is stored on archived or backup system, deletion of CHD may be delayed for up to 6 months after authenticating a consumer's deletion request to restore the archived or backup system.

consent expires one year after it is made and may not be a condition for the sale of goods or services to the consumer; (b) allows regulated entities to collect, use or disclose CHD to prevent, detect or respond to security incidents, identity theft, fraud, harassment or other illegal activities; (c) does not require the establishment of a CHD retention policy requiring deletion of CHD at the end of provision of services; and (d) delays from March 31, 2024 to June 30, 2024 the law's applicability to certain small businesses. Violations of the law are per se violations of the Washington Consumer Protection Act, which allows actions for monetary and equitable relief to be brought by the Attorney General and private parties. *See* R.C.W. Ch. 19.373.

- **Nevada** recently passed legislation, which takes effect March 31, 2024, regulating "consumer health data," which is ***defined more narrowly than in LD 1902*** to include only non-public personal information "reasonably linkable to a consumer" that ***is used by a regulated entity*** to identify a consumer's health status (with examples, like biometric data or location information related to an attempt to obtain health care, that mirror the definition in LD 1902) to the extent it is not regulated by federal HIPAA. **Like LD 1902**, the Nevada law generally (a) requires a regulated entity to obtain separate consent for collection and for sharing of CHD, unless collection or sharing is necessary to provide a product or service requested by the consumer; (b) requires a regulated entity, on receipt of an authenticated request, to confirm collection or sharing (or selling) of CHD, to comply with a consumer's withdrawal of consent for collection or sharing (or selling) of CHD, and to comply with the consumer's request to delete their CHD and notify transferees of the deletion request;[2] (c) requires a regulated entity to establish and adhere to a CHD privacy policy posted on its main Internet website and adopt and follow security practices that limit access to CHD consistent with the industry standard of care; (d) prohibits any regulated entity from discriminating against a consumer for exercising any rights under the law; (e) limits processors to the activities authorized by contract with a regulated entity; and (f) prohibits any person from implementing a geofence to identify a health care facility's customers, except that **unlike LD 1902** the geofence restrictions are limited to the area within 1,750 feet of the facility and also the geofence prohibition applies to the collection ***only of CHD*** from customers or the targeting of customers only with messages ***related to their CHD or health care services***. Also unlike LD 1902, the Nevada law generally: (a) allows the sale of CHD with consent of the consumer, which consent expires one year after it is made and may not be a condition for the sale of goods or services to the consumer; and (b) does not require the establishment of a CHD retention policy requiring deletion of CHD at the end of provision of services. Violations of the law constitute deceptive practices enforceable by the Attorney General for which restitution and injunctive relief may be ordered and, in certain circumstances, civil penalties or criminal misdemeanor penalties. However, there is no private right of action for violations of the law. *See* Nev. Sen. Bill 370 (as enacted).

[2] Unlike LD 1902, the Nevada law provides that, if the CHD is stored on archived or backup system, deletion of CHD may be delayed for up to 2 years after authenticating a consumer's deletion request to restore the archived or backup system.

NON OPLA MATERIALS

AMERICAN CIVIL LIBERTIES UNION
Maine

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

WRITTEN COMMENTS OF MEAGAN SWAY, ESQ.

Work Session regarding LDs 1705, 1902, 1973, 1977

Joint Standing Committee on Judiciary

October 17, 2023

Senator Carney, Representative Moonen, and distinguished members of the Joint Standing Committee on Judiciary, good afternoon. My name is Meagan Sway, and I am the Policy Director at the American Civil Liberties Union of Maine (the "ACLU of Maine"), a statewide organization dedicated to preserving and protecting the constitutional rights of people in Maine. The ACLU of Maine is a state affiliate of the national American Civil Liberties Union (the ACLU). Both the ACLU and the ACLU of Maine have a long history of protecting the right to privacy, both as it pertains to governmental and business intrusions into that right. The ACLU of Maine was instrumental in the writing and passage of several seminal privacy laws in Maine, including our strongest in the nation internet service provider privacy law, *see* 35-A M.R.S. §9301, the law restricting the government's ability to use facial recognition technology, *see* 25 M.R.S. §6001, the law requiring a warrant in order for law enforcement to access portable electronic information or cell phone location information, *see* 16 M.R.S. §641 et seq., §647 *et seq*. I write in response to the Committee's invitation to provide comments regarding LDs 1705, 1902, 1973, and 1977.

Corporations have built a surveillance economy that seeks to collect as much information about a person as possible to turn a profit. They harvest data about what we do at home, what we do at work, what we buy, where we go, what doctors we see, our contacts with the criminal and civil legal systems, and more. In the United States, these companies face almost no real restrictions on the amount of personal information they can amass about us or the ways that they can exploit it. In the absence of protections, companies have compiled massive dossiers on each one of us containing staggering amounts of information. This information can identify us across our interactions with the world both online and off, within our homes and outside of them, creating the potential for private surveillance on a massive scale. That information can then be sold to data brokers or used to power surveillance-based advertising. Some of these uses have discriminatory impacts, as when companies exclude people from seeing advertisements for employment,

housing, or credit on the basis of their race, gender, nationality, or other protected class status.

In order to stop these harms, consumer privacy legislation must, at a minimum, contain strong restrictions on the amount of personal information that can be collected and the ways in which it can be used, including: establishing data-minimization limitations that prevent companies from collecting and retaining more data than they need to provide the service we ask for; requiring opt-in consent before companies collect and use our personal information; providing users with the tools to access and control their personal information; creating strong new civil rights protections; prohibiting companies from discriminating against people who exercise their privacy rights under the law; enabling people to sue privacy-violating companies to obtain meaningful monetary relief; and preserving the ability of local activists to seek—and local governments to enact—stronger protections. Below please find our answers to the questions presented to interested parties.

1. **What are the benefits and drawbacks of including a private right of action in consumer data privacy legislation?**

Without a private right of action, people have little practical ability to seek relief when their personal information is unscrupulously collected or misused. This eliminates a powerful incentive for companies to comply with the law. While corporations will tell this committee that a private right of action benefits only trial lawyers, the lack of any private right of action harms everyday Maine people, and only benefits the large corporations who are banking on being able to sell our data with impunity. When companies ignore the law, a private right of action allows affected individuals to obtain redress for the harm they have suffered. A private right of action is also vital because the Attorney General's Office has very few attorneys dedicated to proactively pursuing companies for violating consumers' rights. This means that, practically speaking, a law without a private right of action will be enforced only when its violation is so egregious as to be a massive violation. Smaller scale but no less intrusive violations of the law will necessarily go unaddressed without a private right of action, because the Attorney General lacks the staff to address all the issues. A private right of action both conserves state resources and ensures that state residents can vindicate their own rights.

2. **Should the Legislature enact standalone bills addressing biometric identifiers and health data in addition to enacting a comprehensive data privacy bill or should the Legislature address all types of consumer personal data in a single bill? Why?**

The question of whether to address specific standalone privacy measures or to address privacy in one bill depends on several factors. Standalone bills (like LD

1705, addressing biometrics, or LD 1902, addressing health data) may be desirable because they address time-sensitive issues, affect a limited number of industries, use more precise and targeted language, and have specific remedies appropriate for the issue at hand. However, when bills address specific topics, such as biometrics or health data, they can run the risk of being under-inclusive, and miss potential areas of concern that are not directly on point to a specific subset of data. One critical example of this is in discussions around health privacy; in the age of big data and machine learning, even once-innocuous data like our geolocation, online browsing, or recent purchases can now be used to infer our health conditions. Comprehensive privacy legislation helps protect our privacy across all types of data, even if their sensitivity is not immediately apparent.

Ultimately, the Legislature should adopt the strongest privacy regulations possible, to ensure that people in Maine are best protected from surveillance and privacy invasions. If comprehensive bills are less protective of privacy, or weaken existing privacy protections, their benefit as a comprehensive bill is diminished or even lost. Although there is room for additional work, LD 1977 provides robust protections that help alleviate the need for bills tailored to specific types of data: data minimization requirements, opt-in consent for many uses of data, and minimum requirements for cybersecurity.

3. **How does the choice between an opt-in or an opt-out model for consumer consent to the collection/sharing/sale of personal data impact consumers?**

Strong consumer privacy bills will have opt-in rather than opt-out provisions to allow the collection and use of consumers' information. (Maine's law protecting consumers' privacy as it relates to internet service providers is the strongest in the country because, in order for ISPs to sell a consumer's data, the consumer must opt in.)

A framework that requires consumers to opt out of all or most collection or use of their personal data places the burden entirely on the consumer to wade through reams of legalese with multiple companies in order to exercise their privacy rights. For example, one FTC study found that some companies required users to navigate a half-dozen steps, including links and tabs buried at the bottom of settings pages. Another company split opt-out choices across *nine* different settings pages.[1] Additionally, the ability to opt out only from sale of personal information, but not

---

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

the collection or use of that information, means that the data practices of the largest surveillance companies like Meta and Google will remain mostly untouched. That is because Facebook and Google claim not to sell our personal information, but rather, they amass information about their own users and buy people's information from other companies, and then sell access to tools that make invasive use of that information. Only a strong and broad opt-in consent requirement can adequately protect people's privacy.

Additionally, oftentimes opt-out bills or laws allow companies to discriminate against users who exercise their right to opt-out of targeted advertising by charging the consumer higher prices or offering inferior service. This pay-for-privacy provision risks making privacy a luxury good, available only to those who can afford to pay for it, further marginalizing the most marginalized, and exacerbating the existing digital divide. We strongly encourage an opt-in framework, but to the extent the committee chooses an opt-out framework, it should ensure that companies cannot then retaliate against those who do opt out.

4. **Are there particular approaches to consumer data privacy in other states that you consider particularly valuable or problematic?**

The privacy legislation passed in other states has run the gamut, from data-specific bills like bills in Illinois, Washington and Texas to protect biometric information, to more comprehensive bills pushed by Big Tech like the laws passed in Connecticut, Utah, Colorado. Each bill has its own approach, but the best approaches to protect consumer privacy include:

- Data minimization. It is not enough that consumers get notice of what personal data is collected and shared and are able to consent – especially when "notice" and "consent" are functionally legal fictions. "Notice" is commonly provided through privacy policies, and those policies are so dense and take so long to read that they fail to provide any real "notice" at all. Similarly, "consent" is often inferred from use of the site or service or by clicking on a banner that provides no information on the service's data practices. Notice and consent cannot be the only protections that consumers are afforded. Instead, laws must minimize data collection and the ways that data can be used – meaning that services and sites may only collect, use, and disclose data as is necessary to provide the service the consumer requested.
- Requiring opt-in consent before companies collect and use our personal information. Maine's internet service provider privacy law requires this opt-in before internet service providers can sell our information, and that is a crucial protection for internet users. Comprehensive bills like Connecticut, Utah, Colorado, etc. often apply "opt-in" only to a limited set of data, which is problematic because as data mining and machine learning can use

information that is not particularly sensitive to get a very specific picture of sensitive information.

- Civil rights protections. Our personal data is increasingly used in ways that affect our opportunities in traditionally protected areas of life such as housing, education, employment, and credit. There is ample evidence of the discriminatory harm that artificial intelligence and algorithmic systems can cause to already marginalized groups. Bias is often baked into the outcomes the AI is asked to predict and the data used to train the AI, which can manifest throughout the AI's design, development, implementation, and use.[2] The impact on the daily lives of Americans is unprecedented. Banks and other lenders use AI systems to determine who is eligible for a mortgage or student loan. Housing providers use AI to screen potential tenants. AI decides who's helped and who's harmed with influential predictions about who should be jailed pretrial, admitted to college, or hired. A comprehensive privacy law must ensure that the use of our data in AI adheres to our foundational values of nondiscrimination and equality.
- Providing a private right of action. A private right of action, especially in a state as small as Maine, is crucial to ensuring that companies are held accountable for breaking the law. We can see what happens when there is a private right of action and when there is not a private right of action, when we look at biometric privacy laws. Illinois has a private right of action to enforce violations of its Biometric Privacy Information Act. Washington and Texas do not. Washington and Texas, though their offices of the Attorney General are much bigger than Maine's, have not meaningfully enforced their biometric privacy laws. The private right of action in Illinois has been enforced through the private right of action. You will hear much about the sky falling in Illinois, but we can learn lessons from that state to ensure that a private right of action serves its intended purpose, rather than jettisoning it altogether.

5. **What existing federal laws protect consumer personal data in your industry (or the industry of concern to you) – what types of data do those laws protect (or not protect) and what types of companies do they regulate (or not regulate)?**

Federal privacy laws are limited to protecting specific data in only specific sectors, leaving "gaps" in privacy protections, even in economic sectors where consumers would reasonably expect their data to be protected. Thus, laws like the Health

---

[2] *See ACLU letter to House Energy and Commerce Committee on American Data Privacy and Protection Act*, Jul. 18, 2022 available at https://www.aclu.org/documents/aclu-letter-house-energy-and-commerce-committee-american-data-privacy-protection-act.

Insurance Portability and Accounability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and the Fair Credit Reporting Act (FCRA) cover "protected health information" handled by health care providers, "personal information from education records," and "consumer reports" furnished by "consumer reporting agencies" – but not data collected by fitness apps, edtech services, or data brokers. Other federal laws such as title V of the Gramm-Leach-Bliley Act, the Privacy Act of 1974, and Genetic Information Non-discrimination Act provide a smattering of protections for some financial information, governmental information, and genetic information. Comprehensive privacy legislation fills those gaps by creating a common, baseline set of privacy protections for all data – regardless of whether they happen to fall within the ambit of now sometimes dated federal law.

Moreover, the data practices of some of the largest, most data intensive industries like social media and targeted advertising remain entirely unregulated. The same is true of sectors that have not traditionally been reliant on monetizing data, such as the automotive industry – as one recent report put it, "every car brand . . . collects more personal data than necessary and uses that information for a reason other than to operate your vehicle and manage their relationship with you."[3] State comprehensive legislation would address the fields that federal law has yet to address.

6. Are there any pending Congressional proposals regarding consumer data privacy of which the Maine Legislature should be aware?

In short, no, although this is the question that everyone is watching. At this point, we are a quarter of the way through the 118th Congress, and the House – where last year's big federal privacy bill originated – has been incredibly quiet. Elsewhere, there has been movement on limited topics including bills addressing children's privacy and speech online, health data, and reproductive data. Some of those bills have gained traction in one chamber or another, but it is not at all clear that any have strong potential to become law. Even if they did, none of the leading bills include preemption provisions, and they would not impact our work here. And critically, those bills would not provide a robust privacy baseline across economic sectors, but would instead leave the "gaps" between sectoral privacy laws unaddressed.

---

[3] Jen Caltrider, Misha Rykov and Zoë MacDonald, *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy*, Mozilla, Sept. 6, 2023, available at https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.

As federal work unfolds, states like Maine have an important place in the conversation. Although legislation has been passed in a dozen states, those laws lack important protections like data minimization, civil rights protections, and a private right of action. As private companies make immense profits off our data and use it to fuel emerging, untested AI technologies, those rights should be a baseline – not optional perks. Maine has the opportunity to lead the nation in establishing those protections, which will set the bar for national standards. If Maine instead joins other states in passing watered down legislation, it will ground the national conversation in those inadequate protections.

* * *

Thank you for the opportunity to present our feedback on the privacy legislation pending before you. The surveillance economy poses some of the biggest threats to democracy and personal autonomy that the world has ever seen, and we welcome the chance to work with the committee to craft legislation that protects people in Maine against these unprecedented threats.

FOR WS 10/17/23

www.ataaction.org

ATA ACTION
Telehealth Policy to Transform Healthcare

October 16, 2023

Hon. Anne M. Carney
Chair, Joint Committee on Judiciary
Senator, District 29
3 State House Station
Augusta, ME 04333-0003
Anne.Carney@legislature.maine.gov

Hon. Matt Moonen
Chair, Joint Committee on Judiciary
Representative, District 38
Room 333, State House
2 State House Station
Augusta, Maine 04333-0002
Matt.Moonen@legislature.maine.gov

CC: JUD@legislature.maine.gov

RE: ATA Action comments for October 17th Committee Work Session on Data Privacy

Dear Chair Carney, Chair Moonen and members of the Judiciary Committee,

On behalf of the ATA Action, I am writing you to provide comments regarding the Committee's upcoming October 17th public hearing and work session to review a series of data privacy bills.

ATA Action, the American Telemedicine Association's affiliated trade association focused on advocacy, advances policy to ensure all individuals have permanent access to telehealth services across the care continuum. ATA Action supports the enactment of state and federal telehealth coverage and fair payment policies to secure telehealth access for all Americans, including those in rural and underserved communities. ATA Action recognizes that telehealth and virtual care have the potential to truly transform the health care delivery system – by improving patient outcomes, enhancing safety and effectiveness of care, addressing health disparities, and reducing costs – if only allowed to flourish.

In light of the advancement of privacy legislation in many states across the country, ATA Action recently published its Health Data Privacy Principles (attached) to aid legislators in crafting legislation that supports both secure data practices and ensures patient access to care. As you review the privacy bills laid before the Committee, ATA Action urges you to keep the following considerations in mind:

State consumer privacy laws should be consistent with and not exceed HIPAA's standards to the greatest extent possible

ATA ACTION
901 N. Glebe Road, Ste 850 | Arlington, VA 22203
Info@ataaction.org

ATA ACTION
Telehealth Policy to Transform Healthcare

Enacted almost thirty years ago, the Health Insurance Portability and Accountability Act ("HIPAA" and the HIPAA Privacy Rule adopted in 2000) is a time-tested health information privacy framework that providers understand and patients expect to keep health data protected. Mirroring these well understood HIPAA standards in state law will be key to providing consistency and reducing complexity while also mitigating compliance and administrative costs on providers.

Therefore, ATA Action recommends that Maine's data privacy laws should explicitly exempt HIPAA covered entities that are already subject to HIPAA privacy rules. Imposing additional, duplicative, and potentially inconsistent regulation on these entities would create unnecessary and inappropriate burdens and costs.

Furthermore, we urge that any privacy framework does not subject healthcare entities that fall outside this HIPAA exemption to greater administrative burdens or more restrictive rules than their exempted HIPAA covered entity peers. For example, a patient's interaction with a telemedicine provider paid in cash out-of-pocket would not be subject to HIPAA, although the information the provider gathers may be similar to patient information gathered during a traditional doctor's office examination reimbursed by insurance and subject to HIPAA privacy rules.

ATA Action therefore urges lawmakers to strive for uniform privacy law burdens across healthcare encounters, both in line with patient expectations and to better ensure competitive equity among providers. If not providers would be subjected to disproportionate regulatory burdens contingent on how a patient pays for care rather than patient expectations related to the nature or sensitivity of the health information gathered.

Privacy laws should require clear and conspicuous disclosures regarding data use, consumer consent for the sharing or sale of data, and the ability for consumers to opt-out of data use

State privacy laws should require clear and conspicuous disclosures on what data an entity collects, how the data will be used and how a consumer can opt-out of data processing. This should include a clear definitions of "sale of data" and "sensitive data", and what explicit disclosures and consumer consent are required related to the sale or marketing use of personal or sensitive data. ATA Action suggests these requirements align with, and be no more burdensome than, the HIPAA Privacy Rule's marketing requirements,[1] which allow for disclosure of protected health information in "exchange for direct or indirect remuneration" so long as the consumer has provided their written authorization for such sale.

Good examples of states that have enacted consumer data privacy laws which balance privacy interests, administrative burdens and clarity in the context of health information include the Virginia Consumer Data Protection Act[2] and the Connecticut Consumer Data Privacy and Online Monitoring Act.[3]

---

[1] *Marketing*, U.S. Dept. of Health and Human Servs. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html.

[2] Virginia Consumer Data Protection Act, VA Code Ann. § 59.1-575 *et seq.*, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/.

[3] Connecticut Consumer Data Privacy and Online Monitoring Act, Conn. Gen. Stat. § 42-515 *et seq.*, https://www.cga.ct.gov/current/pub/chap_743jj.htm.

ATA ACTION
Telehealth Policy to Transform Healthcare

State attorneys general should have sole enforcement authority when privacy laws are violated

ATA Action believes that state attorneys general should have appropriate authority to investigate possible violations of privacy laws and determine when it is appropriate to pursue sanctions against bad actors. ATA Action also recommends that legislators avoid including private rights of action as a method of enforcing privacy laws, which are prone to a lack of clarity, result in frivolous lawsuits and result in out-of-court settlements that exacerbate legal uncertainty.

Please see the attached Privacy Principles for greater detail on ATA Action's data privacy policy positions and do not hesitate to let us know how we can be helpful to your efforts to advance common-sense telemedicine policy. If you have any questions or would like to discuss the telemedicine industry's perspective further, please contact me at kzebley@ataaction.org.

Kind regards,

Kyle Zebley
Executive Director
ATA Action

Health.
Virtually.
Everywhere.

The ATA's Health Data Privacy Principles

The protection of patient data is prerequisite for connected care and a core principle for our organization. The ATA supports efforts to ensure telehealth practices meet standards for patient safety, data privacy, and information security, while advancing patient access and building awareness of telehealth practices.

Consistency:

Regulatory consistency across industries is paramount to protecting consumer privacy while simultaneously mitigating compliance, complexity and financial costs for U.S. companies. A federal policy would offer consistency and is preferable to a state-by-state approach. However, as states adopt privacy statutes and regulations, an effort to establish uniformity with existing federal and other state standards would reduce both complexity of compliance and confusion for consumers and companies alike. Privacy laws should allow for innovation and the advancement of technology-assisted care. Personal health information used in telehealth and virtual care platforms, systems, and devices should be secured and protected from misuses and inappropriate disclosures.

Definition of Consumer Health Data:

State law and policy should define consumer health data (and other terms commonly used to characterize personally identifiable health care information) by adopting the same language that defines protected health information in the Health Insurance Portability and Accountability Act (HIPAA).

HIPAA:

State consumer privacy laws should be consistent with and not exceed HIPAA's standards to the greatest extent possible, to ensure that patient protections are not contingent on whether the entity is HIPAA-covered. HIPAA-covered entities and their business associates should be exempt from state privacy laws. HIPAA is a proven, decades-old data privacy framework. Requiring HIPAA-covered entities to adhere to additional layers of state privacy laws would negatively impact their ability to deliver services, increase compliance costs, and stymie innovation.

Consumer Rights:

Consumers should be entitled to meaningful, accessible, and actionable rights, including: a right to notice, a right to access, a right to correct, a right to portability, a right to delete so long as these rights are consistent with other medical record retention laws and contains an exception for when data may be required to defend against legal claims or to comply with legal obligations. Notices should include all categories of data, processors, and other third parties the data controller is working with. Notices should also indicate that consumers can receive specific information regarding their personal information upon request. At the same time, all covered entities should be allocated a reasonable amount of time to comply with various consumer requests, including a consumer's request to delete data.

Consumer Consent, Sale of Data & Opt-Out:

Consumers should be provided clear and conspicuous disclosures on what data is collected, how it will be used, and a how to opt-out of processing for purposes of (a) targeted advertising, (b) the sale of personal data; or (c) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. If applicable, disclosures should also clarify whether any data will be shared or sold for any purpose outside what is required to provide the service requested by the consumer. What constitutes the sale of data should be clearly defined, and the sharing of any sensitive data should require explicit disclosure to and consent from the patient. Sensitive data should be defined as personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health diagnosis, sexuality, or citizenship or immigration status; genetic or biometric data processed to identify individuals; and precise geolocation data.

Enforcement:

State Attorneys General should be empowered to take enforcement action when privacy laws are violated. However, private rights of action should not be included in data privacy policy because they can lead to a lack of clarity, result in frivolous lawsuits, and result in out-of-court settlements that exacerbate legal uncertainty.

Health.
Virtually.
Everywhere.

www.americantelemed.org

Adopted by the ATA Policy Council: June 2023
Approved by the ATA Board: July 2023

For WS

CATO

Statement

of

Jennifer Huddleston

Technology Policy Research Fellow
Cato Institute

before the

Judiciary Committee
Maine State Legislature

October 17, 2023

RE: Data Privacy Working Session

Cato Institute • 1000 Massachusetts Ave., N.W. • Washington, D.C. 20001 • (202) 842-0200
Fax: (202) 842-3490 • www.cato.org

Chairs Carney and Moonen and Members of the Judiciary Committee:

My name is Jennifer Huddleston and I am a technology policy research fellow at the Cato Institute. My research focuses on the intersection of law and technology, including issues related to data privacy. I thank you for the opportunity to provide informational testimony based on my work on this topic and will focus on five of the questions presented today.

(1) What are the benefits and drawbacks of including a private right of action in consumer data privacy legislation?

A private right of action risks bringing litigation that may particularly burden small firms and not actually improve the underlying concerns if there are not appropriate guardrails that ensure such litigation only responds to actual harm and benefits those truly impacted — not just certain attorneys. For this reason, a private right of action for mere statutory violations, one that encourages class actions and extends beyond actual damages, is likely to have significant drawbacks.

One of the key drawbacks of a private right of action is that the actual individuals who experience harm may not be the ones compensated or provided other forms of redress for that harm. Rather, it's the attorneys that bring the cases. For example, one analysis found that "plaintiffs' lawyers received an average settlement of $11.5 million per firm per case, while individuals received an average settlement of $506 per case in litigation under Illinois' Biometric Information Privacy Act."[i] Additionally, companies may be faced with pressure to settle or change practices even if they would have been successful in court due to the costs of litigation, particularly for startups and small companies. Given the risk of potential litigation even if no harm occurs, companies may be more hesitant to deploy certain technology that is beneficial if it is unclear that it meets specific statutory requirements.

As will also be discussed in answers to Question 2, this is not merely theoretical, as the Illinois Biometric Information Privacy Act (BIPA) has a private right of action. The consequences for Illinois residents and businesses have been significant. But these lawsuits have not only been limited to cases where residents' data has been leaked, but to statutory violations where no harm occurred. This is most notable in the case that was brought against Six Flags, where the Illinois court upheld that mere statutory violations, without injury or adverse effect, were sufficient for harm.[ii] Additionally, the total amount of litigation has risen significantly in light of large settlements and court decisions, often without a need to prove actual harm following such an interpretation.[iii] This includes cases against phototagging on popular websites like Facebook[iv] as well as more unexpected cases against trucking companies[v] and White Castle[vi].

(2) Should the Legislature enact standalone bills addressing biometric identifiers and health data in addition to enacting a comprehensive data privacy bill or should the Legislature address all types of consumer personal data in a single bill? Why?

As an individual cannot change certain features — like their iris or fingerprints — and certain information around health can be considered particularly sensitive, policymakers often want to provide additional protection for this information. However, overly broad definitions may cause problems, as can a failure to specifically define the harm that is sought to be addressed. In most cases, proposals only address the concerns about this information in the hands of private actors and do not consider potential abuse by the government of what is considered particularly sensitive information.

At a federal level, certain health information is already protected under the Health Insurance Portability and Accountability Act (HIPAA). As with any privacy law, proposals should be grounded in particular harms and have clear definitions. Health information could be considered so broadly that it could end up applying to a much wider range of apps than likely intended. For example, the resting heart rate on a fitness tracker, the purchase of special dietary requirement food at a grocery store, or a photo with a cigarette could be considered health information under broad definitions subjecting much more data and many more innovators to a law's requirements. Additionally, some of this same "sensitive" information can be helpful in empowering users to take control of their own health, such as apps that can send reminders for medication, track blood sugar, or provide information about what a pregnant woman could expect.

As biometric information such as fingerprints or voice prints cannot be changed, many advocate for additional privacy protection for such information. Washington, Texas, and Illinois have laws applying broadly to biometric information. Biometric information is also covered under some states' comprehensive privacy laws. While often viewed with a skeptical eye, biometric information can be beneficial both for consumers and improving cybersecurity. For example, for many of the same reasons behind the desire to keep the information more secure, biometric information can also be useful for securing access to certain areas or information in a way that improves cybersecurity. Additionally, this information can be used to help identify family and friends in photos or help identify who is at the door with a smart doorbell. Over-regulation might discourage further development of this technology or limit beneficial applications when faced with inflexible regulatory requirements. The result could be as seen in states that currently have these laws that certain features are unavailable.[vii]

(4) Are there particular approaches to consumer data privacy in other states that you consider particularly valuable or problematic?

A dozen states now have comprehensive consumer data privacy laws. As discussed in previous work, due to the nature of data, a federal approach is preferable to a state-by-state approach. Most of these laws have generally followed either California's heavily regulatory approach or a slightly more flexible approach seen in Virginia and Utah.[viii] Of note, Tennessee became the first state to create a safe harbor for compliance with National Institute of Science and Technology

Standards as part of their privacy law.[ix] Such an approach could lessen the burden of state specific compliance costs and be more flexible and adaptive with industry best practices.

A growing patchwork of laws is likely to increase confusion for consumers who will be unlikely to know their rights from state to state and to innovators who may not know how to respond to potentially conflicting requirements or what to do in certain scenarios. As such, it is a far from ideal solution. For example, there is currently a 50-state patchwork of data breach notification laws, but these laws vary in the type of information covered, what constitutes notification, the timelines for notification, and what consumers should be notified.[x] This will only be more pronounced in the case of more general data privacy laws.

A federal approach remains preferable to a state-by-state approach for both innovators and consumers. For example, one study found "the out-of-state costs from 50 such laws could exceed $1 trillion over 10 years, with at least $200 billion hitting small businesses."[xi] Many of these costs will likely be passed on to the consumer at a time when consumers are already concerned about rising prices.

(5) What existing federal laws protect consumer personal data in your industry (or the industry of concern to you) – what types of data do those laws protect (or not protect) and what types of companies do they regulate (or not regulate)?

Contrary to popular belief, the United States is not without any data privacy laws. Rather than take an overarching approach, the federal government (as well as states) have responded to concerns related to specific types of data that is considered more sensitive or to specific populations, such as children, that are considered more vulnerable or unable to properly consent.[xii] When considering data privacy, it is important to recognize that while it is typically thought of as an online issue, many offline businesses and industries have benefited from the use of data and would be affected by these laws. In fact, looking at Europe, everything from more commonly thought of services like retail loyalty programs to less likely considered entities like churches and cemeteries have been impacted by concerns about ensuring compliance with data privacy laws.[xiii]

Given the growing use of data in a wide array of industries, it is important to consider what harms a privacy law is trying to address. Penalizing certain types of data or creating mere statutory violations might prevent innovative beneficial applications in the future as well as impact those that already exist and do not cause harm.

(6) Are there any pending Congressional proposals regarding consumer data privacy of which the Maine Legislature should be aware?

The 117th Congress saw perhaps the most progress on a federal data privacy bill. The American Data Privacy Protection Act was a bipartisan bill that passed through committee in the House of Representatives, but failed to have further action that Congress. Congress continues to debate

possible data privacy; however, a similar bipartisan approach or comprehensive bill has not yet gained momentum in the 118th Congress.

Conclusion

Thank you for your time and consideration of this information. I welcome any questions related to my research on data privacy and my responses to these questions. This testimony should be considered for informational purposes and not in support of or opposition to any particular piece of legislation.

[i] Kaitlyn Harger, *Who Benefits from BIPA: An Analysis of Cases Brought Under Illinois' State Biometrics Law*. Chamber of Progress (2023). Accessible at https://progresschamber.org/wp-content/uploads/2023/03/Who-Benefits-from-BIPA-Analysis-of-Cases-Under-IL-Biometrics-Law.pdf.

[ii] *Rosenbach v. Six Flags Entertainment Corp*. (Illinois 2019).

[iii] *Illinois Biometric Privacy Cases Jump 65% After Seminal Ruling*. Bloomberg Law (2023). Accessible at https://news.bloomberglaw.com/privacy-and-data-security/illinois-biometric-privacy-cases-jump-65-after-seminal-ruling.

[iv] Victoria Cavaliere, *Judge approves $650 million settlement of Facebook privacy lawsuit linked to facial photo tagging*. Business Insider (2021). Accessible at https://www.businessinsider.com/facebook-settlement-pay-650-million-privacy-lawsuit-biometrics-face-tagging-2021-2?utm_source=copy-link&utm_medium=referral&utm_content=topbar.

[v] Robert D. Boley, Paula M. Ketcham, and Adam L. Littman, *First BIPA Trial Results in $228M Judgment for Plaintiffs*. National Law Review (2022). Accessible at https://www.natlawreview.com/article/first-bipa-trial-results-228m-judgment-plaintiffs.

[vi] Barry P. Kaltenbach and Robert T. Zielinski, *The $17 Billion Slider? Illinois Supreme Court Decides White Castle BIPA Case*. National Law Review (2023). Accessible at https://www.natlawreview.com/article/17-billion-slider-illinois-supreme-court-decides-white-castle-bipa-case.

[vii] *Google's art selfies aren't available in Illinois: Here's why*. Chicago Tribune (2023). Accessible at https://www.chicagotribune.com/business/ct-biz-google-art-selfies-20180116-story.html.

[viii] Jennifer Huddleston and Gent Salihu, *The Patchwork Strikes Back: State Data Privacy Laws After the 2022-2023 Legislative Session*. Cato Institute (2023). Accessible at https://www.cato.org/blog/patchwork-strikes-back-state-data-privacy-laws-after-2022-2023-legislative-session-0.

[ix] Tennessee Information Protection Act (2023), accessible at https://www.capitol.tn.gov//Bills/113/Amend/HA0348.pdf.

[x] *State Data Breach Notification Chart*. International Association of Privacy Professionals (2021). Accessible at https://iapp.org/resources/article/state-data-breach-notification-chart/.

[xi] Daniel Castro et al., *The Looming Cost of a Patchwork of State Privacy Laws*. Information Technology & Innovation Foundation (2022). Accessible at https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/.

[xii] Alan McQuinn, *Understanding Data Privacy*. Real Clear Policy (2018). Accessible at https://www.realclearpolicy.com/articles/2018/10/25/understanding_data_privacy_110877.html.

[xiii] *If You Run a US Cemetery Here's Why GDP's Your New Best Friend.* Plot Box (2019). https://www.plotbox.io/blog/gdpr-in-us-cemeteries; *Data Protection: Parishes and GDPR*. Accessible at https://www.parishresources.org.uk/gdpr/.

October 17, 2023

Committee on Judiciary
Attn: Janet A. Stocco, Esq. - Legislative Analyst
State House
100 State House Station
Augusta, ME 04333

Maine Judiciary Committee Work Session - Consumer Data Privacy Bills

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

On behalf of the Computer & Communications Industry Association (CCIA), I would like to thank you for the opportunity to provide comments as the Judiciary Committee further weighs the various consumer data privacy bills put forth by the legislature.

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] CCIA supports the enactment of comprehensive federal privacy legislation to promote a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights and responsibilities for organizations that collect and process data. A uniform federal approach to the protection of consumer privacy throughout the economy is necessary to ensure that businesses have regulatory certainty in meeting their compliance obligations and that consumers are able to exercise their rights. CCIA appreciates, however, that in the absence of baseline federal privacy protections, state lawmakers are attempting to fill in the gaps. To inform these efforts, CCIA produced a set of principles to promote fair and accountable data practices.[2]

CCIA strongly supports the protection of consumer data and understands that Maine residents are rightfully concerned about the proper safeguarding of their data. To that end, we have outlined our thoughts on the questions that the Committee has requested feedback on.

(1) What are the benefits and drawbacks of including a private right of action in consumer data privacy legislation?

[1] For 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

[2] Computer & Communications Industry Association, *Considerations for State Consumer Privacy Legislation: Principles to Promote Fair and Accountable Data Practices* (January, 2022), https://www.ccianet.org/wp-content/uploads/2022/02/CCIA-State-Privacy-Principles.pdf

Including a private right of action in a privacy law would open the doors of Maine's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. Lawsuits also prove extremely costly and time-intensive – it is foreseeable that these costs would be passed on to individual consumers in Maine, disproportionately impacting smaller businesses and startups across the state. Additionally, studies have shown that law firms are the primary financial beneficiaries from biometric privacy-related lawsuits, as in the eight case settlements involving alleged harm to consumers in Illinois, plaintiffs' lawyers received an average settlement of $11.5 million per firm per case, while individuals received an average settlement of $506 per case.[3] Furthermore, by investing sole enforcement authority with the state attorney general, this allows for the leveraging of technical expertise concerning enforcement authority, placing public interest at the forefront.

(2) Should the Legislature enact standalone bills addressing biometric identifiers and health data in addition to enacting a comprehensive data privacy bill or should the Legislature address all types of consumer personal data in a single bill? Why?

As Maine has not yet passed a comprehensive consumer data privacy law, it would be advantageous to address all types of consumer person data in a single bill as it provides an opportunity to create a uniformed privacy framework in the state that can establish clear privacy standards and protections for businesses and consumers. By separating out certain aspects of data via the passage of standalone legislation, businesses and consumers may be left uncertain as to what standards are in place, and of course there may be unforeseen gaps in privacy protections, which could ultimately result in the legislature having to undertake additional legislative work to address those areas. By combining sensitive data, such as health and biometric data, into a comprehensive data privacy law (an approach that several other states, like Connecticut, have done), consumers and businesses are not burdened by potentially confusing piecemeal laws.

(3) How does the choice between an opt-in or an opt-out model for consumer consent to the collection/sharing/sale of personal data impact consumers?

Establishing a default "opt-in" approach will lead to consumer consent fatigue, ultimately creating a poor user experience online. The use of an "opt-in" approach should be limited to the processing or sale of a consumer's sensitive data (the first of which consumer consent is already required under bills like LD 1973). Extending an "opt-in" approach beyond those items would likely lead to "consent fatigue" amongst consumers, decreasing the utility of the actual control while also creating a worse user experience, where every internet webpage greets them with a consent request pop-up. Maine

[3]https://progresschamber.org/new-study-exposes-impact-of-illinois-biometric-privacy-law/

should follow the model of every other state that has passed a comprehensive state data privacy law, and utilize an opt-out model when it comes to the sale and processing of consumer data.

(4) Are there particular approaches to consumer data privacy in other states that you consider particularly valuable or problematic?

CCIA appreciates the manner by which Connecticut has set up their consumer data privacy law. Connecticut's law established several key privacy rights for consumers (right to access, correct, delete, portability, appeal, and right to opt-out of sale, profiling, or targeted ads), while also providing operators with clear responsibilities and adequate timelines to respond to consumer inquiries and sufficient on-ramp to bring themselves into compliance (just over 14 months). Additionally, Connecticut provided further privacy protections for several specific types of consumer data, as their definition of sensitive data included data pertaining to health, biometric information, geolocation, and childrens' data, among other items. The items falling under sensitive data require processors to obtain a consumer's consent to process these types of information. Additionally, Connecticut's data privacy law places sole enforcement authority with the Attorney General's office, removing the possibility of frivolous lawsuits flooding the state's legal system and enabling the expertise of the AG's office to go after bad-actors.

Connecticut's law has served as a model for other states in the Northeast, with states like Rhode Island, New Hampshire, and Vermont all considering comprehensive data privacy proposals that align with Connecticut's law, and there is the potential for the creation of essentially what would be a uniform data privacy standard throughout the New England region if states like Maine were to follow suit.

(5) What existing federal laws protect consumer personal data in your industry (or the industry of concern to you) – what types of data do those laws protect (or not protect) and what types of companies do they regulate (or not regulate)?

There are numerous sectoral laws that govern privacy in the privacy sector. The first national privacy law was passed in 1970 with the Fair Credit Reporting Act, which is tailored at information about consumer credit. In the subsequent years, various federal laws have been enacted granting agencies both general and specific authority to enforce laws concerning financial, medical, education, and workplace privacy. For example, the FTC has the general authority to enforce against unfair and deceptive trade practices, along with the specific authority to enforce the Children's Online Privacy Protection Act (COPPA) and others. Other agencies are often involved in the oversight and enforcement of these privacy laws including the Departments of Justice, State, Commerce, Homeland Security, and more. In addition to adhering to the relevant sectoral privacy laws, responsible private companies must also comply with important civil rights laws such as title VII of the Civil

Rights Act of 1964 and the Americans with Disabilities Act. Despite the rapid advancements in technology, consumers are still protected by these important civil right laws.

(6) Are there any pending Congressional proposals regarding consumer data privacy of which the Maine Legislature should be aware?

Currently, no. CCIA has long urged Congress to pass comprehensive, bipartisan privacy legislation that would protect all Americans. Last year, the bipartisan and bicameral American Data Privacy and Protection Act (ADPPA) represented a promising step toward achieving this goal but it has yet to be introduced. This act provided a workable framework to build upon. CCIA is hopeful for its re-introduction, so that Congress can pass comprehensive federal privacy legislation that creates a uniform national standard, preempts state law, and ends the privacy patchwork.

* * * * *

We appreciate the Joint Committee's consideration of these comments and stand ready to provide additional information as the Legislature considers proposals related to data privacy policy.

Sincerely,
Alexander Spyropoulos
Regional State Policy Manager - Northeast
Computer & Communications Industry Association

Charter
COMMUNICATIONS

Response of Charter Communications
October 17, 2023Re: Consumer Privacy Work Session
LD 1705, LD 1902, LD 1973 and LD 1977

Charter values and relies on the trust and loyalty of its more than 32 million residential and business customers. Our network provides competitively priced high-speed broadband, video, voice and mobile services across the country and in all regions of Maine, from Portland to the outer islands, from Aroostook to Southern Maine, and from Fortune 100 customers to small businesses.

Ensuring that the privacy of our customers is protected is very important to Charter. As Charter has expressed in testimony before the United States Congress and in this state house, among many others across the country, a comprehensive privacy framework should seek to empower and inform consumers in a uniform and consistent manner.

Charter has long advocated for five core principles that are critical to an effective privacy framework. Those principles are control, transparency, uniformity, parity, and security. Control means that consumers should be empowered to have meaningful choice regarding the collection and use of their data, most thoroughly through opt-in consent. Transparency stands for the idea that consumers should be given the information they need to provide informed consent. Uniformity means that the best way to make consumer protections effective, is for there to be a single national standard. Parity reflects the principles that consumers are best served by a uniform framework that is applied consistently across the entire internet ecosystem. And security means that strong data security practices are essential to promoting privacy.

Charter appreciates the opportunity to respond to the specific questions raised by the committee.

(1) What are the benefits and drawbacks of including a private right of action in consumer data privacy legislation?

Private rights of action can take many forms. To date, all state privacy laws across the country protect privacy through either a separate state agency or through enforcement by the state's Attorneys General. Even California does not afford a private right of action to consumers, except in a very limited set of circumstances involving data breaches. Since the California privacy law was enacted in 2020, 12 other states have passed comprehensive privacy laws without a private right of action, and there is good reason for doing so.

The purpose of any law is to encourage compliance with a set of principles. Inherent in any law are judgment calls as to what is most important. A private right of action allows individuals to

elevate technical, minor violations of a statute with minimal, if any, return or value in protecting a consumer's privacy. On the other hand, regulatory enforcement, with a right to cure, allows businesses to focus on addressing any problems identified by an attorney general or other expert official. Agencies of the state, who have individuals who are subject matter experts, and who know how to investigate and implement existing rules, laws, and regulations, offer the most cost-effective manner to enforce online privacy laws and to deter bad behavior. Instituting a private right of action benefits the plaintiff's bar more than consumers and does not actually result in the implementation or development of new or revised safeguards for data. Costly litigation creates greater uncertainty and may have the effect of stifling technological developments and service improvements.

(2) Should the Legislature enact standalone bills addressing biometric identifiers and health data in addition to enacting a comprehensive data privacy bill or should the Legislature address all types of consumer personal data in a single bill? Why?

The best approach to consumer privacy is uniformity and parity; addressing all data privacy considerations in a single comprehensive bill best protects consumers and gives certainty to businesses. Connecticut recognized this by amending its 2022 comprehensive law in 2023 to better protect health data, rather than adopting a new, separate law to deal with that specific data type. It is ultimately better for regulators, businesses, consumers, legislators, and courts to interpret a uniform framework than it is to try to piece together meaning from many disparate laws written at different times.

(3) How does the choice between an opt-in or an opt-out model for consumer consent to the collection/sharing/sale of personal data impact consumers?

Consumer control means that consumers should be empowered to have meaningful choice regarding the collection and use of their data.

While the best way to ensure consumer control over their data is through opt-in consent, any legal framework that is ultimately adopted should ensure consumer consent is purposeful, clear and meaningful. An opt-in provides consumers with the greatest control of their data, especially for sensitive data. But we also recognize that other states enacting privacy legislation have often chosen a different form of consent and there remains value in uniformity as well.

(4) Are there particular approaches to consumer data privacy in other states that you consider particularly valuable or problematic?

Charter sees significant value in the comprehensive approach taken by all thirteen states to have adopted general consumer privacy laws. We consider particularly valuable the approach that these states have taken on the core principles of uniformity and parity.

With the bills being considered during this work session, Maine has the opportunity to join those other states that have seen the benefit of comprehensively legislating consumer privacy rather than trying to do so piecemeal. 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.

Aligning with the principles of uniformity and parity should serve as guiding principles for any future legislation.

Uniformity means that online consumer protections are most effective when there is a single standard that applies across state borders. A patchwork of state laws can be confusing for consumers, and it is. A patchwork is also difficult for businesses to implement and hinders continued innovation. It is critical that states understand what each of the others is doing so as to avoid an inconsistent or, worse, contradictory set of online protections.

Of the bills being considered in this work session, LD 1973 is the best option for achieving uniformity. While LD 1973 is more consumer-protective than laws adopted in other states, it is still broadly compatible with them. LD 1973 differs from those other laws by imposing additional opt-in requirements where others impose only opt-outs. As previously mentioned, Charter is on the record as having long supported opt-in consent as the best way to ensure consumers' control over their data.

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. Of the bills being considered in this work session, only LD 1973 would achieve parity. While LD 1977 is also a comprehensive privacy bill, it both fails to bring the same protections to the rest of the internet ecosystem that apply to ISPs under LD 946 from 2019 and it adds contradictory requirements for ISPs who may be subject to both laws.

(5) What existing federal laws protect consumer personal data in your industry (or the industry of concern to you) – what types of data do those laws protect (or not protect) and what types of companies do they regulate (or not regulate)?

While there are a number of Federal laws that implicate privacy for certain kinds of data – such as financial or health data – there is no comprehensive, federal privacy standard that governs how Charter handles all of its consumers' data.

(6) Are there any pending Congressional proposals regarding consumer data privacy of which the Maine Legislature should be aware?

There are a number of proposals before Congress, which has not yet adopted a comprehensive federal privacy framework. On July 27, 2023, the Kids Online Safety Act (KOSA) and the Children and Teen's Online Privacy Protection Act (COPPA 2.0) were unanimously passed out of the Senate Commerce Committee. KOSA would require online platforms and services that are reasonably likely to be used by those 17 years old or younger to prevent and mitigate certain harms through the design and operation of their products and services and to include parental tools and disclosures. COPPA 2.0 would prohibit internet companies from collecting personal information from users that companies know or have fairly implied knowledge are 13 to 16 years old without their consent.

CR Consumer Reports®

October 11, 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: LD 1705, An Act To Regulate the Use of Biometric Identifiers—SUPPORT

Dear Chair Carney and Chair Moonen,

Consumer Reports[1] writes in support of LD 1705, an act to protect the privacy of biometric information. Though the collection and monetization of Maine consumers' personal data has dramatically expanded over the last thirty years, consumers have almost no say over whether their biometric information will be shared by a company with countless others. This important proposal will protect biometric information by default, ensure that consumers cannot be charged for protecting their data, and provides appropriate incentives for companies to comply.

Biometric data clearly warrants these additional protections. Collection and retention of such data leaves it vulnerable to unwanted disclosure, either intentional or otherwise. Biometric data is commonly used to confirm consumers' identity and can easily be exploited for identity theft and fraud purposes. Unlike a credit card number, the consumer's biometric information cannot be changed, making its unwanted disclosure all the more dangerous.[2] But concerns about inappropriate disclosure go far beyond its potential misuse for the purposes of fraud. Aside from the inherent privacy interest in keeping this information private, the disclosure of biometric

[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.

[2] Angela Chen, *Why a DNA Data Breach Is Much Worse than a Credit Card Leak*, The Verge (Jun. 6, 2018), https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics.

data—for example, of voice recordings—could lead to reputational or emotional harm. Particularly in light of the plethora of data breaches in recent years, biometric data should have these additional protections.[3]

We appreciate that the bill includes the following key protections:

- *Restrictions on collection without consent and a ban on sales.* Measures largely based on an opt-out model could require consumers to contact many different companies in order to fully protect their privacy—which simply isn't workable. Making matters worse, Consumer Reports has documented that some opt-out processes are so onerous that they have the effect of preventing consumers from stopping the sale of their information.[4] In contrast, LD 1705 would require that companies obtain consumers' written permission before collecting, using, or sharing their biometric data, and prohibits the onward sale of that data outright.

- *Non-discrimination.* We appreciate that the bill includes strong non-discrimination language that clarifies that consumers cannot be charged for exercising their rights under the law. Such protections are important: otherwise, privacy rights are only extended to those who can afford to pay for them.

- *Strong enforcement.* Importantly, the bill includes a private right of action to better ensure compliance. Under an AG-only enforcement framework, businesses that recognize that the AG is only capable of bringing a handful of enforcement actions each year might simply ignore the law and take their chances in evading detection. Further, it's appropriate that consumers are able to hold companies accountable in some way for violating their rights.

For these reasons, we urge you to secure key privacy protections for Maine consumers by voting in favor of LD 1705.

Sincerely,

Matt Schwartz
Policy Analyst

---

[3] See, e.g. *Data leak exposes unchangeable biometric data of over 1 million people*, MIT Technology Review, (Aug. 14, 2019), https://www.technologyreview.com/2019/08/14/133723/data-leak-exposes-unchangeable-biometric-data-of-over-1-million-people/.

[4] Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Rights Protected,* Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

October 11, 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: Maine L.D. 1902, Maine Health Privacy Legislation — *SUPPORT*

Dear Chair Carney and Chair Moonen,

Consumer Reports sincerely thanks you for your work to advance consumer privacy in Maine. L.D. 1902 would extend to Maine consumers important new protections relating to their personal health data, including prohibitions against collecting or sharing consumer health data without affirmative opt-in consent, a ban on data sales, the right to know the personal health data companies have collected about them and well as the right to delete that information.

Many companies that collect especially sensitive personal information, including personal health data, are failing to safeguard it. For example, a 2021 Consumer Reports investigation into seven of the leading mental health apps showed that they had significant privacy issues: many shared user and device information with social media companies and all had confusing privacy policies that few consumers would understand.[1] Similarly, the Federal Trade Commission has recently enforced against several companies that improperly shared personal health information with

[1] Thomas Germain, Mental Health Apps Aren't All As Private As You May Think, Consumer Reports, (March 2, 2021), https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/

third-parties or broke their privacy promises to consumers, including fertility tracker apps Flo[2] and Premom[3], online counseling service BetterHelp[4], and online prescription company GoodRx.[5]

Even when companies do not outright lie about their privacy protections, the hazy bounds of existing privacy law further complicate consumers' ability to understand company data practices. In a 2023 study headed by University of Pennsylvania researchers, 82% of consumers didn't realize that HIPAA does not apply to many health-related data in mobile apps.[6] As a result, many consumers share sensitive health information with businesses under the illusion that it has preexisting legal protections, when, in many cases, none exist.

Lawmakers need to remedy this imbalance. At a minimum, businesses should be required to transparently communicate to consumers when they are collecting and sharing health data, and this data should *only* be disclosed if consumers give an affirmative opt-in consent. While Consumer Reports would prefer a framework that prevents the collection *and* secondary use of personal health data for any purposes other than providing the service requested by the consumer, we are glad to see that L.D. 1902 includes strong protections that would improve consumer privacy.

In particular, we appreciate that L.D. 1902 includes:

- *A strong definition of consumer health data.* The definition of consumer health data included in this legislation covers key categories of personal information consumers may share with businesses that deserve additional protection, including among others, health conditions and interventions, biometric or genetic data, use or purchase of medication, and gender-affirming care.

---

[2] Federal Trade Commission, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others, (June 22, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google

[3] Federal Trade Commission, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order, (May 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc

[4] Federal Trade Commission, FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising, (March 2, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook

[5] Federal Trade Commission, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising, (February 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising

[6] Turow, J., Lelkes, Y., Draper, N. A., & Waldman, A. E, Americans Can't Consent To Companies' Use Of Their Data, (February 20, 2023), https://repository.upenn.edu/asc_papers/830/

- *Restrictions on collecting and sharing without consent and prohibition on sales.* L.D. 1902 requires that regulated entities obtain separate, specific consents to respectively collect and share consumer health data. It also bans the sale of consumer health data outright. Importantly, the bill requires that any consent to *share* consumer health data must be obtained separately from consent to *collect* consumer health data, which itself cannot be bundled into a general terms of service. However, we note that the distinction between sharing and selling is often blurry, and may be confusing to consumers. Instead of bifurcating sharing and sales into separate frameworks, we suggest prohibiting all data disclosures to third-parties unless reasonably necessary to provide the service.

- *Strong enforcement.* Given the AG's limited resources, a private right of action is key to incentivizing companies to comply and we appreciate that one is included in the bill. We strongly encourage legislators to retain this provision going forward. Under an AG-only enforcement framework, businesses that recognize that the AG is only capable of bringing a handful of enforcement actions each year might simply ignore the law and take their chances in evading detection. Further, it's appropriate that consumers are able to hold companies accountable in some way for violating their rights.

- *Prohibitions on geofencing.* Individuals should be able to receive in-person health care services without fearing that companies are tracking their visits and/or disclosing that information to additional third-parties. Potential uses or disclosure of such information could result in consequences that range from embarrassing to outright adversarial. For example, businesses could share healthcare visit information with insurance companies who could then use it as a basis to increase monthly premiums. Some third-parties may even disclose or be forced to disclose geofenced data with law enforcement. L.D. 1902 appropriately bans such activity.

We note one loophole that should be closed in order to provide Maine consumers with the protections they deserve:

- *Clarify that the non-discrimination provision means price or service discrimination.* While we appreciate that the bill prohibits regulated entities from discriminating against consumers that exercise their rights under this act, the term "discriminate" is not defined or otherwise explained, which could lead regulated entities from construing the term narrowly. For that reason, we urge the drafters to specifically include prohibitions against price and service discrimination. Additionally, the legislation should ensure that the non-discrimination provisions apply to *all* consumer rights under the bill, including those in Section 1350-R. We suggest the following language:

  (a) A business shall not discriminate against a consumer because the consumer

exercised any of the consumer's rights under Section 1350-Q or Section 1350-R, or did not agree to information processing for a separate product or service, including, but not limited to, by:

(1) Denying goods or services to the consumer.

(2) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(3) Providing a different level or quality of goods or services to the consumer.

(4) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

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

Sincerely,

Matt Schwartz
Policy Analyst

October 11, 2023

Information for the Joint Standing Committee on the Judiciary Regarding LD 1902, An Act to Protect Personal Health Data

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

We appreciate the opportunity to submit public comments regarding pending legislation LD1902, An Act to Protect Personal Health Data. This bill establishes, among many other protections, consumer rights with regard to consumer health data and defines obligations of regulated entities that collect, use and share consumer health data.

At findhelp, we believe that social care data (non-HIPAA protected information that details sensitive personal information, like referrals to food or housing resources), should also be a protected data class under LD1902. Below we outline our rationale, and appreciate your thoughts and consideration.

About findhelp:

Founded in 2010, findhelp (formerly Aunt Bertha), a Public Benefit Corporation, runs the largest social care network in the United States and has served more than 26 million Americans. Our mission is to connect all people in need with the programs that serve them with dignity and ease. As part of fulfilling this mission, we maintain **findhelp.org**, a free and anonymous search tool for self-navigation to free and reduced cost programs in every U.S. Zip Code. Our network is used by over 600 customers, including 250 health systems, 130 health plans, community health centers, and health departments in the U.S. to manage social care referrals, as well as tens of thousands of CBOs. With a network that includes at least 1,500 program locations in every U.S. county, findhelp's interoperable social care technology works with electronic health records (EHRs) and other Systems of Record (SoRs) to help clinicians and navigators seamlessly connect individuals' with free and reduced cost social care services.

The findhelp network in Maine brings together 3,760 community programs and major Maine-based healthcare organizations to address social care needs. Through customer platforms and our free public site, findhelp.org, our network reaches more than 26 million users across the country (including over 123,000 Maine users), connecting people with local programs and tracking outcomes.

Why we care about privacy legislation:

To date, there are no state or federal protections that directly address consumer social care data housed within systems such as ours when the data is created outside existing privacy frameworks such as HIPAA. This puts vulnerable Mainers at risk of their personal data being used or sold without their knowledge. As states like California lead the way in privacy with the strongest consumer protections in the country, many states, including Maine, have loopholes that put consumers at risk in an unregulated industry. LD1902 makes an incremental yet essential first step to protect clinical data, and we believe that social care data should also be protected within this framework.

Like other areas of health and wellness, the American social safety net is modernizing at an unprecedented pace. Millions of people are using technology every month to connect to social service providers, community organizations, and other forms of social care. They are sharing their most sensitive information at their most vulnerable moments to determine their eligibility for the help they need. We must be wary of those vendors and technology companies that are poised to take advantage of skirting privacy and consent in the name of health equity.

Our industry connects people to care in the most vulnerable moments of their life. **We owe it to the constituents we serve** to create uniform standards that protect their dignity and ensure their trust, so that when someone seeks out substance abuse counseling, domestic violence protection, or is facing homelessness or a mental health crisis, they know that their personal information is being treated with care and protection. Further, community-based organizations that provide social care find that trust is a critical part of effective relationship-building and service-delivery to the people they serve. Being able to reassure individuals that their private social care information is in their control is a powerful way to build that trust. Requiring closed-loop referral systems operating in Maine to meet the minimum privacy standards required in this bill will provide that reassurance and bolster that trust.

There is an existing precedent in states like New Hampshire, who passed Senate Bill 423 in 2021, and pending legislation in California - Assembly Bill 1011, which prevents the sale of private social care data.

We support and will help champion these and future efforts to close the privacy gap in the social care space, to ensure that constituents have transparency, control, and continued dignity in their journey to a better quality of life for themselves and their families.

Recommended language

Findhelp suggests including Social Care Information as a protected data set under LD1902.

Social Care definition language below:
"Social care" is defined as care, services, goods, or supplies related to an individual's social needs. Social care includes, but is not limited to, support and assistance for an individual's food stability and nutritional needs, housing, transportation, economic stability, employment, education access and quality, child care and family relationship needs, and environmental and physical safety.

"Social care information" is defined as any information, in any form, that relates to the need for, payment for, or provision of social care.

a. Social care information created or received by a HIPAA covered entity that meets the HIPAA statutory definition for "protected health information" shall always be handled in accordance with HIPAA and all related regulations

We appreciate the opportunity to hear your thoughts and concerns regarding this legislation and proposed additions for social care data privacy protections. Please feel free to reach out at any time to discuss.

Thank you,

Toby Landau

Regional Director, Government Relations

Findhelp

HOSPITALITY MAINE

Testimony of Nate Cloutier

Before the Joint Standing Committee on Judiciary
October 17, 2023

In Response to Consumer Data Privacy Questions

Senator Carney, Representative Moonen, and distinguished members of the Joint Standing Committee on Judiciary, my name is Nate Cloutier and I am providing these comments on behalf of HospitalityMaine. As a trade association, HospitalityMaine represents more than 1,300 restaurant and lodging establishments of all sizes across the state. Thank you for taking the time to meet as a Committee while the Maine Legislature is adjourned to continue discussion on these complex but very crucial pieces of legislation. As requested, our comments are in response to the six questions posed by the Judiciary Committee.

1. ***What are the benefits and drawbacks of including a private right of action in consumer data privacy legislation?***

While a private right of action (PRA) may serve as a helpful tool for individual consumers to seek redress from potential harms, HospitalityMaine opposes the inclusion of a PRA in consumer data privacy legislation for several reasons:

- A private right of action is often abused by unscrupulous trial lawyers who send endless demand letters to small businesses seeking damages for alleged violations that the business may or may not have actually committed. We have seen this type of practice occur in the form of patent trolls and ADA drive-by lawsuits, and would expect similar results within the data privacy sphere given that these types of laws are so nascent. While larger companies may be able to settle out of court and withstand a constant barrage of demand letters, these types of suits or potential suits can put many small businesses out of business.
- The ADPPA (referenced in Question #6) and other state data privacy bills that attempt to include a PRA have thus far been drafted in ways that ultimately only target Main Street businesses who do not typically buy or sell consumer data. While Main Street businesses are often the first party data collector, data privacy legislation should ensure that all industry sectors are covered and that there are no privacy loopholes that leave consumers unprotected when their personal data is handled by any business, including those downstream that the customer does not directly interact with. All of the companies involved in handling the chain of personal data should have legal obligations to protect it under a privacy law and honor consumers' privacy requests. On a similar note, data privacy legislation should not rely on private contracts to create those legal obligations between parties, particularly between businesses that vary greatly in size and bargaining power (i.e., Main Street businesses versus global service providers).

- Privacy responsibilities should not simply be shifted from one industry sector onto another – not only because that is an ineffective way to protect consumer information but also because it is manifestly unfair to businesses that bear the brunt of those burdens for what should be the other businesses' own obligations to the consumer. Because our members include small businesses, they know that all too often powerful businesses within the telecom and tech industry sectors may use their superior market position to shift what should be their responsibilities onto their clients, typically leaving Main Street businesses with outsized compliance burdens and costs on top of the threat of lawsuits from unscrupulous trial attorneys.

2. ***Should the Legislature enact standalone bills addressing biometric identifiers and health data in addition to enacting a comprehensive data privacy bill or should the Legislature address all types of consumer personal data in a single bill? Why?***

The Legislature should address all types of consumer personal data in a single comprehensive bill because state laws governing biometric data and health data have thus far been flawed and at the same time fail to address the larger issues inherent within the protection of consumer data:

- The Illinois Biometric Information Privacy Act (BIPA) was poorly drafted because the Illinois Supreme Court ruled earlier this year that a violation of the Act occurs each time a company misuses a person's biometric information, not just the first time, resulting in a potential $17 billion fine for White Castle. While biometric data is considered more sensitive in nature than other personally identifying information, it's clear that this type of result was not the original intention of the law.
- The Washington My Health My Data Act was also poorly drafted because the law goes far beyond the regulation of consumer health data, with definitions that make it potentially applicable to nearly any type of personal data. The law also creates substantive requirements unlike any other privacy law on the books, requiring opt-in consent for many common, and benign and beneficial, data uses, notice requirements including a separate and redundant privacy notice, and deletion requirements with virtually no exceptions. Given its overly broad nature and the inclusion of a PRA for any violations, we expect the legislation to be ripe for potential lawsuits against companies that likely were not intended to be covered entities.

3. ***How does the choice between an opt-in or an opt-out model for consumer consent to the collection/sharing/sale of personal data impact consumers?***

Opt-in models are inherently more privacy protective for consumers and their personal data, but can also create potential consumer fatigue as well as major headaches for businesses executing very simple transactions. For instance, a customer paying with a credit card should not have to affirmatively opt-in for the business to use his or her financial data for every single purchase because the customer already has the reasonable expectation that their financial information is being collected and shared with downstream business partners to execute the payment in a safe and secure way. Additionally, requiring consumers to "re-opt-in" to a company's loyalty program may cause more harm than good to both the business and the consumer since the consumer has already agreed to provide certain data to the business in exchange for discounted goods or services. Ultimately, a comprehensive data privacy law

should strike the right balance between when an opt-in vs. an opt-out is used for the collection/sharing/sale of personal data.

4. *Are there particular approaches to consumer data privacy in other states that you consider particularly valuable or problematic?*

The Virginia Consumer Data Protection Act and the Colorado Privacy Act serve as valuable models for data privacy legislation that sufficiently protects consumers and their data, holds all businesses within the digital ecosystem accountable for protecting consumer data, and provides their respective state AGs and district attorneys with sole enforcement power. The vast majority of new state data privacy laws have been modeled after these two laws because they are much more straightforward than the California model for both business and consumers. Most notably, the California law establishes the concept of a "financial incentive" around loyalty programs that creates undue burdens for companies merely trying to retain their customers' business and attract new customers through simple discounted services and offerings.

5. *What existing federal laws protect consumer personal data in your industry (or the industry of concern to you) – what types of data do those laws protect (or not protect) and what types of companies do they regulate (or not regulate)?*

- The Children's Online Privacy Protection Act (COPPA) imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. This law mostly applies to our members' advertising practices.
- The Gramm-Leach-Bliley Act (GLBA) requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. However, this law was passed in 1999 when the Internet was a much more nascent technology, and we believe that financial institutions ought to be included within any comprehensive data privacy legislation at the state and federal levels in order to modernize their data protection obligations.

6. *Are there any pending Congressional proposals regarding consumer data privacy of which the Maine Legislature should be aware?*

There have been several Congressional proposals regarding consumer data privacy over the last year:

- American Data Privacy and Protection Act (ADPPA) (H.R. 8152) – introduced and passed out of the House Energy and Commerce Committee last year, but the bill has not been reintroduced this Congress. This is mostly because the legislation does not provide sufficient federal preemption over the growing patchwork of state data privacy laws and includes a private right of action as the key enforcement mechanism (see arguments against a PRA in Question #1). The bill also includes flawed language that would prevent businesses from utilizing "first party" data for targeted advertising purposes and does not provide sufficient exemptions or safe harbor

mechanisms for small businesses to combat potential demand letters from trial lawyers seeking to abuse the PRA.

- Kids Online Safety Act (KOSA) (S. 3663) – introduced and passed out of the Senate Commerce Committee last year, awaiting a potential Senate floor vote this year. This bill sets out requirements for covered platforms (i.e., social networks, video streaming services, or other applications that connect to the internet and are likely to be used by minors) to protect minors from online harm, including requirements relating to (1) safeguards to restrict access to the personal data of minors, (2) tools to help parents supervise a minor's use of a platform, and (3) reporting of harm to minors from using the platform.

- Children and Teens Online Privacy Protection Act (COPPA 2.0) (S. 1628) – introduced and passed out of the Senate Commerce Committee last year, awaiting a potential Senate floor vote this year. This bill extends to minors (ages 12–16) privacy protections previously applicable only to children (ages 0–12) through COPPA and otherwise establishes greater online privacy protections for children and minors. A concern with this legislation is that it would utilize a "constructive knowledge standard" as opposed to the "actual knowledge standard" included by the original COPPA referenced above.

    - *Both of these kids' online bills may have lost some momentum as a result of the recent ruling in California blocking its California Age-Appropriate Design Code Act from taking effect due to concerns around First Amendment rights and regulating behavior that takes place outside of the state.*

Thank you for your attention to this matter. Should you have any questions following today's meeting I can be reached at the contact information below.

Sincerely,

Nate Cloutier, Director of Government Affairs
HospitalityMaine
45 Melville Street
Augusta, ME 04330

E: Nate@hospitalitymaine.com
P: (207) 623.2178

October 17, 2023

Hon. Anne Carney, Senate Chair
Hon. Matthew Moonen, House Chair
Joint Standing Committee on Judiciary
100 State House Station
Augusta, Maine 04333-0100

Re: Invitation to Provide Comments to Specific Questions related to 10/17/2023 Working Session on privacy bills: LD 1705, LD 1902, LD 1973, and LD 1977

Dear Sen. Carney and Rep. Moonen,

Please accept the following responses to questions about consumer data privacy posed by the Committee.

(1) What are the benefits and drawbacks of including a private right of action in consumer data privacy legislation?

A private right of action will open Maine businesses to potentially frivolous lawsuits. Rather than defend a meritless suit, Maine consumers would benefit from businesses spending that time and money on providing a better customer experience regarding consumer preferences that meets customers' expectations and is responsive to their concerns.

L.L.Bean fully supports granting state regulators, such as the Attorney General, with robust enforcement authority to ensure businesses are in compliance. Providing consumers with a "right to appeal" (a right offered to consumers in several state privacy laws) provides necessary insight to the Attorney General and still results in businesses being held accountable.

It will take time for businesses to become fully compliant and inadvertent minor infractions disputed via the court system could potentially cripple a Maine business.

(2) Should the Legislature enact standalone bills addressing biometric identifiers and health data in addition to enacting a comprehensive data privacy bill or should the Legislature address all types of consumer personal data in a single bill? Why?

The approach being taken by the existing state legislative models is to include biometrics and health information in the definition of "Sensitive Personal Information" within the state's comprehensive data privacy bill. This results in a heightened standard of collection

and retention for those pieces of information. It also streamlines the compliance measures taken and reduces the chance of conflict or confusion.

(3) How does the choice between an opt-in or an opt-out model for consumer consent to the collection/sharing/sale of personal data impact consumers?

The opt-out approach has been adopted by every U.S. state with a comprehensive consumer privacy law. The exception is Sensitive Personal Information. Businesses must obtain opt-in consent for the collection of SPI, limit its use to specific purposes, and accept opt-out requests if the use of that SPI goes beyond those defined purposes.

Maintaining consistency is helpful for both businesses in terms of compliance and consumers in terms of expectations.

Additionally, an opt-in approach may cause confusion regarding a customer's various choices that vary site-by-site and frustrate the customer during their shopping experience.

(4) Are there particular approaches to consumer data privacy in other states that you consider particularly valuable or problematic?

There are a few good state models. Connecticut's model offers a balanced approach, resulting in fair treatment of both businesses and consumers.

Not including a right to cure is problematic to businesses that learn how to interpret a comprehensive consumer privacy law, in part, based on the Attorney General's enforcement.

(5) What existing federal laws protect consumer personal data in your industry (or the industry of concern to you) – what types of data do those laws protect (or not protect) and what types of companies do they regulate (or not regulate)?

The FTC Act provides relevant standards and enforcement. However, we agree that now is the time for Maine to pass a comprehensive consumer privacy law accounting for the now standard rights offered by existing state models (inform, correct, delete, access, opt-out, and appeal).

(6) Are there any pending Congressional proposals regarding consumer data privacy of which the Maine Legislature should be aware?

We do not believe that Maine should wait for the Federal government to act on this topic.

The L.L.Bean privacy team is willing to be a resource for any future questions or conversations regarding this important issue. Our goal is to support Maine's legislators in passing a successful privacy bill in our home state.

Sincerely,

Christy Van Voorhees, Esq.
Senior Associate Counsel
Co-Chair, L.L.Bean Data Privacy Leadership Team

PretiFlaherty

Portland, ME
Augusta, ME
Concord, NH
Boston, MA
Washington, DC

Bruce C. Gerrity
bgerrity@preti.com
207.623.5300

October 11, 2023

Sen. Anne Carney, Chair
Committee on Judiciary
Cross Building, Room 438
Augusta, ME 04330

Rep. Matt Moonen, Chair
Committee on Judiciary
Cross Building, Room 438
Augusta, ME 04330

RE: LD 1705, An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data;

LD 1902, An Act to Protect Personal Health Data;

LD 1973, An Act to Enact the Maine Consumer Privacy Act;

LD 1977, An Act to Create the Data Privacy and Protection Act

Dear Senator Carney and Representative Moonen,

The Maine Automobile Dealers Association ("MADA" or "the Association") will attend the work session on the above-referenced privacy bills. MADA anticipates that in-person oral testimony will be provided by Anne Sedlack, Esq. and/or Diane Johanson of the firm of Preti Flaherty.

MADA provides information on specific questions below:

1. The Association sees no benefit to providing a private right of action. The notion is punitive in nature, particularly regarding the proposed breadth and scope of damages and punitive damages, as well as attorney's fees. The drawbacks to a private right of action are numerous. These actions will clog Maine courts. The cost of opening floodgates to the courts will require a significant appropriation, especially given the technical nature of many of the statutory provisions. Well-meaning businesses will involuntarily fall afoul of one or more complicated provisions of these laws and be subjected to financially crippling litigation, as well as taking invaluable time away from various business operations to try and respond to the allegations. Relationships between employers, employees and customers will deteriorate. There will be businesses that leave Maine for a less hostile business environment. In addition, the rights of consumers are now protected by various other statutes already in place (such as the Maine Unfair Trade Practices Act, Title 5, §206, et seq.) now protecting privacy. See response to Question 5. To the extent enforcement provisions are included in any of these bills the Attorney General's Office has numerous skilled attorneys more capable of impartial and judicious decision-making as to what businesses and avenues to pursue. The expertise of the AG's Office will also help to lessen litigation.

2. Maine already has a plethora of laws addressing various data privacy requirements. An attempt to put all kinds of consumer personal data into a single bill would involve rewriting a number of provisions throughout the Maine statutes, including, for example, privacy protections associated with insurance data, consumer transactions governed by the Bureau of Consumer Credit Protection and banking laws governed by the Bureau of Banking. In addition, the nature of rights provided to consumers vary tremendously from statute to statute, including, for example, rights under the Unfair Trade Practices Act, rights under the Insurance Code, rights under federal laws and regulations, and rights associated with Maine's Data Breach statutes. Under the circumstances, it is not clear how all of these various statutes, situations and rights could be dovetailed into what one might call a "comprehensive data privacy bill." These differing provisions are in place to address specific concerns with each law. Simply put, one size does not fit all. In the event the Committee decides to report out a biometric identifiers bill, given the unique and quickly changing nature of biometrics such legislation should be stand-alone. With regard to health data, the various provisions in Titles 22, 24 and 24-A, dealing with health insurance and health data, as well as federal statutes such as HIPAA, should not be combined with other kinds of privacy acts.

3. Transactions involving automobiles already address the collection, sharing and sale of consumer information. The Association supports opt-out models, where information is provided to consumers unless they specifically opt-out from receiving such information. This kind of information is valuable to automobile consumers in a variety of ways, impacting issues such as safety, options and opportunities to improve the performance of a vehicle or parts and general information about their vehicles. Individuals who do not want to receive this kind of information or provide access to it can opt-out either at the outset or after a period of time after experience with receiving such information. In this fashion, consumer information, disclosures and options are maximized. Since opt-out information does not mandate a response or obligation, such information can only broaden a consumer's knowledge, which works to a consumer's advantage in the purchase or ongoing utilization of a vehicle often costing tens of thousands of dollars.

5. There are numerous federal laws which already protect various aspects of consumer and employee privacy rights involving automobile sales and service. Rules and statutes outlined below all relate to a greater or lesser extent to consumer records, consumer information, disclosure requirements, security requirements involving aspects of consumer information, securing information in a transaction, determining if the individuals in a transaction are who they are supposed to be, and providing various protections involving privacy and disclosure. Several of these laws and regulations include:

- Electronic Deposit of Taxes and Electronic Records Retention in relation to personal and corporate IRS data maintenance records
- Mail, Internet or Telephone Order Merchandise Rule

- Uniform Services Employment and Reemployment Rights Act (governs among other things rights of military members in certain consumer purchases as well as employment and reemployment rights, which often involve personal and private information)
- Military Lending Act (protecting members of the military in consumer transactions)
- Driver's Privacy Protection Act
- Electronic Funds Transfer Act
- FTC Privacy Rule (providing information about privacy policies, what is disclosable restrictions on disclosure of non-public, personal information in a variety of ways)
- FTC Safeguards Rule (which establishes standard for dealers to ensure the security of consumer data)
- FTC Prohibition Against Deceptive and Unfair Trade Practices (which is, as with a number of these statutes and rules, extremely broad)
- FTC Rules and Regulations (particularly regarding unfair and deceptive practices, centering in part on disclosure requirements)
- FTC Telemarketing Sales Rule
- FTC Warranty Rules
- IRS Cash-Reporting Rule (reporting certain transactions with a cash limit that allows the federal government to track payments for a variety of reasons, including but not limited to terrorism activities)
- USA Patriot Act (dealers must search records and disclose information about individuals or entities if requested by the federal Financial Crimes Enforcement Network)
- Magnuson Moss Act (related to warranties and service contracts)
- Telephone Consumer Protection Act (requiring express written consent prior to any text message or prerecorded or auto-dial telemarketing call to a cellphone; it also establishes broad national and company-specific do-not-call rules, time restrictions and various other requirements associated with advertising rules)
- FTC Cooling Off Rule (relating to transactions)
- FTC Used Car Rule
- Monroney Sticker Disclosure Requirements
- National Highway Traffic Safety Administration Odometer Rule
- National Highway Traffic Safety Administration Recall Regulations

- Dodd-Frank Financial Reform Law
- Consumer Finance Protection Bureau Rules and Regulations
- Equal Credit Opportunity Act (ECOA) and regulations (prohibiting discrimination)
- Fair and Accurate Credit Transactions (FACT) Act of 2003 (amending the Fair Credit Reporting Act (FCRA) in part related to identity theft and accuracy, security and reliability of protected financial information)
- Fair Credit Reporting Act
- FTC Credit Practices Rule
- Truth-In-Lending and Consumer Leasing Acts
- Family Medical Leave Act (privacy rights associated with exercising medical and family leave)
- CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act)
- Affordable Care Act (employee privacy with regard to healthcare)
- Health Insurance Portability and Accountability Act (contains privacy provisions associated with denial of coverage for healthcare and in relation to preexisting conditions)
- Consolidated Omnibus Budget Reconciliation Act (COBRA) (again relating to private healthcare information)
- Mental Health Parity Act
- Newborn and Mothers Health Protection Act (again relating to healthcare information)
- Occupational Safety and Health Administration Injury and Illness Recording and Reporting Requirements

This list of 36 statutes and regulations are duplicated in several state Titles, including Titles 5, 10, 11, 22, 24 and 24-A; these bills add more confusing and obscure statutes in relation to the automobile industry. For example, information that these bills would make confidential or subject to limits on disclosure must mandatorily be reported in a used car transaction in relation to prior owners, type of use and contact information under 10 M.R.S. §1475(2-A)(B).

In short, these bills only add more white noise to providing consumers with clear and comprehensive privacy and disclosure laws.

MADA appreciates this opportunity to have provided comments on several of the questions before the Committee.

Respectfully submitted,

Bruce C. Gerrity

cc: Susan Pinette, Committee Clerk

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

Date: Tuesday October 17, 2023

Subject: Privacy Legislation

The League appreciates the opportunity to weigh in on the multiple privacy bills offered this session. Please find below answers to the questions posed by the analyst.

(1) What are the benefits and drawbacks of including a private right of action in consumer data privacy legislation?

A private right of action opens up extensive litigation for potential violations and increases operating costs of any business that holds any type of consumer data. A private right of action has the potential to lead to significantly higher costs for businesses, regardless of their compliance with the law. For risk-adverse industries, especially cooperative business models like credit unions, the majority of cases will settle long before reaching court, regardless of wrongdoing. Settlement is not an admission of guilt, but allows the business to control more factors than they can at court and can avoid risking significant penalties and reputation risk from a court case. In addition, since private rights of action in the privacy sphere are generally not limited to actual damages and may be brought on behalf of a class, the costs can quickly become exponential when inclusive of statutory damages, punitive damages, and attorney's costs.

(2) Should the Legislature enact standalone bills addressing biometric identifiers and health data in addition to enacting a comprehensive data privacy bill or should the Legislature address all types of consumer personal data in a single bill? Why?

A comprehensive privacy bill simplifies compliance for organizations looking to conduct business in Maine. Individual bills for types of data or types of organization decentralizes the statutory requirements making it more difficult for

both consumers looking to exercise their rights as well as for businesses looking to comply with the laws of Maine.

A patchwork of privacy laws is disadvantageous to both consumers and businesses. Data freely flows across jurisdictions, having disparate laws creates a high burden for compliance and leaves individuals and their data vulnerable. A comprehensive bill that is substantially similar to laws in other states would make Maine well positioned to protect consumers and allow businesses to operate successfully in Maine.

(3) *How does the choice between an opt-in or an opt-out model for consumer consent to the collection/sharing/sale of personal data impact consumers?*

Opt-in models result in increased emails, phone calls, and physical mail for those organizations who look to obtain data or information about their users. Opt-in regulations are inefficient, as the majority of people are willing to share their private personal information without regard to privacy concerns. None of the states that have passed comprehensive consumer privacy laws have included an opt-in model, except for personal data for children under a certain age.

(4) *Are there particular approaches to consumer data privacy in other states that you consider particularly valuable or problematic?*

Exemptions for Fair Credit Reporting Act information and for financial institutions under the Gramm-Leach-Bliley Act would provide continuity across states and avoid potential conflicts with federal laws.

(5) *What existing federal laws protect consumer personal data in your industry (or the industry of concern to you) – what types of data do those laws protect (or not protect) and what types of companies do they regulate (or not regulate)?*

Financial institutions are governed federally by two pieces of legislation relating to privacy. The first, and more comprehensive, is the Gramm-Leach-Bliley Act or GLBA. GLBA broadly covers financial institutions, such as banks and credit unions; investment companies; investment advisors; brokers; dealers; and those providing insurance services. Institutions governed by GLBA are required to inform customers and consumers of third-party sharing and give them the right to opt out of third-party information sharing by the financial institution. In addition, GLBA generally prohibits the sharing of nonpublic personal information to a

nonaffiliated third parties.[1] This prohibition includes the sharing of account numbers and similar numbers for marketing purposes.[2] There are exemptions for financial institutions for the sharing of information at the bequest of the consumer or with affiliated third parties who may act as vendors, for example, financial institutions may use a third-party vendor to print and distribute periodic account statements, in which case, some nonpublic personal information may be shared for the purposes of mailing the statements.

GBLA provides a specific exemption on sharing nonpublic personal information for the purpose of protecting the confidentiality or security of financial records or for the use of protecting against fraud.

Financial institutions are furnishers and users under the Fair Credit Reporting Act (FCRA). There is significant societal value to having a full picture of a consumer's credit history, a more complete credit report allows credit to be more available and to reduce risk. Furnishers are required under federal law to report certain personal information. Without an exemption for personal information shared under FCRA, the credit reporting system would be subject to the same right of deletion and restrictions on sharing as all other personal information, making it extremely difficult to rely on the information in a credit report. Furthermore, the organizations that are obligated under federal law to furnish accurate information to credit reporting agencies would be placed in the unfortunate situation of being in violation of either state or federal law. All of the states that have adopted comprehensive privacy laws have an exemption for FCRA information.

(6) *Are there any pending Congressional proposals regarding consumer data privacy of which the Maine Legislature should be aware?*

None at this time.

---

[1] 15 U.S.C. § 6802(a).
[2] 15 U.S.C. § 6802(d).

Comment on Privacy Legislation

LD 1705, LD 1902 and LD 1977

October 17, 2023

Chair Carney, Chair Moonen, Honorable Members of the Judiciary Committee: The following comments are submitted on behalf of the Maine Hospital Association, the Maine Medical Association, the Maine Osteopathic Association, the Maine Health Care Association, the Maine Ambulance Association, the Maine Society of Anesthesiologists and Spectrum Healthcare Partners.

We request that health care entities be given the same exemption from LD 1705, LD 1902 and LD 1977 as has been proposed for government entities.

As you know, hospitals and other health care providers routinely collect the kinds of data covered by these bills. Health care providers are governed by extensive state and federal regulation; HIPAA is not the only health care privacy law. (*See*, for example, 22 MRS Section 1711-C: Confidentiality of Healthcare Information.) Our members and other healthcare providers have worked diligently, for decades, to develop systems of compliance with the existing regulatory structure. These bills present completely new structures for us. It will be unduly burdensome for health care providers to have to comply with these new laws in addition to long-standing state and federal laws.

A review of the previously submitted testimony on these bills makes evident that Maine hospitals and other healthcare providers are not the problem identified by the proponents of the legislation. The three examples given over and over again by proponents are internet searches, cell phone apps and wearables, such as smart watches, which are alleged to be out of the reach of HIPAA and the other existing laws. These are commercial interactions that are not part of traditional healthcare services. The entities that

might need to share personal health information to sign business associate agreements. In those agreements, the outside entities agree to be bound by HIPAA and federal and state privacy laws.

This committee has a record of not imposing new regulations in the absence of a clear showing by proponents of a problem. The proponents did not meet their burden here with respect to traditional healthcare providers. No evidence has been offered that healthcare entities in Maine are doing anything wrong. If there are concerns, existing Maine laws could be used to address such issues.

Please exempt health care entities to the same extent that government entities are proposed to be exempt from these three bills.

Thank you.

MaineHealth

Testimony of Sarah Calder, MaineHealth
In Opposition to LD 1902, LD 1977, and LD 1705
October 17, 2023

Senator Carney, Representative Moonen, and distinguished members of the Joint Standing Committee on Judiciary, I am Sarah Calder, Senior Government Affairs Director at MaineHealth, and I am here to share our significant concerns with the several privacy bills before you today.

MaineHealth is an integrated non-profit health care system that provides a continuum of health care services to communities throughout Maine and New Hampshire. Every day, our over 22,000 care team members support our vision of "Working Together so Our Communities are the Healthiest in America" by providing a range of services from primary and specialty physician services to a continuum of behavioral health care services, community and tertiary hospital care, home health care and a lab.

Consistent with our mission and vision – and in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and other state and federal regulations – MaineHealth is committed to ensuring the privacy of our patients and maintaining the confidentiality of their information and medical records. As an already highly regulated entity, we would ask that health care providers be clearly exempted from LD 1705, LD 1902, and LD 1977.

Based on the testimony this Committee has received as well as the debate occurring in state legislatures across the country, health care providers are clearly not the intended target of the new proposed regulations. With that said, however, should the Committee not pursue a blanket exemption for health care providers, MaineHealth would ask that the Committee include the following amendments:

LD 1902:

- Exclude health care information from "consumer health data" on p. 2:
    - "Consumer health data" does not include health care information, as defined in Title 22, section 1711-C, subsection 1, paragraph E, obtained for health care, as defined in Title 22, section 1711-C, subsection 1, paragraph C;
- MaineHealth is in the process of utilizing geofencing to allow patients to more easily and quickly check-in to their health care appointments, and we would ask that health care facilities be excluded from the geofencing prohibition on p. 10. The language was also adopted by the New York General Assembly:
    - "It shall be unlawful for any person, corporation, partnership, or association to establish a geofence or similar virtual boundary around any health care facility, other than their own health care facility, when the geofence is used to identify, track, collect data from or send notifications or messages to a consumer that enters the virtual perimeter.
- MaineHealth requires certain care team members to use biometric identifiers to access its networks, clinical and business information systems, and software applications. For example, biometric identifiers are used to access secure medications and medical supplies

to prevent misuse. The technology uses numeric algorithmic expressions generated from biological characteristics that alone could not be used to re-identify those biological characteristics. With that said, we would ask the Committee to revise the definition of "biometric data" on p. 1. This language has been adopted in other states, including Washington and Florida:

- "Biometric identifier" does not include a physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996.

LD 1977:

- Exclude HIPAA protected information:
  - "This chapter does not apply to protected health information collected, used or disclosed in accordance with the federal Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act and 45 Code of Federal Regulations, Parts 160 and 164 and implementing regulations."
- Exclude health care information from "Covered data" on p. 1:
  - "Covered data" does not include health care information, as defined in Title 22, section 1711-C, subsection 1, paragraph E, obtained for health care, as defined in Title 22, section 1711-C, subsection 1, paragraph C;
- As with LD 1902, we would ask the Committee to revise the definition of "Biometric information" on p. 1:
  - ", or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996."

LD 1705:

- As with the previous two bills, we would ask the Committee to revise the definition of "biometric identifier" on p. 1:
  - "J. Information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996"
- As mentioned above, MaineHealth requires certain care team members to use biometric identifiers to access its networks, clinical and business information systems, and software applications. These care team members are required to sign consent and authorization forms, which describes our policies, but in order to perform their jobs and access, for example, certain medications and medical supplies, they must provide consent. It is important to note that we do not sell or lease this information to third parties, and we have a policy to permanently destroy the data. With that said, we would ask the Committee to revise the section on "Affirmative written consent" on p. 3:
  - "Uses of affirmative written consent. A private entity may only use the affirmative written consent regarding a biometric identifier of an employee of the private entity to permit access to a secure physical location, medications or medical supplies, or secure computer hardware or software and to record the beginning and end of the employee's work day and meal or rest breaks. ~~The~~

~~private entity may not retain biometric identifier related to access for the purpose of employee tracking.~~

- "Affirmative written consent may be given by electronic means. A user interface may not influence an individual toward giving affirmative written consent, and any default settings in a user interface must be designed to have as a default setting the option not to give affirmative written consent, unless it is a condition of employment."

It is important to note that we have done our best to review all three bills and identify areas that would significantly impact our ability to provide patient care, but because of the substantial scope of these bills and the completely new regulatory structures they would impose, there may be areas that we did not consider. With that said, we ask that the Committee exempt health care entities that are already highly regulated both at the federal and state levels.

Thank you and I would be happy to answer any questions you may have.

Janet T. Mills
Governor

Michael J. Sauschuck
Commissioner

STATE OF MAINE
Department of Public Safety
MAINE STATE POLICE
45 Commerce Drive - Suite 1
Augusta, Maine 04333

COL. Bill G. Ross
Chief

LTC. Brian P. Scott
Deputy Chief

Testimony of Lieutenant Jason Richards
Maine State Police

Neither for nor Against LD 1705, LD1902, LD1973 and LD 1977

- LD 1705, An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data (Rep. O'Neil)
- LD 1902, An Act to Protect Personal Health Data (Rep. O'Neil)
- LD 1973, An Act to Enact the Maine Consumer Privacy Act (Sen. Keim)
- LD 1977, An Act to Create the Data Privacy and Protection Act (Rep. O'Neil)

Joint Standing Committee on Judiciary

Senator Carney, Representative Moonen and other distinguished members of the joint standing committee on Judiciary. My name is Lieutenant Jason Richards. I oversee the Maine State Police Computer Crimes Unit and I am the commander of the Northern New England Internet Crimes Against Children Task Force. I am here representing the Maine State Police and the Department of Public Safety and to offer testimony neither for nor against LD1705, LD1902, LD1973 and LD1977.

We recognize these bills are not addressing a law enforcement concern. We thank the sponsors for including language regarding processing of information from the National Center in regard to child exploitation tips and other language regarding companies complying with legal process. We are hoping that language might be amendable to be a little more clear. By clarifying the phrasing and location of the need for companies to comply with properly obtained legal process from law enforcement and the courts in general, we hope companies will be less concerned or confused about potentially violating any of this legislation. Currently the restrictions on what companies can do with data and the location of the exceptions to that are separated in the bills causing confusion as to which parts those exceptions are applicable. The language within those exceptions is vague and does not highlight specifically that information needs to be shared with law enforcement pursuant to properly obtained legal process documents i.e.; subpoena or search warrant as outlined in current state and federal law. Putting those exceptions in the same sections where sensitive data is defined and restricted along with more specific language would help to clarify the requirement to continue to comply with legal process from law enforcement and others.

Thank you for your consideration.

NATIONAL INSURANCE CRIME BUREAU

Leading the Fraud Fight

For WS
LD 1902

October 16, 2023

The Honorables Anne Carney and Matt Moonen and Members of the Joint Committee
Joint Committee on Judiciary
Maine Legislature

RE: L.D. 1902 (H.P. 1217) – My Health Data Act

Dear Chairs Careny, Moonen, and Members of the Joint Committee:

I am writing to address concerns with Legislative Document 1902 (H.P. 1217), as amended, regarding consumer health data protection. As written, the bill would pose serious hardships on the ability of our organization, the National Insurance Crime Bureau ("NICB") to combat insurance fraud.

Organization and Business Purpose

Headquartered in Des Plaines, Illinois, and with a 110-year history, the NICB is the nation's premier not-for-profit organization exclusively dedicated to leading a united effort to prevent insurance crime and fraud through intelligence-driven operations. NICB is primarily funded by assessments on our nearly 1,200-member property-casualty insurance companies, car rental companies, and other strategic partners.

NICB sits at the intersection between the insurance industry and law enforcement, helping to identify, prevent, and deter fraudulent insurance claims. NICB's approximately 400 employees work with law enforcement entities, government agencies, prosecutors, and international crime-fighting organizations in pursuit of its mission.

NICB maintains operations in every state around the country, including in Maine where NICB is an unmatched and trusted partner in the fight against insurance fraud. NICB analysts and agents work daily with state and local Maine law enforcement and regulatory agencies to provide assistance in all manner of cases. NICB maintains close agency relationships that can directly speak to NICB's value, including: the Bureau of Insurance, Office of the Attorney General, Division of Insurance, Maine State Police, Bureau of Motor Vehicles, federal agencies, including the Federal Bureau of Investigations, Portland Police Department, and many other local police and prosecuting agencies.

Maine's Insurance Fraud Reporting Requirements

Recognizing the adverse impact of insurance crime on the citizens of Maine, the legislature enacted laws requiring Maine insurers to report suspected fraudulent claims to the Bureau of Insurance.[1] The vast majority of suspected fraud cases are reported to NICB through NICB's Fraud Bureau Reporting Program. In partnership with the National Association of Insurance Commissioners, that information is made available to Maine's Bureau of Insurance. Recognizing the critical nature of information

[1] 24-A M.R.S. § 2186; 25 M.R.S. § 2412.

sharing related to insurance fraud, the Maine Legislature has afforded protection from civil liability to those who share insurance fraud information.[2]

Maine's Insurance Information and Privacy Protection Act

Additionally, as an insurance-support organization, NICB is a regulated entity under Maine's Insurance Information and Privacy Protection Act which imposes strict limitations as it relates to the collection, use, and disclosure of personal consumer information, and provides remedies for violations of the Act.[3]

Applicability of L.D. 1902

Unlike similar bills, Legislative Document 1902 provides no exemption to prevent, detect, protect against, respond to, investigate, report or aid in the prosecution of malicious, deceptive or illegal activities, security incidents, identity theft, fraud or harassment. As a result, NICB data used for fraud-fighting purposes and already regulated by the state's Insurance Information and Privacy Protection Act would be left completely exposed and subject to the requirements of the My Health Data Act, including requested deletion of data by criminals in order to purposely evade investigation and prosecution.

Proposed Change and Policy Rationale

Consistent with longstanding public policy determinations already considered and enacted in Maine law, NICB respectfully requests a broad-based fraud exemption and an amendment to ensure NICB's wholesale exemption from the Act by including insurance-support organizations as exempted entities.

Again, the disclosure by an insurance-support organization of personal consumer information is already heavily restricted by Maine law, and absent a carveout, our ability to facilitate information sharing with Maine governmental agencies and conduct criminal investigations will be severely hampered.

We appreciate your consideration of our concerns. We welcome the opportunity to follow up directly with your staff to discuss these issues in more detail. In the meantime, if you have any questions or need additional information, please contact me at hhandler@nicb.org or 312-771-3974.

Sincerely,

Howard Handler

Howard Handler, MPPA
Senior Director
Strategy, Policy, and Government Affairs

[2] 24-A M.R.S. § 2187; 24-A M.R.S. § 2218; 25 M.R.S. § 2412.
[3] 24-A M.R.S., Chapter 24.

2211 Congress Street
Portland, ME 04122
207 575 2211
unum.com

October 10, 2023

Re: Invitation to Provide Comments to Specific Questions related to 10/17/2023 Work Session on LD 1705, LD 1902, LD 1973 and LD 1977

Chair Carney, Chair Moonen and Members of the Judiciary Committee –

Unum writes to share our perspective as a large Maine business and employer operating nationally across all 50 states. As such, we have gained experience and expertise in recent years as several states have debated comprehensive privacy legislation. As a highly regulated financial services entity, Unum's perspective is shaped by the fact that we have long complied with numerous state and federal privacy laws, namely the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA), among others.

(1) What are the benefits and drawbacks of including a private right of action in consumer data privacy legislation?

- A private right of action, especially an open-ended one that applies to "any violation" of a statute, can result in broad damages without demonstration of any harm to any person.
- A private right of action presents such significant risk to companies that it may preclude the use of consumer-friendly technology entirely, such as biometric authentication or voice assistance and translation.
- By usurping the power of regulators to enforce these laws, the PRA would encourage meritless suits to be brought against companies to try to obtain quick settlements in light of the extreme potential exposure.
- Under the current PRA proposal, there are myriad examples of inadvertent violations leading to massive, crippling damages to Maine businesses.

(2) Should the Legislature enact standalone bills addressing biometric identifiers and health data in addition to enacting a comprehensive data privacy bill or should the Legislature address all types of consumer personal data in a single bill? Why?

- The comprehensive approach has been taken by most states that have recently addressed consumer privacy through legislation, and that approach promotes uniformity and clarity for the consumer. It does so in a way that maintains relevant existing exemptions (i.e. health, financial services, information obtained through the employment context, etc.) under one comprehensive standard.
- This approach avoids having competing or conflicting obligations related to a consumer's personal information. If each law is separated out, the obligations will need to be harmonized given that some types of information would be subject to multiple laws.

(3) How does the choice between an opt-in or an opt-out model for consumer consent to the collection/sharing/sale of personal data impact consumers?

- Consumers are familiar with the opt-out model, as it has been adopted by nearly all states in most contexts. Opt-in may be appropriate for more sensitive, risky, or hidden processing of PII.

(4) Are there particular approaches to consumer data privacy in other states that you consider particularly valuable or problematic?

- The comprehensive bills adopted by Connecticut, Virginia, Colorado, Delaware, Montana, Utah, and Iowa are reasonable approaches that balance the needs of consumers and businesses, by including financial services exemptions and taking into account exemptions for information obtained within the employment context (i.e. benefits).

(5) What existing federal laws protect consumer personal data in your industry (or the industry of concern to you) – what types of data do those laws protect (or not protect) and what types of companies do they regulate (or not regulate)?

- Gramm-Leach-Bliley: which regulates all data collected or processed in the course of providing certain financial services
- HIPAA: which regulates PHI in the possession of covered entities.
- Fair Credit Reporting Act: regulates the use of consumer reports and related PII.

(6) Are there any pending Congressional proposals regarding consumer data privacy of which the Maine Legislature should be aware?

- Not at this time. Federal legislative proposals are yet to advance, which has given way to significant activity at the state level.

Sincerely,

Umberto Speranza
AVP, Government Affairs
Law Department
Unum Group

Planned Parenthood® of Northern New England

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

(1) What are the benefits and drawbacks of including a private right of action in consumer data privacy legislation?

A private right of action is essential to ensure that consumers in our state see the full benefit of the protections proposed in these bills. Agency enforcement is an important component of implementation. However, a lack of agency resources or information about violations can leave consumers without any recourse for violations. Coupling agency enforcement with a private right of action fills this gap by giving individuals the tools they need to bring their own suits against companies that violate their rights.

(2) Should the Legislature enact standalone bills addressing biometric identifiers and health data in addition to enacting a comprehensive data privacy bill or should the Legislature address all types of consumer personal data in a single bill? Why?

Ensuring privacy protections for and personal control over the collection, use, and disclosure of our own data is even more important as the breadth of information collected and inferred from our personal data grows. As states across the country ban access to abortion and gender-affirming care, Planned Parenthood of Northern New England is particularly committed to ensuring increased protections for consumer's health-related data. Everyone should be able to access the health care they need without their personal health information being collected and shared without their permission or knowledge.

Consumer data bills addressing health-related data–whether comprehensive or addressing consumer health data specifically–should be tailored to address consumer data without creating unworkable, additional requirements for patient data held by health care providers and other entities already regulated by state and federal law.

(3) How does the choice between an opt-in or an opt-out model for consumer consent to the collection/sharing/sale of personal data impact consumers?

An opt-in consent model is preferred. Opt-in consent affirms that consumers must meaningfully and affirmatively consent to the collection, use, or disclosure of their personal information and means that a company cannot just collect or share this data by default. On the other hand, opt-out consent reinforces the business-friendly status quo and demands that consumers seek out

and actively request that a company stop collection or disclosure of that data. Further, opt-in consent is more consumer friendly and gives users meaningful notice of the scope of data collection, use, or disclosure sought. In order to ensure that an opt-in consent model functions as intended, consent must be freely given, informed, and revocable.

(4) Are there particular approaches to consumer data privacy in other states that you consider particularly valuable or problematic?

This year, a number of states took action to increase protections for consumers' health-related data. Most relevant here, Washington enacted HB1155, a first of its kind law that, like LD1902, limits entities' collection, maintenance, and disclosure of consumer health data, including reproductive health information, without user consent, and provides consumers with additional control over the use of their health data. This new Washington law is an example of a novel consumer health data protection that includes strong enforcement mechanisms through the Attorney General and through private right of action.

(5) What existing federal laws protect consumer personal data in your industry (or the industry of concern to you) – what types of data do those laws protect (or not protect) and what types of companies do they regulate (or not regulate)?

Currently, the federal Health Insurance Portability and Accountability Act ("HIPAA") defines minimum standards for patient health information privacy, allowing states to require more stringent patient health information privacy standards.[1] Unless a state has more stringent state law requirements, covered entities (health care providers, health plans, health care clearinghouses) and their business associates (a person or entity that performs certain functions/activities or provides services to a covered entity) must comply with HIPAA minimum privacy standards.[2]

HIPAA's "Privacy Rule" describes minimum privacy standards for protected health information ("PHI"). Generally, PHI must not be disclosed without the patient's consent. However, there are many exceptions to this rule, including that HIPAA permits disclosure without patient consent in a few key instances:

- When such disclosure would be required by law. This means the disclosure is required under a statute, regulation, or court order;
- When disclosure is part of a judicial or administrative proceeding, meaning the disclosure is made pursuant to court order or subpoena;

[1] 45 CFR § 160.202.

[2] 45 CFR § 160.203.

- When disclosure is made for law enforcement purposes,[3] for example pursuant to a non-court ordered administrative request or to identify or locate a suspected perpetrator of a crime.

On the federal level, there are also significant privacy protections for information related to participation in federally assisted treatment programs for substance use disorders.[4] 42 CFR Part 2 provides broad protections against the use of program participants' treatment records by law enforcement or in criminal prosecutions against those patients.[5] Federal law lacks significant protections for reproductive health-related PHI specifically. Ideally, federal law would prohibit HIPAA covered entities from disclosing reproductive health-related PHI without consent, without the exceptions to disclosure in the HIPAA Privacy Rule detailed above.

On April 12, 2023, OCR issued a Notice of Proposed Rulemaking (NPRM) to strengthen the HIPAA Privacy Rule protections by prohibiting the use or disclosure of PHI to identify, investigate, prosecute, or sue patients, providers and others involved in the provision of legal reproductive health care. Reproductive health care would be defined to include, but not be limited to, prenatal care, abortion, miscarriage management, infertility treatment, contraception use, and treatment for reproductive-related conditions such as ovarian cancer. We support this effort to strengthen HIPAA protections for reproductive health data.

Even if the HIPAA privacy rule is strengthened, there will still be consumer health data that is not protected under federal law, as health data collected by non-HIPAA covered entities, including certain apps and websites, are not afforded the same protections.

(6) Are there any pending Congressional proposals regarding consumer data privacy of which the Maine Legislature should be aware?

Even as the scope and information available through consumer data has continued to expand, we have yet to see comprehensive consumer data privacy policies enacted at the federal level. Given this federal inaction, the role of states in ensuring privacy protections for and personal control over the collection, use, and disclosure of our own data is even more vital.

---

[3] *See Summary of the HIPAA Privacy Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last viewed July 25, 2022).
[4] *See Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule*, SAMHSA (July 13, 2020), https://www.samhsa.gov/newsroom/press-announcements/202007131330.
[5] *Id.*

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

October 17, 2023

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

RE: Additional Information for Consideration of Privacy Legislation / October 17, 2023 Work Session

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

The Retail Association of Maine and the Maine Grocers & Food Producers Association are jointly submitting comments regarding the discussion of establishing a state-level consumer privacy protection law. Our business trade associations represent Main Street businesses including independently owned and operated grocery stores and supermarkets, general merchandise, specialty retailers, and convenience stores, distributors and supporting partners — together representing more than 500 members statewide. Maine's retail sector employs more than 85,000 Mainers.

To help refresh the committee's memory, we testified in qualified support of LD 1973 which is modeled after a strong privacy law in Connecticut. We were also opposed to LD 1705, and we remain strongly opposed to that proposal as it is very similar to a problematic law in Illinois.

The Committee has asked stakeholders to respond to six questions:

Q1. What are the benefits and drawbacks of including a private right of action in consumer data privacy legislation?

A. We are strongly opposed to the inclusion of a private right of action. The experience in Illinois bears that out as thousands of Illinois small businesses find themselves faced with expensive litigation. Many of the thousands of Maine retail establishments are small businesses with a single location in the state of Maine. That is not unusual, as approximately 95% of all retail establishments nationwide have less than 50 employees and only a single location.

Illinois small businesses are not willfully violating the law. Instead, small businesses have limited resources to understand complex regulations, and they are finding themselves faced with enterprising trial lawyers looking to cash in. The businesses want to do the right thing. It would be more important for regulators to work with businesses to improve their operations and compliance. As we noted in our May testimony, the inclusion of a notice and cure provision, like what is in LD 1973 needs to be maintained, and not removed from the bill prior to enactment.

Q2. Should the Legislature enact standalone bills addressing biometric identifiers and health data in addition to enacting a comprehensive data privacy bill or should the Legislature address all types of consumer personal data in a single bill? Why?

A. We appreciate the desire of policymakers to try to address privacy as comprehensively as possible, but we think that will be an impossibly difficult challenge. It will likely create a Frankenstein type of law that will continuously be challenged and would likely be wrought with unintended consequences.

To give you an example of that since the posed question mentions 'health data,' some of our retail members have told us that we need to be careful how 'health data' gets defined. Would a store that sells health and beauty products like aspirin, toothpaste, cosmetics, shampoo, or hygiene products be included in a definition of health data? Some retailers also offer pharmacy services. We need to strongly urge the committee to be very careful how health data gets defined and applied.

It is worth noting the amendment to the Connecticut data privacy act defines "consumer health data" as ***any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis***. Examples provided include gender-affirming health data and reproductive or sexual health data. The "identify" language is critically important since selling a product, providing an advertisement or coupon for it, etc. does not mean that a retailer is trying to identify or wishes to know a consumer's physical or mental health condition. Rather, the retailer is simply trying to make available to customers the products they need and prefer. The product involved may be intended for use by the purchaser, a family member, a neighbor or other third party. Washington state made this mistake in their consumer health data law, which has resulted in retailers having to obtain consent for purchases of products as benign as aspirin and rash cream. This is why it is so important to keep these provisions focused on the areas of concern (generally, reproductive privacy) and not any product that could be tangentially related to a sweeping definition of "health."

We also think it is critical that Maine not try to reinvent the wheel. Many states have passed comprehensive privacy legislation, and Maine should not create a situation where it has a unique law that differs from legislation in different states. Many retailers operate in multiple states, and the more there is a patchwork of legislation across the country, it makes it much more difficult for Maine's small businesses to comply. We feel that the Connecticut law is a strong model that provides solid consumer protections.

In regards to biometric identifiers, LD 1705 includes a very expansive private right of action that will only benefit trial lawyers. Illinois has a similar private right of action in their law, and more than 1,000 class action lawsuits have been filed in the last five years[1]. Additionally, the Illinois law has caused businesses to avoid offering services that involve biometric identifiers because of the increased litigation risk.

The bill, as written, will require entities to make available to the public a written policy that establishes a retention schedule and guidelines for permanently destroying an identifier, and has significant requirements for disclosing to individuals, upon request, a significant list of data that may be impossible to produce. This will lead to companies violating the law unknowingly.

Biometric identifiers are not new; they have been around for years. What is new, however, are the evolving applications that can provide consumers several benefits such as negating the need for multiple passwords, increased security systems such as Ring Door Bell and a variety of other new products that are produced. Features such as voice recognition in cars prevent distracted driving. We live in a world of new development of products that increase productivity and safety.

Putting overly burdensome constraints on policies that govern the possession of biometric identifiers needs to be crafted in a way that protects an individual's rights but does not hamper or discourage a business from the lawful use of an identifier associated with a person.

[1] https://www.littler.com/files/wpi_rpt_bipa_white_paper_0623.pdf

Q3. How does the choice between an opt-in or an opt-out model for consumer consent to the collection/sharing/sale of personal data impact consumers?

A. We are glad you are asking this question. Maine retailers believe that if data privacy regulation is to be successful – that is, if it will achieve its intended public policy goals – the regulations must be biased towards consumers. Consumers must be assured that the legislation is for their benefit and not just another mechanism for businesses to profit from them or, worse, take advantage of them. This principle is fundamental to all Maine businesses that use consumer data as an element of doing business and serving their customers.

Maine retailers believe that the use of consumer data to better serve their customers is a fundamental part of their business. They have a long history of building trust and confidence with their customers, and they believe that this trust is essential to their success.

Retailers view customer data differently than data brokers or other businesses that do not have a direct relationship with consumers. To retailers, customer data is not a commodity to be sold or traded. It is an asset that can be used to improve the customer experience. It is a core element of the customer relationship and key to retailer's success in serving consumers as they expect to be served. Maine retailers use customer data to personalize the shopping experience, offer targeted promotions, and improve customer service.

We support an opt out provision in privacy legislation. This is what retail consumers have come to expect, and adding an opt in provision creates a point of friction in the consumer experience. It may sound good on paper, but repeatedly being asked to opt in on e-commerce websites, apps, and other channels is frustrating for consumers and difficult for businesses, especially small businesses, to manage.

Q4. Are there particular approaches to consumer data privacy in other states that you consider particularly valuable or problematic?

A. As we noted above, we are supportive of the Connecticut law. Not only is the legislation strong for consumers, it will help create consistency among New England states considering similar legislation. New Hampshire is discussing SB255 which is also modeled after Connecticut. Aligning a privacy law protecting Maine's consumers with a state like Connecticut will ensure that Mainers have the same great experience when they shop as our fellow New Englanders. A new regulation that differs from our neighbors could lead to the loss of loyalty rewards like free coffee, discounted shipping, and fuel points for the people of Maine.

Q5. What existing federal laws protect consumer personal data in your industry (or the industry of concern to you) – what types of data do those laws protect (or not protect) and what types of companies do they regulate (or not regulate)?

A. I am by no means an expert on federal privacy legislation. We are working some of our national organizations, like National Retail Federation, and they have deeper experience with what has or has not happened at the federal level.

Q6. Are there any pending Congressional proposals regarding consumer data privacy of which the Maine Legislature should be aware?

A. Same as Q5 above.

In closing, we want to stress some other important considerations for any privacy legislation that advances:

- **Use a July 1st Effective Date for Maine Businesses, Not January 1**: To avoid having the thousands of Maine retail establishments that employ more than 85,000 Mainers engage in a disruptive, significant implementation of new technology to comply with significant legislation during the busiest time of the year for retailers, it is critical to set the effective date of the Act for July 1, rather than January 1.

  An earlier effective date would require significant technical implementation during the busiest holiday sales period for the retail industry and could impact online operations at the worst possible time for retail employees and customers. For this same reason, Connecticut, and Colorado set a July 1, 2023, effective date (more than two years after enactment of its law), and California has previously set July 1 as the effective date for some of its promulgated data privacy regulations. We urge you to similarly adopt a July 1 effective date that is at least two years after enactment of the state's first general privacy law.

- **Two-Year Implementation Period Urged for Maine Businesses:** Most states enacting general privacy laws for the first time have given businesses up to two years to implement the new law to ensure that they will have sufficient time to comply prior to enforcement of the law commencing.

  California, for example, provided more than two years to implement its latest CPRA, adopted by ballot initiative in 2021, and enforcement of the CCPA, the predecessor law in effect now, began over two years after its enactment in 2018. This implementation period is extremely important for retail establishments in Maine, nearly all of whom will be subject to the new privacy law (not exempt from it, as are other businesses).

  As a result, the effective date of the Act should be set far enough out to permit these Maine-based businesses to develop and achieve compliance with what will be a new law with new provisions for these businesses to follow. Two years is the fair and appropriate amount of time for implementation, as demonstrated by all other states that have enacted similar laws permitting two-year implementation periods before enforcement takes effect.

- **Customer Loyalty Programs for Maine Consumers:** Retail customers value the personalization and benefits that loyalty programs provide. Nearly 80% percent of consumers participate in at least one loyalty program and the average adult participates in more than nine.

  Maine retailers are committed to using consumer data in a responsible way, and consumers should be able to trust that their data will be used responsibly. Maine retailers believe that data privacy regulations can help to ensure that consumers' rights are protected, and that they can help to build trust between retailers and their customers. Retailers believe that data privacy regulations should be designed to protect consumers' privacy, while also allowing businesses to use data in a responsible way.

It is in all our best interests to get this right.

Thank you for the consideration of our comments.

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

Prepared Testimony of Katie Hawkins
Work Session on Data Privacy Acts
Maine Judiciary Committee
October 17, 2023

Good morning, my name is Katie Hawkins and I am a Director of Regulatory Affairs in the General Counsel's office at WEX, a global financial services and technology company headquartered in Portland. Thank you for the opportunity to speak about these pieces of legislation. In this testimony I will address each of the six questions presented by the Committee and then I will welcome your questions.

We are grateful that the Legislature is considering thoughtful safeguards that protect the data and general privacy rights of Maine's consumers. However, we caution that creating new requirements for businesses that diverge from those standards that exist in other states that have successfully passed comprehensive privacy legislation likely will place a costly and unnecessary compliance burden on businesses, making Maine a less attractive place to do business without materially adding to consumer protections.

The private right of action is an issue that has time and again stymied the efforts of the federal government and states across the country to pass effective data privacy protections into law. We believe the ability for a private individual to hold an enterprise accountable for violating the individual's rights is fundamental in terms of civil and employment rights, but the ability to litigate unilaterally on data disclosures (or lack thereof) exposes a state to being overrun by moneyed interests. Class-action lawsuits and a search for rewards and settlements distract from establishing standards that companies must abide by. This also threatens consumers' ability to access and enjoy innovative products and services. For instance in Illinois where the Biometric Information Privacy Act was passed, rampant litigation has forced companies to remove products from the Illinois marketplace altogether.

In order to reach quick and effective results, it would be best to consider unified, holistic legislation proposed in a single law requiring companies to safeguard consumers' and employees' data privacy interests. For instance, LD1977, as proposed, already protects biometric information. In light of that, the bill LD1705, "An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data," should be dropped in its entirety as it only sows confusion. For example, s. 9605 of that bill defines "Confidential and Sensitive Data" differently from "Sensitive Data" found in s. 9602 of LD1977. Repetitions and inconsistencies like this can weaken privacy protections by confusing enforcers, consumers, and businesses all at once, and bringing privacy laws into disrepute.

On the Committee's interest in the opt-out versus opt-in models for consumer consent to the collection, sharing and sale of personal data, we note that today's consumers are most familiar with the opt-out model for consent. In keeping with our call for a unified path forward that best protects consumers' rights, it would be reasonable to structure this legislation similar to other already passed legislation, to ensure that its execution can be easily adopted by Maine companies doing business across multiple states and territories.

Related to enforcement of the ultime legislation, we suggest that the Legislature consider whether a dedicated privacy regulator would be a superior enforcer of this legislation rather than an appointed or elected official selected for their prosecutorial mindset, rather than their expertise in privacy or business matters. For better - not weaker - enforcement of this legislation, s. 9620 could be dropped in its entirety in favor of establishing a Maine Privacy Protection Authority, staffed by both privacy and business experts, which will work constructively - and consistently - with consumers and companies alike for fair, reasonable, and effective enforcement of the data privacy requirements passed as part of one comprehensive bill. This is similar to the model in Europe, where 27 EU member states - plus the United Kingdom, Norway, and Switzerland - have created dedicated Data Protection Agencies (DPAs), all staffed by subject-matter experts. These agencies have the powe to detect, investigate, and punish privacy law violations, as well as educate both consumers and businesses in what the law requires. Importantly, these DPAs are apolitical and separate regulators from governments. This independence and impartiality allows them to resolve consumer complaints more quickly and efficiently, while helping businesses comply with the law and avoid infractions in the first place.

Like other companies across the across, today WEX is subject to the data privacy reguyaltuon at the federal and state level. WEX currently complies with the Gramm-Leach-Bliley Act (GLBA) and HIPAA. GLBA is a federal law that regulates "financial institutions" - however, the term financial institution is defined very broadly to capture far more than the banks and credit unions that we typically think of as financial institutions. GLBA, as implemented by two regulations, requires annual privacy notices to customers and requires the safeguarding of consumer information by businesses. HIPAA protects consumers' private health information (PHI). While the average consumer is most familiar with HIPAA from disclosures received at medical offices, businesses like WEX that have access to PHI for business purposes must comply with stringent requirements related to the protection of PHI. In addition to these federal laws, where state law is more restrictive - like in California - WEX, as an issuer of a commercial credit card product, follows that state's laws.

Finally, the U.S. Congress has repeatedly revisited legislation to address data privacy protections. And while certain proposals have made it through Committees, it is likely appropriate for the Maine Legislature to act prior to passage and implementation of a federal law. Waiting on a federal solution - one that will likely preempt legislation that this Committee proposes in the interim - will be a lengthy process. In addition to your efforts today to provide protections and safeguards to consumers, we urge you to instead consider one comprehensive piece of legislation in line with other states' passed legislation - including, Texas, Virginia, Montana, Indiana and Iowa to ensure a quick and thorough remedy to regulating data privacy.