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: December 11, 2023

RE: ***Additional Information***: other state comprehensive consumer data privacy legislation: HIPAA/GLBA exemptions; employment/employee exemptions; "publicly available information" definitions; and data minimization standards

As requested at the work session on November 8, this memorandum provides additional information on other states' comprehensive data privacy laws.

1. Other States' Exceptions for: HIPAA entities or data; GLBA entities or data; and employee information

State	HIPAA Exemption(s)	GLBA Exemption(s)	Employee Exemptions
California Cal. Civ. §1789.100 et. seq.	**Data**: Protected health information collected by a covered entity/business associate governed by HIPAA **Entity**: Covered entity/ business associate governed by HIPAA "to the extent" they maintain, use and disclose patient information in the same manner as protected health information	**Data**: Data collected, processed, sold or disclosed subject to GLBA **Entity**: *No exception*	**"Personal Information"**: includes "professional or employment-related information" **Data**: exempt data of applicants, employees, owners, directors, officers, medical staff, indep. contractors
Colorado SB 21-190	**Data**: Protected health information collected, stored and processed by a covered entity/business associates; and data created to comply with HIPAA or maintained in same manner as PHI by a covered entity/ business associate **Entity**: *No exception*	**Data**: Data collected, processed, sold or disclosed in compliance with GLBA **Entity**: Financial institutions and affiliates subject to GLBA	**"Consumer"**: define to exclude actors in commercial or employment context, applicants or beneficiaries of employee **Data**: Data maintained for employment records purposes
Connecticut Pub. Act 22-15 Pub. Act 23-56	**Data:** Protected health information; intermingled data or data treated like PHI by covered entity/business associate **Entity**: Covered entity/business associate	**Data**: Data subject to GLBA **Entity:** Financial institution [*affiliates not listed*] subject to GLBA	**"Consumer":** define to exclude actors in commercial or employment contact or employee, owner, director, officer or contractor of business/govt. agency **Data**: exempt data of applicants, employees, agents, indep. contractors

State	HIPAA Exemption(s)	GLBA Exemption(s)	Employee Exemptions
Delaware T. 6, Ch. 12D	**Data:** Protected Health Information under HIPAA **Entity:** *No exception*	**Data**: Data subject to GLBA **Entity**: Financial institutions and affiliates subject to GLBA	*Same as Connecticut*
Indiana T. 24, Art. 15	**Data:** Protected health information; intermingled data or data treated like PHI by covered entity/business associate **Entity**: Covered entity/ business associate governed by HIPAA	**Data**: Data subject to GLBA **Entity:** Financial institutions and affiliates subject to GLBA	**"Consumer":** define to exclude actors in commercial or employment context **Data**: exempt data of applicants, employees, agents, indep. contractors
Iowa §715D *et seq.*	**Data:** Protected health information; intermingled data or data treated like PHI by covered entity/business associate **Entity**: Persons who are subject to and comply with HIPAA	**Data**: Data subject to GLBA **Entity:** Financial institutions and affiliates subject to GLBA	*Same as Indiana*
Montana T.30, Ch. 14, Pt. 28	**Data:** Protected health information; intermingled data or data treated like PHI by covered entity/business associate **Entity**: covered entity/business associate	**Data:** Data collected, processed, sold or disclosed in accordance with GLBA **Entity**: Financial institution and affiliates governed by GLBA	*Same as Connecticut*
Oregon S.B. 619	**Data**: Protected health information a covered entity/business associate processes in accordance with or creates for purpose of comply with HIPAA; and intermingled data treated like PHI in manner required by HIPAA by covered entity/business associate **Entity**: *No exception*	**Data**: Data collected, processed, sold or disclosed in accordance with GLBA **Entity**: *No exception*	**"Consumer"**: define to exclude actors in commercial or employment context **Data**: exempt data of applicants, employees, owners, directors, officers, contractors
Tennessee T. 47, ch. 18, Pt. 33	**Data**: Protected health information; intermingled data or data treated like PHI by covered entity/ business associate **Entity**: Covered entity/ business associate governed by HIPAA	**Data**: Data subject to GLBA **Entity**: Financial institutions and affiliates subject to GLBA	*Same as Indiana*
Texas HB 4	**Data**: Protected health information; intermingled data or data treated like PHI by covered entity/business associate **Entity**: Covered entity/ business associate governed by HIPAA	**Data**: Data subject to GLBA **Entity:** Financial institution [*affiliates not listed*] subject to GLBA	*Same as Indiana*
Utah T. 13, ch. 61	**Data**: Protected health information; also data intermingled with PHI maintained by health care facility or provider **Entity**: Covered entity/business associate & no person required to take any action in conflict with HIPAA	**Data**: Data collected, processed, sold or disclosed in accordance with GLBA **Entity**: Financial institution and affiliates governed by GLBA	*Same as Indiana*
Virginia T. 59.1, ch. 53	**Data**: Protected health information; intermingled data or data treated like PHI by covered entity/ business associate **Entity**: Covered entity/ business associate governed by HIPAA	**Data**: Data subject to GLBA **Entity:** Financial institution [*affiliates not listed*] subject to GLBA	*Same as Indiana*

2. Other States' Data Minimization Standards

State	Data minimization for personal data / covered data
California	**Collection & Processing**: "reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes."
Colorado	**Collection:** "adequate, relevant, and limited to what is reasonably necessary" for disclosed processing purpose **Processing**: not for purposes "that are not reasonably necessary to, nor compatible with" disclosed purpose absent consent **Exempt activities**: if data is collected or processed for a purpose exempt from the Act (ex: to comply with a subpoena or provide requested product) such activity must be "necessary, reasonable and proportionate" to that purpose
Connecticut	**Collection:** "what is adequate, relevant, and reasonably necessary" for disclosed processing purpose **Processing**: not for purpose "neither reasonably necessary to, nor compatible with" disclosed purpose absent consent **Exempt Activities**: if data is collected or processed for a purpose exempt from the Act (ex: to comply with a subpoena or provide requested product) such activity must be "reasonably necessary and proportionate" to and "adequate, relevant, and limited to what is necessary" in relation to that purpose
Delaware	*Same as Connecticut*
Indiana	*Same as Connecticut*
Iowa	**Collection & Processing:** none found **Exempt activities**: *same as Connecticut*
Montana	*Same as Connecticut*
Oregon	*Same as Connecticut*
Tennessee	*Same as Connecticut*
Texas	*Same as Connecticut*
Utah	None found
Virginia	*Same as Connecticut*

3. Other State Definitions of "Publicly Available Information" Not Covered by Consumer Data Privacy Legislation

State	"Publicly Available Information" excluded from legislation's scope
California	"Publicly available" means: • information that is lawfully made available from federal, state, or local government records; or • information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or • information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

State	"Publicly Available Information" excluded from legislation's scope
Colorado	*Same as Delaware (with different paragraph structure)*
Connecticut	"Publicly available information" means information that: A. is lawfully made available through federal, state, or municipal government records or widely distributed media; and B. a controller has a reasonable basis to believe a consumer has lawfully made available to the public.
Delaware	"Publicly available information" means any of the following: a. Information that is lawfully made available through federal, state, or local government records. b. Information that a controller has a reasonable basis to believe that the consumer has lawfully made available to the general public through widely distributed media.
Indiana	*Nearly identical to California (except no biometric exclusion)*
Iowa	*Nearly identical to California (except no biometric exclusion)*
Montana	*Same as Connecticut (with "or" instead of "and" connector between ¶a and ¶b)*
Oregon	*Same as Montana (but not called "publicly available information"; instead, this information is excluded from the "personal data" definition)*
Tennessee	*Nearly identical to California (except no biometric exclusion)*
Texas	*Nearly identical to California (except no biometric exclusion)*
Utah	*Nearly identical to California (except different word order and no biometric exclusion)*
Virginia	*Nearly identical to California (except no biometric exclusion)*

4. **<u>Other Handouts (from non-OPLA sources)</u>**

- ***Office of the Attorney General*** — (a) data minimization memo and spreadsheet; (b) publicly available information memo; and (c) cover email
- ***Maine Association of Health Plans*** — email and chart comparing other states' HIPAA, GLBA and employee data exemptions
- ***Confidentiality Coalition*** — comment on LD 1977
- ***L.L. Bean*** — letter explaining its use of "trackers" on the llbean.com website
- ***American Council of Life Insurers*** — explanation why it requests an entity-level GLBA exception in any state privacy legislation
- ***Securities Industry and Financial Markets Association*** – comment on LD 1977
- ***National Crime Insurance Bureau*** — email requesting exception for 501(c)(4) organizations in any state privacy legislation
- ***Advanced Medical Technology Association (AdvaMed)*** — comment on LD 1902 and LD 1977
- ***Coalition of Maine Healthcare Organizations*** — explanation why it requests an entity-level HIPAA exception in LD 1977
- ***Consumer advocate critiques of the GLBA*** — these materials were provided to the committee by Representative O'Neil

Memorandum

To: Janet Stocco, Legislative Analyst, OPLA (janet.stocco@legislature.maine.gov)
From: Brendan O'Neil, AAG, Consumer Protection Division
Date: November 28, 2023
Re: Judiciary Committee questions (email dtd 11/13)
Data Minimization

Question: The Judiciary Committee Chairs posed the following question to the Attorney General's Office:

> "1. Data minimization: LD 1973, §9605(1)(A) requires controllers to "limit the collection of personal data to what is ***adequate, relevant and reasonably necessary*** in relation to the purposes . . . disclosed to the consumer" while LD 1977 requires covered entities to limit "the collection, processing or transfer" (a) of covered data "to what is ***reasonably necessary and proportionate*** to provide or maintain a specific product or service," §9604(1), and (b) of sensitive data to what "is ***strictly necessary*** to provide or maintain a specific product or service," §9605(2).
>
> Do you have a sense of how other states approach data minimization? Is the approach of LD 1973, which is also the approach in Connecticut, used in all states or do some states use the LD 1977 approach (or a different approach)?
>
> If you do not have easy access to this information we at OPLA can certainly look into the question. Just let me know.

Response:

I put together the attached spreadsheet to compare the relevant provisions[1]. To answer your question: in general, the Connecticut-style statutes all use the LD 1973 approach. In contrast, the ADDPA-style bills use the LD 1977 approach, although Colorado's privacy regulations flesh out the specific duties. Finally, California is more like the Connecticut-style statutes.

A few things stand out from this exercise. First, as you can see from the text in blue, LD 1977 limits more activities than LD 1973. Second, as you can see from the text in red, LD 1977 permits the use of data for a more limited purpose: to provide a product or service. In contrast, LD 1973 permits data to be used for whatever the entity says it will be used for in its privacy policy disclosure. In this way, it can be said that LD 1973 does not require entities to minimize the data they collect, use, and transfer – it only requires that they notify individuals of the data the entities collect, use, and transfer. LD 1977, on the other hand, requires entities to limit their

[1] Note that the provisions may not exactly line up because the different bills/statutes are structured differently, and because I wanted to get back to you in short order and did not want to delay by trying to line things up more precisely.

data collection, processing, and transfer of data to only what is needed to provide a specific product or service requested by an individual.

Third, LD 1977 requires entities, in § 9616 (2)(D), to delete covered data when it is no longer needed for the purpose for which it was collected. Colorado's privacy regulations have similar provisions. LD 1973 does not have such a provision.

Fourth, the data of children is an important part of data minimization. LD 1977 includes minors in the definition of sensitive data, and bars the processing of sensitive data for targeted advertising. This means that targeted ads cannot be targeted to minors, not even with consent. While LD 1977 does not define the age of minors, the Massachusetts legislation and ADPPA define it as under 18.

In contrast, LD 1973 and the Connecticut-style statutes permit the processing of information about minors, for targeted advertising or other purposes, of any age so long as there is opt-in consent: most refer to a federal statute, COPPA, for parental consent for under-13s; others permit the minor themselves to opt-in when 13 or older. More recent versions raise the age of minors to under 18, and Connecticut this year amended its statute to do so. We question why children's data should be collected and processed for targeted advertising and building user profiles, even with consent. That is, why should entities be permitted to ask children or their parents for consent to collect and use their data for targeted ads and profiling? Why should children be allowed to give their consent to this practice? We think the better approach is in LD 1977.

Attorney General position. The Attorney General strongly prefers the data minimization provisions of LD 1977 because it is a core part of any meaningful privacy legislation in at least the following ways:

- It better aligns with the expectations of individuals that entities will only collect the data necessary to provide the product or service for which the individual is interacting with the entity.
- It reduces the administrative burdens of entities to explain their practices in privacy notices and to respond to the individual rights of privacy legislation to access, correction and deletion – that is, an entity won't have to spend time providing access to, correcting or deleting data that the entity doesn't collect.
- It reduces the technological and security obligations of an entity to protect the data it collects and stores by reducing the data subject to the obligations, and by requiring entities to delete data when it is no longer needed.
- It reduces the risk and impact of a data breach, which increases protection for consumers and reduces liability risk of entities. The less data an entity collects, and the sooner it deletes it, the less risk of harm to consumers resulting from the disclosure of their data in the event of a breach and the less exposure the entity has to claims that it put individuals' data at risk by unreasonably collecting excessive data and storing it too long.
- It reduces the risk of liability under this legislation, whether there is a private right of action or only Attorney General enforcement, by minimizing what entities need to disclose to individuals, to obtain consent, and to otherwise give effect to the individual rights and other obligations of this legislation.

- It is the first level of protection for individuals' privacy, reducing the impact of potentially weaker-than-ideal other protections (such as consent, access, targeted advertising, enforcement tools, etc.).

Data Minimization Approaches in Different States' Privacy Statutes and Legislation

As of November 17, 2023

ADPPA-style		Connecticut-style				California Consumer Privacy Act (as amended by CPRA)
MA S. 25	**LD 1977**	**LD 1973**	**Delaware**	**Oregon**	**Colorado**	**California**
Section 2. Duty of Loyalty	**§9604. Actions regarding covered data**	**§9605. Actions of controllers**	**§ 12D-106. Duties of controllers.**	**Section 5**	**6-1-1308. Duties of controllers.**	**1798.100. General Duties of Businesses that Collect Personal Information.**
(a)A covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to carry out one of the following purposes:— (1)provide or maintain a specific product or service requested by the individual to whom the data pertains;	1. Prohibitions. Except as provided by subsection 2, a covered entity may not collect, process or transfer covered data unless the collection, processing or transfer is limited to what is ***reasonably necessary and proportionate*** to provide or maintain a specific product or service requested by the individual to whom the data pertains. A covered entity or service provider may not engage in deceptive advertising or marketing with respect to a product or service offered to an individual.	1. Duties. A controller shall: A. Limit the collection of personal data to what is ***adequate, relevant and reasonably necessary*** in relation to the purposes for which the data is processed, as disclosed to the consumer; ... C. In the case of the processing of sensitive data concerning a child, process the data in accordance with the federal Children's Online Privacy Protection Act of 1998, 15 United States Code, Section 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to that Act; and ...	(a) A controller shall do all of the following: (1) Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer. (2) Except as otherwise permitted by this chapter, not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent. ... (4) Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without first obtaining consent from the child's parent or lawful guardian and otherwise complying with § 1204C of Chapter 12C of this title.	(1) A controller shall: (a) Specify in the privacy notice described in subsection (4) of this section the express purposes for which the controller is collecting and processing personal data; (b) Limit the controller's collection of personal data to only the personal data that is adequate, relevant and reasonably necessary to serve the purposes the controller specified in paragraph (a) of this subsection;	(2) **Duty of purpose specification**. A controller shall specify the express purposes for which personal data are collected and processed. (3) **Duty of data minimization**. A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed.	A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.
(2)initiate, manage, complete a transaction, or fulfill an order for specific products or services requested by an individual, including any associated routine administrative, operational, and account-servicing activity such as billing, shipping, delivery, storage, and accounting; (3)authenticate users of a product or service; (4)fulfill a product or service warranty; (5)prevent, detect, protect against, or respond to a security incident. For purposes of this paragraph, security is defined as network security and physical security and life safety, including an intrusion or trespass, medical alerts, fire alarms, and access control security; (6)to prevent, detect, protect against, or respond to fraud, harassment, or illegal activity targeted at or involving the covered entity or its services. For purposes of this paragraph, the term "illegal activity", a violation of a federal, state, or local law punishable as a felony or misdemeanor that can directly harm; (7)comply with a legal obligation imposed by state or federal law, or to investigate, establish, prepare for, exercise, or defend legal claims involving the covered entity or service provider;	2. Allowed purposes. A covered entity may collect, process or transfer covered data for any of the following purposes if the collection, processing or transfer is limited to what is reasonably necessary and proportionate to that purpose: A. To initiate, manage or complete a transaction or fulfill an order for a specific product or service requested by an individual, including associated routine administrative, operational and account-servicing activity including billing, shipping, delivery, storage and accounting; B. With respect to covered data previously collected in accordance with this chapter: (1) To process the data as necessary to perform system maintenance or diagnostics; (2) To develop, maintain, repair or enhance a product or service for which the data was collected; (3) To conduct internal research or analytics to improve a product or service for which the data was collected; (4) To perform inventory management or reasonable network management; (5) To protect against spam; (6) To debug or repair errors that impair the functionality of a service or product for which the data was collected; (7) To process the data as necessary to provide first-party advertising or marketing of products or services provided by the covered entity for individuals who are not minors. For purposes of this subparagraph, "first-	2. Prohibitions. A controller may not: A. Process sensitive data concerning a consumer without obtaining the consumer's consent; ... E. Except as otherwise provided in this chapter, process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.		(2) A controller may not: (a) Process personal data for purposes that are not reasonably necessary for and compatible with the purposes the controller specified in subsection (1)(a) of this section, unless the controller obtains the consumer's consent; (b) Process sensitive data about a consumer without first obtaining the consumer's consent or, if the controller knows the consumer is a child, without processing the sensitive data in accordance with the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 et seq. and the regulations, rules and guidance adopted under the Act, all as in effect on the effective date of this 2023 Act; (c) Process a consumer's personal data for the purposes of targeted advertising, of profiling the consumer in furtherance of decisions that produce legal	(4) **Duty to avoid secondary use.** A controller shall not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's consent. ... (7) **Duty regarding sensitive data**. A controller shall not process a consumer's sensitive data without first obtaining the consumer's consent or, in the case of the processing of personal data concerning a known child, without first obtaining consent from the child's parent or lawful guardian. *(Note: Child is under 13. s. 6-1-1303(4))*	
Section 3. Sensitive covered data. *(note: sensitive covered data includes information about minors, defined as under 18)*	**§9605. Actions regarding sensitive data** *(note: sensitive data includes information about minors)*					**1798.121. Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information**

Data Minimization Approaches in Different States' Privacy Statutes and Legislation

As of November 17, 2023

ADPPA-style		Connecticut-style				California Consumer Privacy Act (as amended by CPRA)
MA S. 25	**LD 1977**	**LD 1973**	**Delaware**	**Oregon**	**Colorado**	**California**
(a)A covered entity or service provider shall not:— … (2)collect or process sensitive covered data, except where such collection or processing is strictly necessary to provide or maintain a specific product or service requested by the individual to whom the covered data pertains or is strictly necessary to effect a purpose enumerated in paragraphs (1), (2), (3), (5), (7), (9), (10), (11), (13), (14) of subsection (a) of section 2, and such data is only used for that purposes; … (4)process sensitive covered data for purposes of targeted advertising.	A covered entity or service provider may not: … 2. Collections and processing. Collect or process sensitive data, except when the collection or processing is **strictly necessary** to provide or maintain a specific product or service requested by the individual to whom the sensitive data pertains or is strictly necessary to achieve a purpose described by section 9604, subsection 2, paragraphs A to N; … 5. Targeted advertising. Process sensitive data for the purposes of targeted advertising. *(Note: see also s. 9610 (2) re: minors)* …		(7) Not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge or willfully disregards that the consumer is at least thirteen years of age but younger than 18 years of age.			(a) A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, to perform the services set forth in paragraphs (2), (4), (5), and (8) of subdivision (e) of Section 1798.140, and as authorized by regulations adopted pursuant to subparagraph (C) of paragraph (19)of subdivision (a) of Section 1798.185. A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in this subdivision shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be used, or disclosed
	§9616. Data security *(Note: aligns with s. 208 (b)(4) of the ADPPA)*				**Rule 6.07 DATA MINIMIZATION** COLORADO DEPARTMENT OF LAW, Consumer Protection Section Colorado Privacy Act Rules, 4 CCR 904-3	**1798.120. Consumers' Right to Opt Out of Sale or Sharing of Personal Information**
	2. Requirements. The data security practices of the covered entity and of the service provider required under this subsection must include, for the respective entity's own system, at a minimum, the following practices: … D. Disposing of covered data in accordance with a retention schedule that requires the deletion of covered data when the data is required to be deleted by law **or is no longer necessary for the purpose for which the data was collected, processed or transferred, unless an individual has provided affirmative consent to that retention.** Disposal may include destroying, permanently erasing or otherwise modifying the covered data to make the data permanently unreadable or indecipherable and unrecoverable to ensure ongoing compliance with this section. A service provider shall establish practices to delete or return covered data to a covered entity as requested at the end of the provision of services unless retention of the covered data is required by law;				A. To ensure all Personal Data collected is reasonably necessary for the specified purpose, Controllers shall carefully consider each Processing purpose and determine the minimum Personal Data that is necessary, adequate, or relevant for the express purpose or purposes. B. Personal Data should only be kept in a form which allows identification of Consumers for as long as is necessary for the express Processing purpose(s). To ensure that the Personal Data are not kept longer than necessary, adequate, or relevant, Controllers shall set specific time limits for erasure or to conduct a periodic review. 1. Any Personal Data determined to no longer be necessary, adequate, or relevant to the express Processing purpose(s) shall be deleted by the Controller and any Processors that the Controller has shared the Personal Data with.	(c) Notwithstanding subdivision (a), a business shall not sell or share the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.

Memorandum

To: Janet Stocco, Legislative Analyst, OPLA (janet.stocco@legislature.maine.gov)
From: Brendan O'Neil, AAG, Consumer Protection Division
Date: November 28, 2023
Re: Judiciary Committee questions (email dtd 11/13)
Publicly Available Information

Question: The Judiciary Committee Chairs posed the following question to the Attorney General's Office:

> "2. Publicly available information: Neither LD 1973 nor LD 1977 protects or provides a consumer with any rights to "publicly available information." LD 1973 defines "publicly available information" in §9601(18) but LD 1977 does not define this phrase. The committee chairs are wondering if the Office of the Attorney General is comfortable with the definition in LD 1973 or would propose an alternate definition. They are also wondering if the Office of the Attorney General recommends that Maine legislation include any protection for publicly available information (for example, a requirement that controllers/covered entities or processers/service providers disclose, on request of a consumer, public data they have for that consumer and where it was obtained)?

Response:
Publicly available information is a significant exception from covered data and has the potential to be a major loophole. We believe other states are identifying this as an enforcement challenge and a frustration for individuals. This issue is just one of the areas in which the AGO believes LD 1977 is the better vehicle to protect Mainers' information, data, and privacy.

Alternate Definition: The Attorney General's Office (AGO) is not comfortable with the definition in LD 1973 and would prefer an alternative definition. We would propose a modified version of a definition that is found in federal legislation on which LD 1977 is modeled, the ADPPA, which was reported out of a U.S. House of Representatives committee by a vote of 53-2.[1] The text of this proposed definition follows.

Individual rights regarding Publicly Available Information: The AGO recommends that Maine legislation 1) provide individuals with rights to sufficient detail about their data and information so that they can make informed choices and can act on the information; and 2) include publicly available information ("PAI") among that information.

Specifically, we believe individuals need more detail in privacy policies about what entities are doing with their information and who they are sharing it with, and that this should include PAI. This will better enable individuals to make informed choices about whether they want to engage

[1] The ADPPA's definition is also in a version of LD 1977 which is being considered the legislature in Massachusetts (and which itself, as I understand it, was modeled on the ADPPA).

with a service or product. However, we recognize that in privacy policies, entities may be able to provide only general, not individualized, information and we understand that in some cases information about categories of business partners, rather than specific names, may be more workable in privacy policies.

Specific names of business partners should be more available, though, in individual rights to access, correction, and deletion, including regarding PAI. Providing specifics here will enable individuals to know what their data or information is, where it is coming from, and where it is going. This will give individuals the ability to act on this information – without being able to act on the information, these individual rights may be of little benefit.

The potential loophole of PAI may be somewhat mitigated in the individual rights if entities will need to disclose the specific items of PAI they claim to have and from which other entities they obtained it. In particular, we recommend the Committee give serious consideration to a process in the individual rights by which entities would need to establish that information is in fact PAI; failure to establish that information is PAI should create a presumption that it is not, therefore making it covered data.

Also, PAI may need correcting just as non-PAI covered data, and individuals should be able to exercise this right, which may be similar to individual rights regarding credit reports under the Fair Credit Reporting Act. Lastly, whether individuals may request deletion of PAI is worth considering: legislation may enable a request, and an entity may comply with a request, but it is unclear at this time whether state legislation may require entities to comply with a deletion request regarding PAI.

All of this dovetails with the concept of data minimization, in that an entity will have fewer obligations and less risk of liability, under this legislation, under data breach statutes, or other statutes, if it collects only the data it absolutely needs to provide its product, and keeps the data only for as long as it needs to provide that service. The AGO will address data minimization in a separate memo.

Finally, the Committee may wish to consider giving individuals separate notice and consent rights regarding when they make their information publicly available. In the proposed definition below, section A(3) identifies as public that information which is posted to a public website or online service, except when there is an indication that the individual has attempted to restrict the information to a particular audience (for example, a public vs private posting to a website). Individuals may not be aware when they post to a website how, or the extent to which, they are converting their information into PAI. Internet 'scrapers', such as Clearview AI, or data brokers, use technology to scrape such posts for information, which then becomes broadly commercialized. Websites may take steps to restrict such scrapers but are not required to. In short, individuals may benefit from being separately notified that what they post may become PAI unless they choose to limit it to private (which is opt-out consent), and may also benefit from opt-in consent for either public posting or from companies engaging in such scraping.

Proposed definition of Publicly Available Information:

§ 9602 Definitions

(XX) Publicly available information.

A. "Publicly available information" means information that has been lawfully made available to the general public from:

(1) Federal, state, or local government records, if the covered entity collects, processes, and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity;

(2) Widely distributed media;

(3) A website or online service made available to all members of the public, for free or for a fee, including where all members of the public, for free or for a fee, can log in to the website or online service;

(4) A disclosure that has been made to the general public as required by federal, state, or local law; or

(5) The visual observation of the physical presence of an individual or a device in a public place, not including data collected by a device in the individual's possession.

For purposes of this paragraph, information from a website or online service is not available to all members of the public if the individual who made the information available via the website or online service has restricted the information to a specific audience.

B. The term "publicly available information" does not include:—

(1) Any obscene visual depiction, as defined in section 18 U.S.C. section 1460;

(2) Any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive covered data with respect to an individual;

(3) Biometric information;

(4) Publicly available information that has been combined with covered data;

(5) Genetic information, unless otherwise made available by the individual to whom the information pertains; or

(6) Intimate images known to have been created or shared without consent.

From: Stocco, Janet <Janet.Stocco@legislature.maine.gov>
Sent: Tuesday, November 28, 2023 2:56 PM
To: Legislature: Committee on Judiciary <JUDMembers@legislature.maine.gov>
Subject: OAG Answers to Questions from Judiciary Committee Chairs on Consumer Privacy Bills

Dear Judiciary Committee Members,

Please find in the forwarded email below and the attachments information in response to the following two questions related to the pending consumer privacy bills that Senator Carney and Representative Moonen asked me to pose to the Office of the Attorney General:

1. Data minimization: LD 1973, §9605(1)(A) requires controllers to "limit the collection of personal data to what is ***adequate, relevant and reasonably necessary*** in relation to the purposes . . . disclosed to the consumer" while LD 1977 requires covered entities to limit "the collection, processing or transfer" (a) of covered data "to what is ***reasonably necessary and proportionate*** to provide or maintain a specific product or service," §9604(1), and (b) of sensitive data to what "is ***strictly necessary*** to provide or maintain a specific product or service," §9605(2).

   Do you have a sense of how other states approach data minimization? Is the approach of LD 1973, which is also the approach in Connecticut, used in all states or do some states use the LD 1977 approach (or a different approach)?

   If you do not have easy access to this information we at OPLA can certainly look into the question. Just let me know.

2. Publicly available information: Neither LD 1973 nor LD 1977 protects or provides a consumer with any rights to "publicly available information." LD 1973 defines "publicly available information" in §9601(18) but LD 1977 does not define this phrase. The committee chairs are wondering if the Office of the Attorney General is comfortable with the definition in LD 1973 or would propose an alternate definition. They are also wondering if the Office of the Attorney General recommends that Maine legislation include any protection for publicly available information (for example, a requirement that controllers/covered entities or processers/service providers disclose, on request of a consumer, public data they have for that consumer and where it was obtained)?

OPLA will provide hard copies of these materials during the next work session on these bills on December 11th.

Sincerely, Janet

--

Janet A. Stocco, Esq.
Legislative Analyst
Office of Policy and Legal Analysis
Maine State Legislature
Office Tel.: (207) 287-1670

From: ONeil, Brendan <Brendan.ONeil@maine.gov>
Sent: Tuesday, November 28, 2023 1:32 PM
To: Stocco, Janet <Janet.Stocco@legislature.maine.gov>

Cc: Hayes, Danna <danna.hayes@maine.gov>
Subject: RE: Questions from Judiciary Committee Chairs on Consumer Privacy Bills

Janet,

Here are two memos responding to the Committee's questions. Delivery was slowed down by the holiday break. We'd be happy to discuss them or answer questions about them.

Regarding Data Minimization, we recently became aware of the work in this area of the Mozilla Foundation, which makes the Firefox internet browser. I forward this information for your or the Committee's information about one internet company's approach to this concept.

- Mozilla's version of data minimization appears to be their Lean Data Practices – this website describes the principles in very general terms and appears geared towards providing tools for other companies to implement the practices, with sample worksheets, toolkits, and discussions of privacy policies.
- Mozilla included a brief discussion of its Lean Data Practices in Congressional testimony earlier this year, which also called for the ADPPA to advance in Congress.
- Here is a blog post discussing the Practices a bit more.

I hope this is helpful as a real-world example of data minimization.

Thanks,
Brendan

Stocco, Janet

From: Dan Demeritt <Dan.Demeritt@MEAHP.com>
Sent: Wednesday, November 22, 2023 12:04 PM
To: Stocco, Janet
Cc: Dan Demeritt
Subject: Comparison of Privacy Bills
Attachments: Exemption Comparison between Enacted State Comprehensive Privacy Laws - 11-6-23.pdf

Follow Up Flag: Flag for follow up
Flag Status: Completed

Janet,

Thank you for your great work on the privacy bills. The updates and materials are very well done.

One of our stakeholders shared the attached summary of exemptions in place in enacted state comprehensive privacy laws around the country. I am passing it along in the event that it could be helpful.

Have a great Thanksgiving.

Best,

Dan

Dan Demeritt
Executive Director
Maine Association of Health Plans

Dan.Demeritt@MEAHP.com
(207) 852-2087 (mobile)

Enacted State Comprehensive Privacy Laws

The below table highlights that all state comprehensive privacy laws enacted to date include entity and/or data level exemptions related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). It also shows that all states have enacted some form of exemption for certain employment related uses, and that all but California exclude commercial and employment data from their definition of consumer/personal data. **Note:** The Tennessee Information Protection Act additionally exempts state licensed insurance companies from its scope.

State	Bill	HIPAA Exemption(s)	GLBA Exemption(s)	B2B/ Employee Data Exemption(s)
Delaware	HB 154	Yes (data-level)	Yes (entity-level)	Yes (consumer definition (Both) and certain employment use exemptions)
Indiana	SB 5	Yes (entity-level)	Yes (entity-level)	Yes (consumer definition (Both) and certain employment use exemptions)
Iowa	SF 262	Yes (entity and data-level)	Yes (entity-level)	Yes (consumer definition (Both) and certain employment use exemptions)
Montana	SB 384	Yes (entity and data-level)	Yes (entity-level)	Yes (consumer definition (Both) and certain employment use exemptions)
Oregon	SB 619	Yes (data-level)	Yes (data-level)	Yes (consumer definition (Both) and certain employment use exemptions)
Tennessee	HB 1181	Yes (entity and data-level)	Yes (entity-level)	Yes (consumer definition (Both) and certain employment use exemptions)
Texas	HB 4	Yes (entity and data-level)	Yes (entity-level)	Yes (consumer definition (Both) and certain employment use exemptions)
California	CCPA, as amended	Yes (entity and data-level)	Yes (data-level)	No and Yes (personal information definition includes professional and employment- related data, but there are certain employment use exemptions)
Colorado	SB 21-190	Yes (data-level)	Yes (entity and data-level)	Yes (consumer definition (Both) and employment records exemption)
Connecticut	CTDPA, as amended	Yes (entity and data-level)	Yes (entity and data-level (latter only if compliant))	Yes (consumer definition (Both) and certain employment use exemptions)
Utah	SB 227	Yes (entity and data-level)	Yes (entity and data-level(latter only if compliant))	Yes (consumer definition (Both) and certain employment use exemptions)
Virginia	SB 1392	Yes (entity and data-level)	Yes (entity and data-level)	Yes (consumer definition (Both) and certain employment use exemptions)

Submitted via email to JUD@legislature.maine.gov

December 1, 2023

Maine Joint Standing Committee on Judiciary
c/o Legislative Information Office
100 State House Station
Augusta, ME 04333

RE: LD 1977/HP 1270 An Act to Create the Data Privacy and Protection Act

Dear Chairpersons Carney and Moonen:

The Confidentiality Coalition respectfully submits the below comments on LD 1977/HP 1270, An Act to Create the Data Privacy and Protection Act (LD 1977) to the Maine Joint Standing Committee on Judiciary (the Committee).

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, and others, committed to advancing effective health information privacy and security protections. Our mission is to advocate policies and practices that safeguard the privacy and security of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

The Confidentiality Coalition strongly supports robust privacy protections for all personal health data, and has long called for federal legislation that would provide strong national privacy and security protections, similar to those under the Health Insurance Portability and Accountability Act and its implementing regulations (HIPAA), for personal health information that falls outside HIPAA. We have enclosed for your consideration a copy of the Coalition's "Beyond HIPAA Privacy Principles" which set forth our position on this important issue.

While we support the goals of LD 1977 in requiring strong privacy protections, transparent privacy policies and consumer rights with respect to their personal data, we are concerned that LD 1977 proposes to apply to personal health data that is already subject to HIPAA, which provides extensive privacy and security protections and rights for such information, referred to

as “protected health information” (PHI). For example, among other things, HIPAA requires risk-based security safeguards for PHI and a patient’s written authorization for any use or disclosure of PHI beyond certain health care functions. In addition, it requires notification of any breaches of unsecured PHI and provides patients with extensive rights with respect to their PHI, including the right to access, amend, receive an accounting or confidential communication of their PHI and to receive a notice of privacy practices explaining how their PHI is used and disclosed and how to exercise their privacy rights. The HIPAA framework is well-established, its requirements clearly understood by the health care organizations to which it applies, and its rights and protections utilized and trusted by patients.

Thus, there is no need to have LD 1977 apply to PHI and, more importantly, its application to PHI would have significant unintended adverse consequences. These include redundancies and duplication of effort by HIPAA covered entities and their business associates (HIPAA entities) and compliance challenges as they attempt to reconcile and apply inconsistent and potentially conflicting definitions, terms, concepts and requirements. Ultimately, the increased compliance burden on the health care system will be borne by the very consumers LD 1977 is intended to benefit without any commensurate benefits to them and likely increased confusion and uncertainty.

It is for this reason that other states[1] that have passed comprehensive data protection laws similar to LD 1977 have all clearly exempted PHI and, in many cases, HIPAA entities, from their ambit. We strongly urge the Committee to do the same in LD 1977.

Thank you for your consideration of our comments. Please do not hesitate to contact me at tgrande@hlc.org or 202-449-3433 if you have any questions.

Sincerely,

Tina O. Grande

Tina O. Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council

[1] As of September 2023, thirteen states - California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia - have enacted comprehensive data privacy laws.

15 Casco Street Freeport ME 04033 | llbean.com

December 6, 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: Summary of "Trackers"

Dear Sen. Carney, Rep. Moonen, and members of the Judiciary Committee:

Representative O'Neil's November 8, 2023 testimony before the Committee regarding LD 1977 referenced L.L.Bean's use of "trackers" on llbean.com. The reference seemed to imply that L.L.Bean might be doing something inappropriate. To avoid any further misunderstanding, I am writing to provide a brief summary of the use of "trackers," more commonly referred to as "tags" and "cookies," that are widely used across the internet by all industries, and even by the Maine Legislature.

Cookies are used for various purposes including for website functionality, analytics, and retargeting. Some of the cookies on the L.L.Bean site are aimed at ensuring the website is functioning as intended. Other cookies are placed on the website with L.L.Bean's permission by vendors with whom we contract. These so-called "third-party cookies" are used for analytics or for personalized advertising. For example, analytics cookies are used to determine the number of visitors to a specific page so that we can gauge customer interest. Given the various uses for cookies, it is not unusual to have large numbers of cookies running in the background of a visitor's session with a website.

Downloadable tools can detect the presence of cookies on a website. These tools simply provide a name to the cookie, but importantly, they do not provide an explanation of its use. In fact, one of these downloadable tools, Ghostery, recently identified seven cookies on the Maine Legislature's own website. Much like L.L.Bean, some of these are likely to ensure the website is operating as intended.

It is important to note, too, that consumers are notified about the use of cookies upon navigating to the site and have options to manage the use of their Personal Information specifically via cookies. A consumer can choose to block cookies via their browser, they may use a browser-based opt out signal also known as the Universal Opt-Out mechanism, or they may make a request directly with a business to opt-out of targeting advertising.

Thank you for the opportunity to offer some clarity on this issue. Should you have any additional questions or concerns, I would be happy to try to answer them at the December 11 work session.

Sincerely,

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

ACLI
Financial Security for Life

To: The Honorable Anne Carney, Senate Chair
The Honorable Matt Moonen, House Chair, Maine Committee on Judiciary
From: Jill Rickard, Vice President - State Relations, ACLI
Date: December 8, 2023
Re: Privacy Legislation

Dear Senator Carney, Representative Moonen, and Distinguished Committee Members:

On behalf of ACLI, I write to provide additional information as to why it is crucial to the life insurance industry that any entity subject to the Gramm-Leach-Bliley Act (GLBA) be exempted from any new comprehensive state privacy legislation.

For over 175 years, life insurers have ably managed consumers' confidential health and financial data. Insurers must collect and use personal information to perform essential business functions - for example, to underwrite applications for new insurance policies, pay claims submitted under these policies, and provide longevity protection through retirement products.

Appropriately, insurers have long been subject to the federal GLBA, one of the most comprehensive information privacy laws to date. The requirements of the GLBA reflect a critically important balance between consumers' legitimate privacy concerns and the proper use of personal information to the benefit of existing and prospective customers. The GLBA imposes transparency, confidentiality, and security obligations on all financial institutions, including life insurers, with respect to the collection, disclosure, and protection of consumers' nonpublic personal information and personally identifiable information.

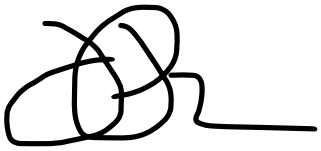
The life insurance and financial services industries would be uniquely affected by the establishment of new general privacy requirements at the individual state level. Many other states, including Connecticut, Colorado, Delaware, Virginia, and Utah, have exempted entities regulated by GLBA from their laws based on their recognition of the adverse impacts to these industries of new comprehensive state privacy laws.

To properly serve their customers, insurance companies must be able to easily share a customer’s personal information within their holding company framework. Exempting only data subject to the GLBA would place financial institutions in the untenable position of trying to parse through their files to determine which information is exempt and which is not. It would also create uncertainty based on duplicative and even conflicting rules. For these reasons, the exemption should apply to all entities and data subject to the GLBA.

Without an entity-level GLBA exemption, any new state privacy law would add complexity and expenses of implementation and would inevitably result in conflicting scopes, definitions, notice requirements, and consumer rights. Importantly, consumers benefit from privacy requirements that are consistent across state borders. Differing privacy standards lead to consumer confusion based on differing rights and protections, obstruct the flow of information, and impede interstate commerce. They also risk consumer frustration over divergent rights to control their personal information based on where they live or with whom they do business. To illustrate, a life insurance policy involves multiple parties and transactions that may take place in different states. An insured may live in Maine, but the policy beneficiaries may not, and the insurance company would likely be domiciled elsewhere. If the states involved have different privacy laws, an insurance company would have the undue burden of determining the situs of a transaction and apply the appropriate protections.

ACLI is proud of our member companies' longstanding role as conscientious and responsible guardians of their customers' personal information. We remain strongly committed to the proper use and protection of consumer data. I would be happy to discuss or provide any additional information that is helpful to you or your committee.

Sincerely,



Jill Rickard
202-624-2046 t
jillrickard@acli.com

December 8, 2023

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

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

RE: Oppose Unless Amended – LD 1977, Data Privacy and Protection Act

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

On behalf of the Securities Industry and Financial Markets Association (SIFMA),[1] we thank you for the opportunity to provide comments on LD 1977, which would enact the Data Privacy and Protection Act. SIFMA brings together the shared interests of hundreds of securities firms, banks and asset managers located across the country. There are more than 25,400 people employed by the financial services industry, more than 900 financial advisors, and 19 broker-dealers who call Maine home.[2] SIFMA's mission is to support a strong financial services industry, investor opportunity, capital formation, job creation, and economic growth.

SIFMA commends the Committee for its dedication to protecting the privacy of Maine residents and for hosting hearings to listen to stakeholders about their concerns with LD 1977. Financial institutions have been and remain committed to adhering to specific, effective and reasonable privacy laws and regulations for decades. Although LD 1977 provides a good foundation for consumer protections, it falls short in harmonizing with existing federal privacy laws and regulations applicable to financial institutions, thus creating unnecessary, overlapping regulation. The bill also includes a private right of action, which is not supported by financial institutions and the business community more broadly as such litigation is often frivolous and generally inordinately burdensome on companies while providing consumers with little, if any, benefit or compensation for losses.

[1] SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. For more information, visit http://www.sifma.org.
[2] US Department of Labor - Bureau of Economic Analysis (202s)

1. **There is no exemption for financial institutions regulated under the Gramm-Leach-Bliley Act (GLBA).**

SIFMA requests an amendment to include an exemption for financial institutions and their affiliates regulated by GLBA, to prevent regulatory conflict and limit consumer confusion. As currently drafted, LD 1977 does not include an exemption for financial institutions or their affiliates whose privacy and data practices are already robustly governed by GLBA.

Enacted in 1999, the GLBA established comprehensive federal law that, among other things, governs financial institutions' privacy and data protection controls, including disclosure of privacy practices to customers, cybersecurity controls, and restrictions on the unauthorized sharing of non-public consumer financial information with significant oversight and enforcement by financial regulators. As a result, financial institutions covered by GLBA already have comprehensive, mature privacy programs in place, thus making required compliance with LD 1977 duplicative, conflicting, and confusing for customers. An exemption for GLBA-regulated entities would help to alleviate that confusion.

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

In total, 13 states have enacted comprehensive consumer data privacy laws aimed at providing consumers with additional rights over their personal information. In fact, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Tennessee, Texas, Utah and Virginia have exempted entities subject to GLBA and only two states - California and Oregon, only exempt data from their comprehensive data privacy law. If enacted as currently drafted, Maine would be the only state without any GLBA exemption.

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

We also request consideration of a change in the enforcement mechanism in the bill to give exclusive authority to the Maine Attorney General (AG). As currently drafted, LD 1977 would allow for the Maine AG to bring a civil action against a covered entity as well as Private Right of Action (PRA). The Maine AG's office is the most familiar with industry standards and best practices. Consumer protection is a prime duty of the Maine AG, and they are very active in bringing lawsuits and enforcement actions against companies that violate state laws.

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

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

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

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

Sincerely,

/s/

Stephanie Klarer
Assistant Vice President
SIFMA

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

Stocco, Janet

From: Handler, Howard <HHANDLER@nicb.org>
Sent: Saturday, December 9, 2023 4:51 PM
Subject: NICB | Consumer Data Privacy Bills

Dear Chair Carney and Members of the Joint Committee on Judiciary:

I am reaching out related to the comprehensive consumer data privacy bills considered by the Joint Committee on Judiciary. **In short, if an exemption for 501(c)(4) organizations – as is provided in the comprehensive consumer data laws of California, Florida, Tennessee, Montana, Utah, and Connecticut -- is not provided in the finished product, we respectfully ask for an exemption specific to the National Insurance Crime Bureau (NICB). Comprehensive consumer data privacy laws enacted in Virginia, Iowa, Texas, Delaware, and Oregon provide NICB specific entity-level exemptions, as do leading bills introduced in Ohio, Washington (state), Kentucky, Hawaii, and Wisconsin.**

For more than 112 years, the National Insurance Crime Bureau (NICB) is the nation's premier not-for-profit organization exclusively dedicated to leading a united effort to prevent insurance crime and fraud through intelligence-driven operations. NICB sits at the intersection between the insurance industry and law enforcement, helping to identify, prevent, and deter fraudulent insurance claims. NICB maintains operations in every state around the country, including in Maine where NICB analysts and agents work daily with federal, state, and local law enforcement and regulatory agencies.

Recognizing the adverse impact of insurance crime on the citizens of Maine, the legislature enacted a law requiring Maine insurers to report suspected insurance fraud to the Bureau of Insurance. In support of that mandate, NICB collects insurance fraud information from insurers through NICB's Fraud Bureau Reporting Program (FBRP). The FBRP connects through the National Association of Insurance Commissioner's OFRS system to make available fraud reporting information to Maine regulators. In addition to mandating that information be provided to the State, the Maine legislature also recognized the importance of reporting insurance crime and fraud information to law enforcement by enacting statutes providing civil immunity to insurers and insurance professionals delivering such information.

Importantly, as an insurance-support organization, NICB is already covered and limited by the Maine Insurance Information and Privacy Protection Act which sets standards for the collection, use and disclosure of personal information. Additionally, due to our law enforcement partnership, NICB is regularly audited by the FBI for cybersecurity standards.

While the introduced bills do provide limitations on the reach of the proposed law for purposes of preventing, detecting, and protecting against fraud and illegal activity. Although our charter aligns with this provision, and NICB would benefit from this section, this language is not meant to provide a

wholesale entity-level exemption – meaning that, notwithstanding our ability to continue fighting fraud and other insurance crimes consistent with our charter, NICB would still be subject to consumer requests to, for example, delete their data. Even for non-viable requests under the statute, NICB would nevertheless bear the burden of proving to each consumer directly, or in litigation, that NICB's activities fall within the limitation. The obligation to do so would strain our organization's resources to such a degree that our operations, and ability to protect Maine consumers, would be significantly encumbered.

The policy reasons for exempting NICB from these burdens are several-fold. First, NICB provides significant benefits to the millions of consumers who are victims of insurance fraud. Second, as a non-profit organization that serves a public interest, NICB is not equally situated with private entities that typically establish more complex compliance infrastructure for private-sector-related obligations. Furthermore, NICB's required responses to individual consumer requests would likely expose otherwise covert criminal investigations. In addition, imposing what is essentially a "compliance, response, reporting, and litigation" obligation – without any benefit to consumers – is wholly inconsistent with Maine's civil immunity provisions for fraud reporting referenced above. Finally, NICB would not be afforded protection for our operations relating to our natural disaster response in which we provide critical disaster data and imagery to first responders at no cost.

Thank you for your review and consideration of this matter. I would love the opportunity to discuss this request in further detail.

NATIONAL INSURANCE CRIME BUREAU
Leading the Fraud Fight

Howard Handler, MPPA
Senior Director, Government Affairs
Office of Strategy, Policy, and
Government Affairs
National Insurance Crime Bureau
m. 312.771.3974

AdvaMed
Advanced Medical Technology Association

1301 Pennsylvania Avenue, NW
Suite 400
Washington, D.C. 20004
P :: 202.783.8700
F :: 202.783.8750
W:: AdvaMed.org

December 11, 2023

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

Representative Matt Moonen, Chair
Committee on Judiciary
100 State House Station
Augusta, ME 0433

RE: LD 1977, An Act to Create the Data Privacy and Protection Act
LD 1902, An Act to Protect Personal Health Data

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

AdvaMed, the MedTech Association, is the largest medical technology association, representing the innovators and manufacturers transforming health care through earlier disease detection, less invasive procedures, and more effective treatments. Our more than 450 members range from small, emerging companies to large multinationals and include traditional device, diagnostic, and digital health technology companies.

We appreciate Representative O'Neil's efforts to tackle this complex issue and engage on LD 1977 and LD 1902. As was stated during AdvaMed's verbal testimony during the October 17 hearing and work session, we have concerns with LD 1977 unless amended and we support LD 1902. Unlike other industries, health care is already subject to extensive regulation at the federal level. Our work on similar legislation around the country -- and our goal for this bill – is focused on avoiding conflict between state and federal laws and ensuring both the continued delivery of high-quality patient care and ensuring essential health research is not disrupted.

Our goal is to ensure clarity on how healthcare now, and in the future, will be safeguarded for patients and providers. Currently LD 1977 legislation does not advance these objectives. However, LD 1902, which addresses health care data does. We would request that LD 1902 be incorporated into LD 1977. If the health care bill is not combined with the general privacy bill, or if the general privacy bill does not include the exceptions that are currently in the health data bill, patient care could be compromised under either model.

Under HIPAA, PHI cannot be sold without the express written authorization of the patient, so it is only the collection and sharing of data that is of concern. An opt-out model (to collecting and sharing health data) generally does not make sense in the context of medical devices used in patient care and is inconsistent with how care is performed and managed (e.g., one would generally refuse the CT scan instead of opting out of collecting and sharing the health data).

In many instances, medical technology companies do not directly interface with patients. Often, physicians select the medical device and choose to use it with certain patients based on their clinical judgment. The burden of obtaining the opt-in consent would fall on the clinician, who is already pressed for time.

Protected Health Information (PHI) under HIPAA may be collected and shared for treatment, payment, safety, internal operations, and public health purposes without the opt-in or affirmative express consent of the patient. Collecting and sharing medical device data may be needed to coordinate care and enable clinicians to make more informed care decisions when a patient is incapacitated and not able to opt in or provide consent.

Consent fatigue, meaning requiring specific and potentially repetitive consent for the permutations of data uses that support essential health care purposes is an unworkable approach, can result.

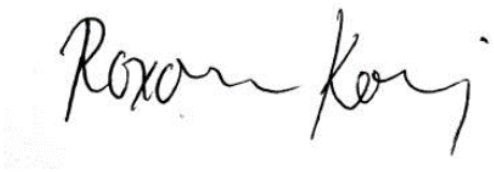
- A patient may interact with many different technologies during a single episode of care.
- For example, an individual presenting with a heart attack may interact with more than a dozen different technologies to diagnose and treat the condition—e.g., diagnostics in the ambulance, vitals, electronic medical records, electrocardiogram, echocardiogram, pulse oximetry, fluoroscopy, anesthesia machine, implanted device to maintain proper heart function, and many more.
- Requiring consents (in the form of opt-ins) specific to each device during an emergency would waste valuable time.
- In less urgent scenarios, repeated consent could more detrimentally burden the very sick or elderly.

Furthermore, by including a private right of action, we are most concerned about the potential for frivolous lawsuits, as some will exploit such provisions to harass businesses to extract settlements, burdening the legal system and siphoning resources that could go to R&D. This could have a chilling effect on innovation, hindering the development of life-saving and life-enhancing products and services.

To date, fourteen states have passed their data privacy reform laws that include the healthcare amendments addressing continued delivery of high-quality patient care

and ensuring essential health research is not disrupted. We encourage the committee to follow suit and ensure that there continues to be alignment across the country. Thank you and we look forward to working with the committee moving forward.

Sincerely,



Roxolana Kozyckyj
Senior Director
AdvaMed

Comment on Privacy Legislation – Part 2

LD 1977

December 9, 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.

This letter is intended to supplement our previous testimony in support of our position that health care entities should be given the same exemption from LD 1977 as has been proposed for government entities. Our comments make references to certain sections of LD 1977 as that bill appeared to be the possible vehicle for your action; however, our concerns would apply to all of the legislation to the extent that one of those bills is used as the vehicle to regulate privacy in a manner that would affect healthcare providers.

We have a number of points we would like you to consider.

First, the exemption we seek is for industries whose primary data set(s) are already regulated by robust privacy statutes/regulatory regimes.

Healthcare providers collect data that is necessary for accurate patient identification, treatment, follow-up communication with patients, processing of insurance coverage, billing, and utilization review. Data collected for those purposes is regulated by HIPAA and by state healthcare and insurance privacy laws. It is difficult to state, definitively, that there is no data, or item of information, collected for a legitimate business purpose that falls outside of the regulatory reach that is proposed by L.D. 1977 et al. because some of the proposed definitions of data are new and, in some ways, vague (e.g., what is derived data?). What is clear, however, is that any such data we might have is ancillary to the primary purposes of a

healthcare provider's data collection purposes and is insignificant relative to the health data which is subject to HIPAA and other such laws.

Second, the Committee received *no* testimony that healthcare providers were misusing their ancillary data in any way. This committee has historically not legislated on theoretical issues but, instead, has focused on actual problems that have been experienced by Maine people. Inasmuch as there have been no allegations made against healthcare providers, healthcare providers should be exempt.

Third, the legislation proposes to exempt government. Statements by proponents that no categorical exemptions are appropriate fly in the face of their simultaneous argument that government entities – which possess substantial amounts of sensitive data should be exempt.

Fourth, the legislation creates a number of unfunded administrative mandates even if an entity never "sells" data or undertakes any other disfavored action with it. The legislation is not a simple list of prohibitions. It constructs a new, master regulatory scheme for the collection and use of data that is not only agnostic as to existing federal and state privacy statutes but, also, ignores the meaningful, inherent difference between the operations of entities such as healthcare and financial services entities on the one hand, and internet and cable companies on the other. The legislation contains several new regulatory requirements, no matter how an entity uses the data.

The following are new mandates:

- §9606 – Policies, Practices and Procedures
- §9608 – Privacy Policies
- §9609 – Regulates how to obtain consent
- §9611 – Managing individuals' control over the data
- §9617 – Data Officer (including a new mandate to have a data privacy program and a data security program; a new mandate to conduct a "privacy impact assessment" every other year.)

Healthcare providers are subject to regular criticism in the State House about the amount of our administrative costs and how those costs impact the cost of healthcare for the public. Healthcare providers are willing to accept some unfunded new administrative tasks, but only upon a showing of real need. No such showing has been made here.

Fifth, the legislation is flawed. The bill has not been enacted anywhere in the country; it contains novel definitions and concepts; and no state agency is being given responsibility to do rulemaking or provide guidance to the regulated community. If the Committee moves forward with privacy legislation, and regardless of whether healthcare entities are exempted, we would encourage you to use the Connecticut law as your template.

Finally, the decision to exempt healthcare providers this session is not a final decision. As you know, the focus of concern for this legislation are the apps and large social media companies. The sponsor repeatedly cites Facebook and Google while presenting her bill. The Committee can begin by pursuing the identified problem areas and then, if and when concerns about healthcare providers arise, bring focused legislation that addresses those concerns.

Members of our coalition are happy to meet with the Committee to discuss our concerns.

Thank you.

re: critiques of GLBA by consumer advocates

Protect consumer privacy: Repeal GLBA's privacy provisions

Jul 30, 2020 | Save This 0

Robert Gellman
Nonmember Contributor (/about/person/0011a00000DlG2qAAF)

How do the privacy protections in the Gramm-Leach-Bliley Act — the well-known banking law — help consumers? The short answer is that the GLBA does almost nothing to help consumer privacy. Understanding that the GLBA is essentially a privacy fraud is important because exemptions for the GLBA are features of some state and federal privacy bills.

Let's look at the provisions of the GLBA. The privacy part of the law provides two — and only two — provisions for consumers. First, each financial institution must have a privacy notice. That's something but not much. We know that consumers don't read privacy notices, although others — regulators, consumer groups, reporters — do. Notices used to be an annual event, but the banks lobbied Congress to dilute that obligation. In any event, at this stage, law or not, banks would have privacy notices anyway.

Second, the GLBA provides that a financial institution that wants to share personal information with a non-affiliated third party — anyone outside the corporate family — must give consumers the chance to "opt out" under some circumstances. Even if a consumer doesn't opt out, the law prevents sharing of account and credit card numbers for third-party marketing uses. But the opt-out does not apply to joint marketing agreements with other financial institutions. That means that if one financial institution wants to share consumer information with another financial institution, it can do so through a joint marketing agreement, and consumers have no opt-out rights.

Some financial institutions don't bother offering opt-outs, choosing not to share information with third parties at all. The minor benefits of data sharing aren't worth the bother of telling consumers about their opt-out rights and processing the opt-outs.

That's it for the GLBA and privacy.

There is nothing else in the law for consumer privacy. No limits on data collection. No right of access or amendment. No restrictions on use. Some financial institutions have dozens of lines of business, and they can share consumer data freely with all those affiliated businesses without restriction from the GLBA. The control on disclosure for non-affiliate sharing is not all that meaningful because few consumers read notices and even fewer bother to opt out.

does the security requirement count here? No, because we're talking here about privacy protections and not security obligations.

In some ways, the GLBA is worse for consumers than nothing. At this late date, it actually harms consumer privacy interests. The California Consumer Privacy Act offers an example. The CCPA does not apply to personal information collected, processed, sold or disclosed pursuant to the GLBA. The CCPA doesn't just effectively exempt financial institutions; it exempts any information that a financial institution discloses to others. The exemption apparently follows the data.

Let's try an example: Suppose a bank offers consumers an opt-out of data sharing to third parties. With few exceptions, the usual opt-out rate rarely exceeds a few percentage points. If the bank discloses consumer data to a third party, that data is exempt from the CCPA in the hands of the recipient, as well.

In California, the effect of the GLBA exemption is to deny consumers the rights that they would have with respect to data that banks disclose to third parties, rights that they would have but for the CCPA's GLBA exemption. In California, the GLBA is effectively a get-out-of-regulation-free law for consumer data originating with financial institutions. It's an incredibly broad exemption, to say the least.

Not all state law exemptions for federal privacy laws are terrible. The CCPA also exempts credit reports under the federal Fair Credit Reporting Act. That exemption is OK because the FCRA is probably the best federal privacy law, with real limits on the use of credit reports and real rights for consumers.

In privacy battles in Congress and states, banks use the GLBA as a privacy shield. Don't regulate us, they argue, because we are already regulated federally for privacy. But the federal regulation is so thin that it offers no meaningful privacy protection to consumers. In effect, the only real beneficiaries of the GLBA privacy provisions are the financial institutions themselves. They use it to avoid real privacy regulations.

Consumer privacy would be enhanced by actually repealing the privacy provisions in the GLBA. That is just how perverse the GLBA privacy provisions are now. Banks would have privacy notices anyway, and repeal would make financial institutions fully subject to the CCPA and perhaps other state laws, too.

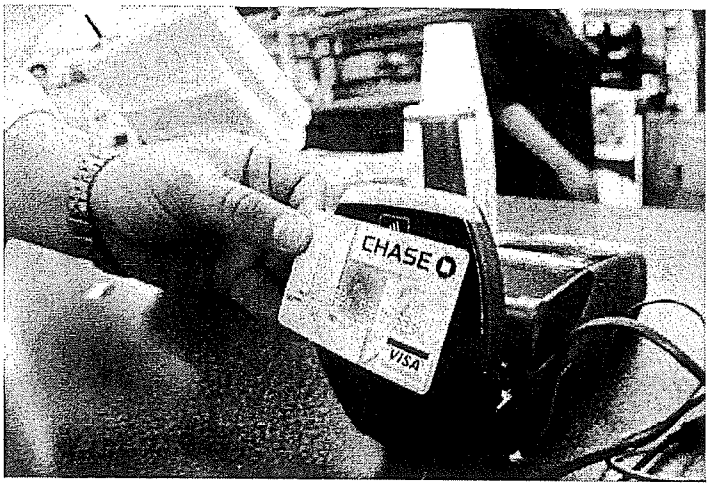
For the moment, a better result would be for federal and state legislators to not provide a GLBA exemption in their privacy laws. California should repeal its GLBA exemption at the next opportunity. At this time, however, repealing the privacy parts of the GLBA is just a fantasy.

Photo by Sharon McCutcheon on Unsplash

ACLU

NEWS & COMMENTARY

Why Don't We Have More Privacy When We Use A Credit Card?



Jay Stanley, Senior Policy Analyst, ACLU Speech, Privacy, and Technology Project
August 13, 2019

Yesterday, we published a piece on cashless stores and how they are bad for low-income communities, undocumented people, and many merchants – and for privacy. In this post, we take a closer look at the privacy problems with electronic payment systems such as credit cards.

Simply put, cash is good for keeping people from prying into our lives, and credit cards are not. That starts with the stores and restaurants where we use them. When we use a credit card to buy something, the seller can learn our first and last name, which, combined with a zip code (either requested at the register or guessed at, since most transactions take place near where people live), can be used to learn a lot more about us. Using "data appending" services, the merchant may then be able to acquire our email and postal addresses and our telephone number. That, in turn, permits a merchant to tap into the databases of the giant data broker industry and learn anything from demographic information to our employment, marital, and homeownership status to our interests and hobbies and even our medical conditions. A

retailer may also add our personal data, including purchases, into a "data cooperative" where it will become available to all the other participating companies as well.

It is true that there are other ways for merchants to track people and their purchases, including those made with cash – from loyalty programs to Bluetooth tracking to face recognition. It is also theoretically possible that cash could be tracked using serial number readers, but we know of no existing infrastructure for doing that. Cash is not a guarantee of privacy, but it is still far more privacy-protective than credit cards.

A big reason that electronic payment systems threaten privacy is that they introduce a middleman. When a middleman becomes part of the process, that company often gets to learn about the transaction – and under our weak privacy laws has a lot of leeway to use that information as it sees fit.

The primary middlemen in most non-cash transactions today are the oligopolistic credit card companies (Visa has around 60% of the credit and debit card market, MasterCard has 25%, American Express 13%, and Discover 2%). Mobile apps such as Apple Pay, Venmo, and Square are also gaining a foothold.

But, regardless of who plays that role, Congress has bent to the will of the financial industry and refused to enact adequate privacy protections. In 1999, Congress passed the Gramm-Leach-Bliley Act (GLB). Although it has often been described as a "financial privacy law," Gramm-Leach created nothing more than a weak "fig leaf" privacy standard. The real effect of the law, which manages to be both extremely complex and weak, has been to ratify the abandonment of customer privacy by an industry (banking) that, once upon a time, prided itself on discretion:

- Under GLB, companies can sell their customers' financial data to anyone they choose, including credit card information such as the date, amount, and recipient of charges, and the personal details consumers provide when they fill out applications. Consumers have no privacy under federal regulations unless they affirmatively take steps to "opt out" of this sharing, repeating the process for each and every financial service provider who may have data about them. (Personally,

I've found that opting out with a credit card issuer, which should be made easy, is like pulling teeth.) That means these companies could be collecting a vast amount of detail about our lives: how much we spend on travel, restaurants, political or religious donations, liquor stores, sex shops, and on and on. And of course, that kind of information is more powerful and revealing when combined with other data.

- Even this opt-out option is not available for consumers to stop credit card companies and issuing banks from sharing this data with their financial affiliates and financial "joint marketers," a vaguely defined term that provides a giant loophole in privacy protections.
- Nor do consumers get the transparency they should as to how their information is being shared. Companies are required to provide "privacy notices," but they don't have to reveal the specific information that they share with third parties, or the names of those parties – only the *categories* of information they share and the *categories* of organizations shared with. When the journalist Kashmir Hill tried to find out what was being done with her Amazon/Chase credit card data, both companies basically stonewalled her. The impossible number of click-through contracts we're swamped by online makes these notices just part of a wave of fine print and even less meaningful.

In 2002, citizens in states around the country began to rebel against this rule by passing their own, tougher "opt-in" financial privacy rules requiring people's affirmative permission before their information could be shared. In North Dakota, for example, the battle over a proposed ballot measure to require opt in for the sharing of financial data was a true David and Goliath story. On one side were wealthy and powerful financial interests including big, national banks and insurance companies, which ran a sophisticated media campaign opposing the measure, and outspent the pro-privacy forces by a factor of at least 6-to-1. On the other side was a group of citizen-volunteers led by Charlene Nelson, a homemaker and mother of three working out of her home. Until a last-minute $25,000 contribution by the ACLU for radio ads, the grassroots effort had reported donations of just $2,450.

Yet despite this lopsided battle, the ballot measure won with over 70 percent of the vote.

Unfortunately, in the face of this rebellion by North Dakota, and another in California, as well as similar "opt-in" laws in some other states, financial interests ran to Congress and were able to use their sway to thwart states' ability to pass stronger standards than GLB. In many crucial areas, GLB was made the ceiling rather than the floor for privacy protection. (A similar preemption battle is shaping up today over consumer internet privacy legislation.)

The result is that we now have a situation in which consumers' credit card and other financial information is bought, sold, traded, and accumulated by the private sector at an ever-faster pace – and made all the more convenient and available for access by the government.

For example:

- The major credit card companies have quietly turned their access to consumer transactions into a new revenue stream, according to AdAge. And not just the networks like MasterCard and American Express, but also issuing banks. "Representatives from the four top credit card issuers – Bank of America, Citi, Chase and Wells Fargo – declined to discuss details of how they use purchasing data internally," a credit card analyst wrote in 2009, adding that "a spokeswoman from a banking industry trade group acknowledged that the practice is common."
- Google has made secret data-sharing agreements with credit card companies and, according to the Washington Post, now has access to 70% of the nation's credit and debit card transactions. Google, which refused to explain how its new system works, uses it to track the success of its online ads, which already rely on access to highly personal data about consumers' search, browsing, and location histories. Although advertisers regularly protest that ad data is based on anonymized information, that system could only work if Google connects people's online clicks to their real offline identities.

- "Behavioral scoring" by credit card companies can be used in unfair ways. One man who had paid his credit card off in full every month received a notice that his credit limit was being lowered. When he asked why, according to ABC News, he was told it was because *other shoppers* at certain stores he patronized had proven to have poor credit records. It's very easy to see how that kind of analytics, especially when done in secret, could have strong, even if unintentional, discriminatory consequences.

The current ecosystem of privacy invasion needs to stop, and is one more reminder why Congress needs to enact strong, comprehensive privacy legislation – and why we need to preserve cash as a widely-available option for making purchases in our society.

Learn More About the Issues on This Page

Privacy & Technology **Financial Privacy**

Consumer Privacy

Related Content

Press Release

ACLU Applauds Introduction of Bipartisan Government Surveillance Reform Act to Rein in Warrantless Government

epic.org / ELECTRONIC PRIVACY INFORMATION CENTER

STATEMENTS

EPIC Statement re: Data Privacy Act of 2023

February 27, 2023

DOWNLOAD PDF 226.6KB

CONTENTS

Dear Chair McHenry and Ranking Member Waters:

We write to you regarding tomorrow's markup of the Data Privacy Act of 2023 proposed by Chairman McHenry.[1] EPIC appreciates your attention to the need for improved privacy protections in the financial services sector. However, this bill's reliance on an outdated system of notice-and-choice does not meaningfully protect privacy and is out of step with recent developments in privacy legislation.

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC is a leading advocate for consumer privacy, including in the financial sector, and has appeared before this Committee on several occasions.[3]

The Bill's Focus on "Notice and Choice" is Outdated

The Data Privacy Act unfortunately relies on an outdated system that does little to protect privacy by extending the notice-and-choice provisions of the Gramm-Leach-Bliley Act (GLBA). GLBA requires financial institutions to provide their customers with privacy notices. This notice-and-choice regime, in which consumers are expected to read extensive privacy policies, makes it impossible for consumers to meaningfully protect their privacy. Even if consumers had the time to read every privacy policy and statement, they would in most cases come away with woefully incomplete information. Such policies tend to be vague and expansive, designed to protect a company from liability rather than inform privacy-conscious consumers.

Notice and choice simply does not work. We have all received these notices in the mail – a pamphlet from our bank or credit card company explaining all the ways they disclose our data to other entities. Under GLBA, the notice must give consumers the option of opting-out of a limited amount of data sharing. But in reality, very few consumers read these notices or exercise their opt-out option. Even though the Data Privacy Act provides a new deletion right for consumers, this 1) still puts the burden on consumers to protect their privacy; and 2) is not a meaningful right as so few consumers will be aware it exists. The Data

Privacy Act assumes that consumers have the time, knowledge, and know-how to read company legalese and exercise their rights. This framework simply hasn't worked.

Rather than move past this outdated notice-and-choice system, the Data Privacy Act simply adds another layer of notice – notice must now be given at the point of collection rather than just at the point of disclosure. This is out of step with the progress made by the House Energy & Commerce Committee last Congress on the American Data Privacy and Protection Act ("ADPPA"). Sponsored by Democratic and Republican leaders on the Committee, ADPPA takes the burden of protecting privacy off the consumer and instead imposes a data minimization standard[4] that requires businesses to limit the collection, use, and retention of personal information to what is reasonably necessary to provide the product or service the consumer has requested.[5] This is very different than the purported "data minimization" provosions of the Data Privacy Act that simply require that institutions limit their collection of personal data for the purposes they list in their "privacy policies" – policies that no one reads. Under this standard, companies would be permitted to collect and use data for purposes that are not consistent with what a reasonable consumer would expect, so long as they disclose the purpose and get consent. This gives incredible leeway to companies to determine the purposes for which they can collect data.

On the contrary, ADPPA's baseline requirement that companies must limit their data collection to what is reasonably necessary and proportionate "to provide or maintain a product or service requested by the individual" (or pursuant to certain enumerated purposes) means that data collection will more closely match consumer's expectations. This is the standard that the Committee on Financial Services should be imposing on entities subject to the GLBA.

The Committee on Financial Services simply should not advance a bill in 2023 that uses a notice-and choice-regime, particularly when paired with a preemption provision that prevents states from enacting stronger protections. The standard has changed. The Committee should not advance legislation that purports to be a privacy bill unless it includes a data minimization standard similar to what is set forth in the bipartisan American Data Privacy and Protection Act.

Data Aggregators Should Not be Added to GLBA Without Stronger Privacy Protections

The Data Privacy Act would add "data aggregators" to the types of financial institutions covered by GLBA. "Data aggregators," more commonly known as "data brokers," buy, aggregate, disclose, and sell billions of data elements on Americans with virtually no oversight. For these companies, consumers are the product, not the customer. Most consumers do not even know that data brokers exist, as they have no direct relationship with them. This comes at huge cost to individual privacy and our national security.[6] Data brokers have sold data on military personnel to foreign adversaries[7] and facilitated elder scams.[8] Foreign governments seeking personal data on Americans can simply purchase it from a data broker – no cyberattack needed.

Given the lack of regulation of this industry, it would seem to be a step in the right direction to include data brokers as covered entities under the GLBA. Unfortunately, that is not the case. Adding data brokers to GLBA simply allows them to evade stricter regulations, whether from existing state privacy laws or stronger national standards that may come into effect in the coming years. The so-called privacy protections in GLBA are so weak that some consumer advocates have called for their repeal and said that "In some ways, the GLBA is worse for consumers than nothing."[9]This is due to the success that entities regulated by the GLBA have had in lobbying state lawmakers to exempt them from stronger state privacy laws. Any data collected pursuant to GLBA is exempt from the California Consumer Privacy Act. In the other four states that have passed comprehensive privacy laws (Colorado, Virginia, Connecticut, and Utah), entities governed by GLBA are exempted entirely, even for data that is not covered by the law. This is why data aggregators would like

to be covered by GLBA, as proposed in this bill – such coverage exempts them from stronger privacy laws. The Committee should not include data aggregators under GLBA coverage unless the privacy protections in this bill are substantially improved and set a higher standard than existing state laws.

We ask that this letter be entered in the record. EPIC looks forward to working with the Committee on these issues.

[1] Amend. in the Nature of a Substitute to H.R.1165, the "Data Privacy Act of 2023," https://docs.house.gov/meetings/BA/BA00/20230228/115381/BILLS-118-HR1165-M001156-Amdt-12.pdf.

[2] EPIC, *About EPIC*, https://epic.org/about/.

[3] *See, e.g, Examining the Current Data Security and Breach Notification Regulatory Regime: Hearing before the Subcomm. on Fin. Inst. and Consumer Credit of the H. Comm. on Fin. Services* (testimony of Marc Rotenberg, EPIC Exec. Dir.) 116th Cong (2018), https://epic.org/documents/examining-the-current-data-security-and-breach-notification-regulatory-regime/; *Examining the EU Safe Harbor Decision and Impacts for Transatl. Data Flows: Hearing before the Subcomm. on Commn'c and Tech. of the H. Comm. on Fin. Services* (testimony of Marc Rotenberg, EPIC Exec. Dir), 114th Cong. (2015), https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf.

[4] EPIC and Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

[5] American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. Title I (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

[6] *Promoting Competition, Growth, and Privacy Protection in the Technology Sector: Hearing Before the Subcomm. on Fiscal Responsibility and Economic Grown of the Sen. Comm. on Finance* (testimony of Justin Sherman, Duke University) (Dec. 2021), https://www.finance.senate.gov/imo/media/doc/Written%20Testimony%20-%20Justin%20Sherman.pdf.

[7] Suzanne Smalley, *Brokers' sales of U.S. military personnel data overseas stir national security fears*, CyberScoop (Apr. 2022), https://cyberscoop.com/data-brokers-national-security-risk/.

[8] U.S. Dept. of Justice, "List Brokerage Firm Pleads Guilty To Facilitating Elder Fraud Schemes," Justice.gov, (Sept. 2020), https://www.justice.gov/opa/pr/list-brokerage-firm-pleads-guilty-facilitating-elder-fraud-schemes.

[9] Robert Gellman, *Protect consumer privacy: Repeal GLBA's privacy provisions*, IAPP Privacy Perspectives (Jul. 30, 2020), https://iapp.org/news/a/protect-consumer-privacy-repeal-the-glbas-privacy-provisions/.

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

December 11, 2023

TO: Judiciary Committee

FROM: Unum Group

RE: Entity v. Data-level Exemptions and the Employer/Employee Data Context

An entity-level exemption for financial institutions governed by the GLBA provides two distinct advantages over the data-level approach: (i) it prevents financial institutions from expending significant resources to ensure compliance with privacy laws that are only applicable to a de minimis portion of data collected by that entity; and (ii) it reduces consumer confusion/frustration.

The two benefits derive from the same fundamental issue: the vast majority of data collected/processed by a financial institution will be collected or processed "subject to" the GLBA. With a data-level exemption, we must construct two separate compliance programs, one under the GLBA that covers 99% of our data, and a second for a specific state privacy law, which only covers 1% of our data.

Why does a data-level exemption result in undue compliance obligations on GLBA regulated entities?

In short, compliance with the GLBA differs from compliance with state privacy obligations, so we must stand up two separate programs. Since there is a tiny portion of our data that might fall outside of a GLBA data-level exemption, we must institute a program to ensure compliance with the legal obligations associated with that data. However, the costs of instituting a compliance program are the same whether the data subject to those obligations is significant or miniscule. State-specific notices, disclosures, and processes must be stood up irrespective of the amount of data that would be governed by the state-specific laws. In for a penny, in for a pound. Regulated entities are therefore required to expend a tremendous amount of resources to ensure compliance with a law that will only be applicable to a fraction of their data, and have only a de minimis impact to consumers.

Why would an entity-level exemption reduce consumer confusion?

An entity-level exemption prevents consumers from mistakenly believing that the state privacy laws will apply to the data collected about them during an interaction with a financial institution. A member of the public is generally not going to be sufficiently familiar with what information is "subject to" the GLBA at the point of collection to understand what information will be subject to state privacy laws, and what will be regulated by the GLBA.

They reasonably assume that since the regulated entity provides state-specific notices and avenues to exercise state specific rights, these rights and obligations will cover all of the data collected by a regulated entity. When they are subsequently informed that their request cannot be acted upon because all information in our possession is collected/processed "subject to" the GLBA, they can be confused and upset. This has been our experience with the CCPA. We have not executed any individual rights request seeking deletion of information because of our obligations to retain GLBA-covered

information for a specified period of time. Consumers often ask (with good reason) why do we indicate these rights are available if we almost never act on them? That is a valid question, and exactly what an entity level-exemption would prevent.

If GLBA-covered entities are exempt wholesale, there will be no confusion from consumers as to the applicability of the GLBA or state privacy laws to their information. Only the GLBA will apply, and they will be able to exercise the rights provided under that law with regard to the information collected.

The Employee/Employer Data Context

Finally, as one of Maine's largest employers, we are already subject to numerous laws governing the collection and confidentiality of employment-related data. If the bill lacks an exemption for data collected in the employment context, we would be faced with competing obligations with respect to this information. All states that have adopted comprehensive privacy legislation have, in some form or other, carved out employment-related data from the scope of their bills.

There are two common elements of the employment-employee benefits exemption included in other states:

First, the definition of a "consumer" excludes "an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context."

Second, there is an explicit exception for: "data processed or maintained: (i) in the course of an individual applying to, employed by, or acting as an independent agent or contractor of a business to the extent that data is collected and used within the context of that role including for the administration and provision of employee benefits; (ii) as the emergency contact information of an individual; or (iii) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subdivision (i) and used for the purposes of administering such benefits."

This exemption recognizes that information collected in the employment context is already subject to rigorous regulation and any interference with those laws will not improve consumer's privacy.

Sincerely,

Umberto Speranza
AVP, Government Affairs
Unum Group

601 Pennsylvania Avenue, NW
South Building, Suite 500
Washington, D.C. 20004
T 202.778.3200
F 202.331.7487
ahip.org

December 11, 2023

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

RE: AHIP Comments on Consumer and Health Data Privacy Legislation (LD 1705, LD 1902, LD 1973, and LD 1977)

To Chairs Sen. Carney, Rep. Moonen and Members of the Joint Standing Committee on Judiciary,

America's Health Insurance Plans appreciates this opportunity to respectfully express our concerns with the following bills that seek to place duplicative and conflicting consumer data protections:

- 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

We share Maine's commitment and efforts to protect our consumers' personal identifiable information. For decades health insurance providers have done so under robust, strict, and effective legal and regulatory frameworks, notably through the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, which amended HIPAA, and the Gramm-Leach-Bliley Act (GLBA).

Through the exemptions provided by these bills, AHIP and its members are grateful for Maine's recognition of our commitment to these obligations. However, the exemption provisions vary widely among these bills, creating costly, inefficient data protection requirements. The current exemptions in the legislation are as follows:

- LD 1705 provides data-level (personal health information) exemptions that are governed under HIPAA and GLBA.
- LD 1902 provides data-level (protected health information, patient identifying information, and health care information) exemptions that are governed under HIPAA, HITECH, 42 Code of Federal Regulations, Part 2, established pursuant to 42 United States Code, Section 290dd-2, and Title 22, section 1711-C of the Maine Revised Statues.
- LD 1973 provides data-level exemptions for HIPAA covered information and for HIPAA-and GLBA-governed entities, among others.
- LD 1977 does not provide exemptions for health insurance providers or the maintenance of information under HIPAA, HITECH, or GLBA.

The varying exemptions provisions are duplicative, yet incomplete, creating a confusing patchwork of protection requirements for different types of information and entities. It is not just confusing for the affected entities, but for consumers as well. Furthermore, it would be incredibly costly to implement and maintain, adding to high health care costs. It is our understanding there is consideration of a larger, single omnibus legislation that would include provisions from each bill. Because of the varying

601 Pennsylvania Avenue, NW
South Building, Suite 500
Washington, D.C. 20004
T 202.778.3200
F 202.331.7487
ahip.org

exemptions in the current drafts, it is unclear to us how the final exemptions will take form. In whichever bill(s) that moves forward for consideration, we urge the Committee to ensure that the appropriate **entity-level exemptions** are included, as they are in LD 1973, in order to prevent cumbersome state-level requirements that conflict with or duplicative of those that the federal government requires of health plans.

We thus urge the Committee to include the following exemption provision in any and all legislation that is recommended for further action relating to consumer and health data privacy and security:

> "*A Licensee which is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and which maintains Nonpublic Information in the same manner as protected health information shall be deemed to comply with the requirements of this Act*."

AHIP would also support the healthcare exemptions in LD 1973 (under §9602(2)(F-O)) be used as a model, as they most closely and comprehensively align with other state privacy bills. In addition to our proposed exemption language, LD 1973 entity-level exemptions also alleviate our concerns addressed above. Either approach is acceptable to AHIP.

This language allows entities to avoid wasting time and money implementing and monitoring protection measures for different types of data under state and federal requirements – it does not avoid any obligations to protect such data. The proposed provision provides a data-level exemption as well as a coverall entity exemption. It is also self-executing in that if a company protects all its non-personal health information with the same federal requirements, then it is exempt. However, if it does not, then the company would be subject to state law.

AHIP is also concerned with the private right of action provisions in LD 1705 and LD 1902. HIPAA has its own enforcement mechanism under federal law (through the Office of Civil Rights) and actively pursues that enforcement to protect consumers' rights. See, for example, Eleven Enforcement Actions Uphold Patients' Rights Under HIPAA[1]; Oklahoma State University - Center for Health Services Pays $875,000 to Settle Hacking Breach[2]; OCR Settles Case Concerning Improper Disposal of Protected Health Information[3].

HIPAA, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, also has state enforcement by the states' attorneys general, under 42 US Code 1320d-5(d). Additionally, state Insurance Commissioners also enforce consumer privacy and data security in the states and have dealt promptly with breaches of HIPAA Covered Entities.

A new enforcement mechanism creating a private right of action only adds unnecessary costs and confusion to a long-standing, effective, and uniform national system of Privacy Protections, Data Security, and Consumer Notice which began in 2002 and 2003 and has been regularly fine-tuned and updated ever since, most recently with new rules for Interoperability and a pending Notice of Proposed Rulemaking on HIPAA "Part 2" dealing with sensitive substance use disorder information.

---

[1] (OCR), Office for Civil Rights. "Eleven Enforcement Actions Uphold Patients' RIGHTS UNDER HIPAA." HHS.gov, 15 July 2022, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/july-2022-hipaa-enforcement/index.html.

[2] (OCR), Office for Civil Rights. "Oklahoma State University – Center for Health Services Pays $875,000 to Settle Hacking Breach." HHS.gov, 14 July 2022, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/osu/index.html.

[3] (OCR), Office for Civil Rights. "OCR Settles Case Concerning Improper Disposal of Protected Health Information." HHS.gov, 23 Aug. 2022, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/nedlc/index.html.

601 Pennsylvania Avenue, NW
South Building, Suite 500
Washington, D.C. 20004

T 202.778.3200
F 202.331.7487
ahip.org

A private right of action in this scenario will only hinder the efficient enforcement of consumers' rights which are already well-protected in this arena, and much more so than in most other areas of industry. For these reasons, we urge the Committee not to advance legislation that includes any kind of enhanced enforcement mechanism through a private right of action.

AHIP and its members appreciate the opportunity to provide these comments. We stand ready for continued discussions with you on this important issue. If you have any questions or concerns regarding our comments and would like to discuss these matters further, please contact Sarah Lynn Geiger at slgeiger@ahip.org or by phone (609) 605-0748.

Sincerely,

Sarah Lynn Geiger, MPA
Regional Director, State Affairs

AHIP is the national association whose members provide health care coverage, services, and solutions to hundreds of millions of Americans every day. We are committed to market-based solutions and public-private partnerships that make health care better and coverage more affordable and accessible for everyone. Visit www.ahip.org to learn how working together, we are Guiding Greater Health.

Margaret O'Neil
21 Sheila Circle
Saco, ME 04072
Phone: (207) 590-1679
Margaret.O'Neil@legislature.maine.gov

HOUSE OF REPRESENTATIVES
2 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0002
(207) 287-1400
TTY: MAINE RELAY 711

December 11, 2023

Dear Members of the Judiciary Committee,

Thank you for the opportunity to update you on consumer privacy legislation. Given that we have two bills with many similar provisions, the following letter makes recommendations about how to combine our bills and focus on key issues. To help focus the committee's conversation, I have identified points where (a) the committee could use Connecticut's base text as a framework and (b) places where it is important to make a language tweak or language addition.

Although LD 1977 has a different structure than privacy laws that have been passed in other states such as Connecticut, Oregon, and Virginia, *many of the rights are the same*. If the Committee is more comfortable starting with the Connecticut Data Privacy Law or similar, there are ways to do that while adding in protections from LD 1977 that provide stronger privacy protections for Mainers.

Many of the provisions of CTDPA and LD 1977 overlap, such as:

- The right to access, correct, or delete your personal data
- The right to opt-out of targeted advertising
- The obligations for controllers to have transparent privacy policies
- The responsibilities of controllers to have contracts with the processors they work with
- Requirements for controllers to conduct data protection assessments

The ways LD 1977 provides higher protection that could be integrated into the Connecticut base text are:

1. **Data Minimization**

In previous hearings and work sessions, we have talked about the idea of data minimization.

Data minimization is a baseline protection. Before we reach a question of whether we will consent (or "opt-in") to data collection, a data minimization rule requires the company collecting our personal information to determine whether the information they plan to collect is "reasonably

necessary" for the product or service a consumer requests. For sensitive data such as a social security number, biometrics, or health information, the bar is higher; the company must determine the information is "strictly necessary."

A. Mainers deserve the same protections that other places have.

Maine won't be an outlier. These "reasonably necessary" and "strictly necessary" terms are already used in the EU's data protection rules called the "GDPR." That means major companies already comply with this standard in multiple countries.

California already has a data minimization rule in place that went into effect in March of this year. Thus, many companies that would be covered by Maine's law already have to comply with this in California, which is the fifth largest economy in the world. California's rules say that the purposes for which personal data is collected must be consistent with the reasonable expectations of the consumer, and they give guidance in their regulations to help businesses make these determinations. Mainers deserve these protections too.

B. Data minimization shifts the current burden on consumers to protect our information.

Data minimization is a critical component to Maine's privacy protections. Companies that use best practices follow this principle. A rule will help bring the other companies in line to protect consumers.

We've all seen how little pop-up cookie banners that are on every website we visit do to protect our personal information. See Attachment 1 for an example of what websites look like without a data minimization rule in place. A pop-up on a website asks for our consent before deploying cookies. Because we have to select "no" 10 times on each website to protect our personal information, we often forfeit privacy protection because of sheer annoyance or exhaustion. Attachment 1 provides an example of what websites look like without a data minimization rule in place.

We shouldn't pass a law that requires a similar set-up for data collection generally. This approach puts all the work on the consumer to fend off unwanted data collection.

Instead, companies should first evaluate whether the data they are collecting is consistent with consumer's expectations – that will reduce the number of times a consumer needs to click no ("opt-out") to protect their information, and it will provide a more meaningful privacy protection. To accomplish this, the Committee could import the data minimization language from either LD 1977 or California's rules into Connecticut's base text, and that would significantly improve the CT law.

2. Private Right of Action

The other critical piece from LD 1977 is a private right of action to ensure adequate enforcement. Adequate enforcement ensures our rights are actually protected.

When the Legislature passed the Maine Unfair Trade Practices Act in 1970, it included a private right of action to ensure that even if the AG's office didn't have the resources to bring an

enforcement action, Mainers would be protected from these harmful practices. Privacy violations are a form of unfair trade practices.

Unfortunately, the remedies in the private right of action under the Maine Unfair Trade Practices Act are insufficient for privacy cases as they are limited to actual damages, which courts often have a difficult time determining in privacy cases as it can be difficult to assign a specific economic value to the harm caused by a privacy violation. Because courts have struggled with this issue, the legislature must make a clear law to ensure consumer rights are actually protected.

We can focus a private right of action to ensure businesses that collect so much personal information that the harms can be much more consequential are motivated to comply with the law. I'd be happy to work with the Committee on a compromise there.

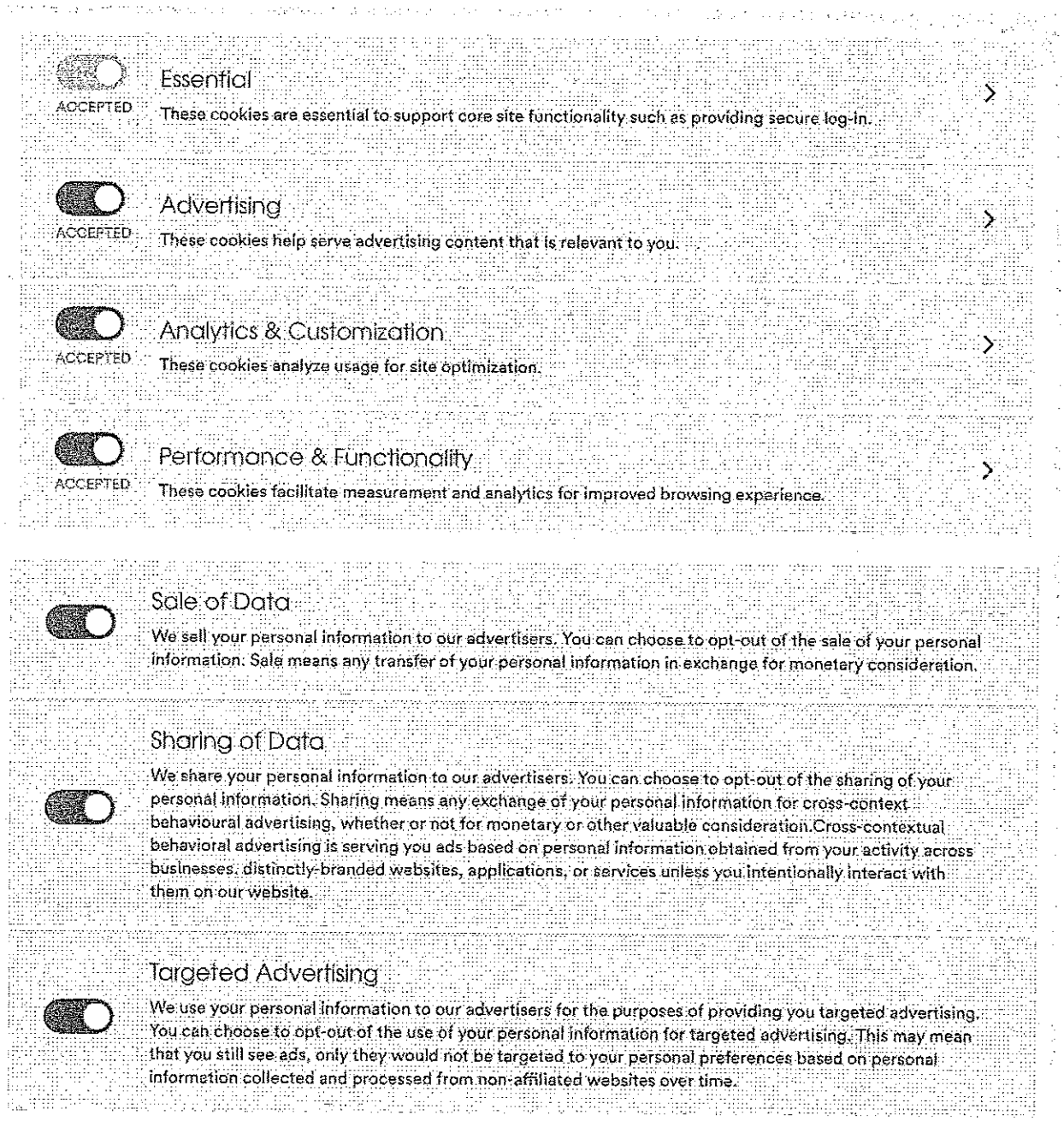
There are other smaller differences between the protections in the two bills, but those are the two overarching protections that, if imported into Connecticut's base text, would provide strong privacy protections for Mainers. To help focus the committee's conversation, I have identified points where we can use Connecticut's base text and places where it is important to make a language tweak or language addition.

Thank you for your time,

Rep. Maggie O'Neil
H.D. 129, Saco

Attachment 1

Here's an example of what websites look like without a data minimization rule in place:



Attachment 2

LD 1973 provisions to adopt

- § 9602(1) Scope - Applicability
- § 9603 Consumer rights:
  - (1) right to access/correct/delete/port
  - (3) Exercise of consumer rights
  - (4) responding to exercise of consumer rights
  - (5) appeals
- § 9604 Authorized agent
- § 9605(4) Transparency
- § 9606 Responsibilities of processors and controllers -- *would suggest adding additional protection in LD 1977 that prohibits processors from comingling data they get from different entities.*
- § 9607 Data Protection Assessments -- *would suggest adding requirement from LD 1977 to require entities to make a summary of the assessment public.*

LD1977 provisions to adopt

- Definition of covered data/personal data (to include inferences), definition of biometric information
- §9604 - §9605 Data minimization requirements (can alter structure) and sensitive data protections
- §9607 Prohibition on retaliation against an individual for exercise of rights and unlawful pricing (to include limitation on data collection/use for loyalty programs to what is functionally necessary to operate the loyalty program.)
- §9609 Affirmative consent requirements (could alternatively be brought into definition)
- §9610 Targeted advertising (includes prohibition on targeted advertising to minors)
- §9614 Civil rights protections
- §9616 Data security (similar, but more detailed, to data security language in LD1973 §9605(1)(B))
- §9620 Enforcement

For discussion

- Definition of sensitive data
- Exceptions for entities/data types already covered by federal law
- Opt-in or opt-out for targeted advertising, profiling, sale of personal data?
- Algorithmic impact assessments requirements
- Require appointment of Privacy officers/Data security officers?
- Data broker registry