Joint Standing Committee on Judiciary

MEETING AGENDA
Wednesday, November 8, 2023
Maine State House, Room 438 (JUD Committee Room)
The meeting will be livestreamed at the following link: https://legislature.maine.gov/Audio/#438

10:00 a.m. **Work Session**

LD 1056, An Act Restricting State Assistance in Federal Collection of Personal Electronic Data and Metadata (Sen. Brakey)

LD 1576, An Act to Update the Laws Governing Electronic Device Information as Evidence (Rep. O'Neil)

- **Responses to requests for information**
- **Updates from bill sponsors**
- **Committee discussion**

1:00 p.m. **Work Session**

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

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

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

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

- **Information from legislative analyst**
- **Overview of confidentiality provisions in the federal Gramm-Leach-Bliley Act** (Bureau of Financial Institutions)
- **Overview of confidentiality provisions in the federal Fair Credit Reporting Act** (Bureau of Consumer Credit Protection)
- **Overview of confidentiality provisions in the federal Health Insurance Portability and Accountability Act and the state Insurance Information and Privacy Protection Act** (Bureau of Insurance)
- **Impact of the proposals in LD 1977 on the media** (MainePublic & Maine Association of Broadcasters)
- **Updates from bill sponsors**
- **Committee discussion**

Followed by: **Discussion of Next Steps**

- Additional Work Sessions on privacy bills?
  - Wednesday, November 29th at 10:00 a.m.
  - Monday, December 11th at 10:00 a.m.
- Meeting to provide background information on Indian law in Maine
  - Tuesday December 12th at 10:00 a.m.

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

MEMORANDUM

TO: Joint Standing Committee on Judiciary

FROM: Janet Stocco, Legislative Analyst

DATE: November 8, 2023

RE: **Information requested for work session on November 8, 2023**

LD 1056, An Act Restricting State Assistance in Federal Collection of Personal Electronic Data and Metadata (Sen. Brakey)

LD 1576, An Act to Update the Laws Governing Electronic Device Information as Evidence (Rep. O'Neil)

The committee requested the following information from the following stakeholders during the September 25, 2023 work sessions on LD 1056 and LD 1576.

1. **To bill sponsors:**
   a. Please provide an update on negotiations with the Office of the Attorney General and other stakeholders regarding the language of your bills.

2. **To Office of the Attorney General and Maine Prosecutors' Association**:
   a. Currently, federal and state law allow law enforcement to seek limited subscriber information (including the subscriber's name, address, IP address, session times and duration and payment information including any credit card or bank account) using a grand jury subpoena. Do you have any data on how often evidence is gathered through a grand jury subpoena without a criminal indictment or prosecution resulting from the investigation?

   b. If a grand jury investigation does not result in an indictment or prosecution when, if ever, are the records of the investigation, including evidence gathered with a grand jury subpoena, purged?

   c. Does an individual's Fourth Amendment protection against unreasonable, warrantless searches survive the individual's death?

   d. Does Senator Brakey's proposal to replace the language of LD 1056 with the language of the majority amendment to LD 531 in the 127th Legislature—which would in proposed subsection 1(D) allow state and local law enforcement to share with federal agencies any electronic data or metadata that they lawfully possess—assuage your concerns with LD 1056?

3. **To Maine State Archivist**:
   a. Under current records retention schedules, how long must records of evidence gathered through a grand jury subpoena be retained; when may or must such records be destroyed? Is there a difference in records retention guidance for evidence collected through a grand jury subpoena that leads to a criminal indictment or prosecution as opposed to evidence that does not?

4. **To ACLU of Maine**:
    a. Under the California Electronic Communications Privacy Act, the definition of "subscriber information" that law enforcement may obtain from a service provider excludes IP addresses; thus, IP addresses may be obtained by law enforcement only through a search warrant. Please provide, as offered, a copy of a search warrant application for a law enforcement agency to access an IP address under the California Electronic Communications Privacy Act.

        See email response from Megan Sway (Attachment A).

5. **To Electronic Privacy Information Center**:
    a. Are you aware of any mass data surveillance activities being conducted currently or in the recent past by the federal government?

        See email response from EPIC Counsel Thomas McBrien and links therein (Attachment B).

Attachment B

From: mcbrien@epic.org <mcbrien@epic.org>
Sent: Monday, October 2, 2023 10:44 AM
To: Stocco, Janet <Janet.Stocco@legislature.maine.gov>
Cc: fitzgerald@epic.org
Subject: RE: follow-up information on LD 1056 (Maine)

Dear Janet,

Thank you so much for having me. I have a few resources to share that my colleague Chris Baumohl has prepared and that should be responsive to Senator Brakey's question.

First, here is a piece (https://epic.org/it-will-take-more-than-reforming-section-702-to-rein-in-warrantless-government-surveillance/) we have published that discusses the need to reform Section 702, a federal statute that law enforcement and intelligence agencies rely on to engage in a lot of surveillance activities. The piece also details other instances of mass surveillance (though the government would dispute that term) and the laws that allow them.

Here is a record (https://epic.org/documents/epic-v-dea-hemisphere/) of a FOIA dispute that EPIC was involved in relating to a surveillance tool called Hemisphere, and a news story (https://techcrunch.com/2019/03/28/hemisphere-phone-records/) just a few years ago confirming that federal agencies continue to use the product.

Finally, here is a webpage about an amicus brief (https://epic.org/documents/sequeira-v-department-of-homeland-security-et-al/) we recently wrote in a case involving mass surveillance of immigrant communities in the southwest.

Please let me know if you or the Senator have any follow-up questions.

Best,
Tom

-----Original Message-----
From: "Stocco, Janet" <Janet.Stocco@legislature.maine.gov>
Sent: Thursday, September 28, 2023 12:43
To: "mcbrien@epic.org" <mcbrien@epic.org>
Cc: "fitzgerald@epic.org" <fitzgerald@epic.org>
Subject: follow-up information on LD 1056 (Maine)

Dear Attorney McBrien,

On behalf of the Maine Legislature's Judiciary Committee, I want to thank you for the information you provided to the committee this past Monday.

I am also writing to remind you of Senator Brakey's request for further information about any mass data surveillance activities currently (or in the recent past) being conducted by the federal government about which EPIC is aware. You very kindly offered to reach out to one of your colleagues who may have information on this topic. The Judiciary Committee hopes to continue its discussions of LD 1056 and LD 1576 on Wednesday, November 8th, and would be delighted to review the information your colleague gathers before or during that meeting if possible.

Sincerely, Janet

Stocco, Janet

From: Hayes, Danna <Danna.Hayes@maine.gov>
Sent: Tuesday, November 7, 2023 4:14 PM
To: Stocco, Janet
Cc: Shira Burns; Marchese, Lisa J; aeberggren@yorkcountymaine.gov; Risler, John; Boyle, Charles M; Rucha, Paul
Subject: RE: Follow-up questions on LD 1056 and LD 1576

Hi Janet,

Here are the responses to the questions, as requested- I believe the negotiations cover the MPA as well, but Shira can correct me if she has any different answers to the data pieces.

1. **Please provide an update on your work with / negotiations with the sponsors of LD 1056 and LD 1576, if any.**
    a. We all met with Rep. O'Neil in early October and have emailed with her intermittently since then. Unfortunately the situation in Lewiston required us to cancel a follow-up meeting we had previously scheduled. We have proposed some alternative language that we are still negotiating.
    b. Our Offices discussed the concerns we had with 1056 and came up with some proposed alternative language (see below). Both Shira and Danna have been in contact with Senator Brakey to share those alternatives.
2. **Please provide any data you have on how often evidence (either evidence generally or electronic evidence specifically) is gathered through a grand jury subpoena without a criminal indictment or prosecution resulting from the investigation.**
    a. There exists no centralized, statewide repository for data concerning the issuance of grand jury subpoenas, nor concerning the ultimate disposition of the related investigation. Assembly of such data would require significant resources. Anecdotally, the share of cases involving such materials that result in charges vary widely by type of case. Among homicide cases, nearly all cases identified as homicides by the OCME involve grand jury subpoenas, and nearly all of those result in charges (unless unsolved). Among financial crimes investigations, election crime investigations, or public corruption investigations, a larger proportion of investigations employing grand jury subpoenas result in no criminal charges; In many of these cases, subpoenaed materials enable prosecutors to determine that no crime was committed by the target, without creating publicly-available warrant requests and affidavits unnecessarily.
3. **If a grand jury investigation does not result in an indictment or prosecution, when (if ever) are the records of that investigation, including evidence gathered with a grand jury subpoena, purged? If the records are not purged, why not?**
    a. Materials obtained by the Office of the Maine Attorney General via grand jury subpoena are maintained, archived, and destroyed in accordance with the applicable records retentions schedules promulgated by the Department of the Secretary of State. Each investigative or prosecutorial agency that may be in possession of similar records would be bound by its own applicable retention policies. These same parameters would apply to all types of investigative material, however obtained.
4. **Does an individual's Fourth Amendment protection against unreasonable, warrantless searches survive the individual's death?**

a. No, a deceased person is unable to assert a violation of a reasonable expectation of privacy that would be protected by the Fourth Amendment. "Fourth Amendment rights are personal rights which . . . may not be vicariously asserted." *Rakas v. Illinois*, 439 U.S. 128, 133-34.

5. **Does Senator Brakey's Proposal to replace the language of LD 1056 with the language of the majority committee amendment to LD 531 in the 127th Legislature (see http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=SP0200&item=2&snum=127) assuage each of your office's/organization's concerns with LD 1056?**

   a. OAG's concerns with LD 1056 are also appliable to LD 531's committee amendment language: Both would unnecessarily impede the free-flow of information between State and Federal agencies that is necessary to successfully fulfill law enforcement responsibilities on a day-to-day basis in the State of Maine.

   b. We proposed this language as an alternative:
   "State law enforcement agencies may not knowingly share with federal law enforcement agencies content, location information, or subscriber information obtained from an ECS or RCS in violation of Maine law or the United States or Maine Constitutions." This language both includes statutory definitions from within Maine's existing framework and ensures that the State would have known the information was illegally obtained.

See you tomorrow! Call my cell if you have any questions before then.
Danna

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

From: Stocco, Janet <Janet.Stocco@legislature.maine.gov>
Sent: Monday, November 6, 2023 10:58 AM
To: Marchese, Lisa J <Lisa.J.Marchese@maine.gov>; Risler, John <John.Risler@maine.gov>; Rucha, Paul <Paul.Rucha@maine.gov>; Boyle, Charles M <Charles.M.Boyle@maine.gov>; aeberggren@yorkcountymaine.gov
Cc: Hayes, Danna <Danna.Hayes@maine.gov>; Shira Burns <shira.burns@maineprosecutors.com>
Subject: RE: Follow-up questions on LD 1056 and LD 1576

Hello!

I am just writing to remind you of the information requests (see below) from the Judiciary Committee for its work session on LD 1056 and LD 1576 this Wednesday.

Sincerely, Janet

--

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

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

MEMORANDUM

TO: Joint Standing Committee on Judiciary

FROM: Janet Stocco, Legislative Analyst

DATE: November 8, 2023

RE: **Information requested for today's work session on:**

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

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

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

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

This memorandum provides follow-up information requested by the committee during the October 17, 2023 public hearing on LD 1977 and work sessions on LD 1705, LD 1902, LD 1973 and LD 1977.

A. Specifically requested exemptions to state consumer privacy bills

During the work session on LD 1705, LD 1902, LD 1973 and LD 1977, various stakeholders requested that entities or information subject to certain federal privacy laws be exempt from state consumer data privacy legislation. Other stakeholders objected to these exceptions. The exceptions specifically requested include:

- *Entities subject to the federal Health Insurance Portability and Accountability Act (HIPAA)*
  (Request from ATA Action; Maine Hospital Association, Maine Medical Association, Maine Osteopathic Association, Maine Health Care Association, Maine Ambulance Association, Maine Society of Anesthesiologists, Spectrum Healthcare Partners, State Farm, MaineHealth and Wex, Inc.)
- *Information protected under the federal Health Insurance Portability and Accountability Act (HIPAA)*
  (Request from Planned Parenthood NNE. The Office of the Attorney General also suggested considering the extent to which information collected by health care providers should be exempted.)
- *Financial Institutions subject to the federal Gramm-Leach-Bliley Act (GLBA)*
  (Request from American Council of Life Insurers, Fidelity Investments, Maine Bankers Association, Maine Credit Union League, Receivables Management Association International, State Farm and Wex, Inc.)
- *Information subject to the federal Gramm-Leach-Bliley Act (GLBA)*
  (The Maine Credit Union League prefers an entity-level exemption, but proposed this as a backup.)
- *Information shared with credit reporting agencies Fair Credit Reporting Act (FCRA)*
  (Request from Maine Credit Union League.)
- *Entities regulated by the state Insurance Information and Privacy Protection Act in Title 24-A, chapter 24*
  (Request from Maine Bureau of Insurance and National Insurance Crime Bureau for LD 1902 and from Maine Association of Health Plans for both LD 1902 and LD 1977.)

B. Information about scope of current federal privacy laws (and state insurance law)

Committee members requested further information on the scope of current federal data privacy laws, especially HIPAA, GLBA and FCRA, the federal laws for which the committee has been asked to include either entity-level or information-level exemptions to its consumer data privacy legislation. The Bureau of Financial Institutions, Bureau of Consumer Credit Protection and Bureau of Insurance, all within the Maine Department of Professional and Financial Regulation, have been invited to today's meeting to provide the following information on these federal laws as well as the state Insurance Information and Privacy Protection Act in Title 24-A, chapter 24:

- What entities are regulated by each law?
- What types of consumer data are regulated by each law?
- How is that data protected (for example, prohibitions or requirements for collecting, using, sharing or selling that data)?

In addition, the following Congressional Research Service Report provides an overview of the data privacy provisions in several federal laws including: the GLBA, HIPAA, FCRA, the Communications Act of 1934, the federal Video Privacy Protection Act, the Family Educational Rights and Privacy Act of 1974, section 13(b)(2)(B) of the Securities and Exchange Act of 1934, the Children's Online Privacy Protection Act, the Electronic Communications Privacy Act (including the Wiretap Act, the Stored Communications Act and the Pen Register Act), the Computer Fraud and Abuse Act, the Federal Trade Commission Act and the Consumer Financial Protection Act. [Note: The description of California's Consumer Privacy Act (CCPA) within this report does not reflect amendments adopted by California voters in November 2020 that took effect Jan. 1, 2023.]

- Stephen P. Mulligan & Chris D. Linebaugh, *Data Protection Law: An Overview*, Congress. Res. Serv. Report #R45631(March 25, 2019), available at https://crsreports.congress.gov/product/pdf/R/R45631.

C. Methods of crafting exceptions based on existing federal and state privacy laws

At the work session, Representative Lee asked whether it is possible to craft exemptions for entities regulated by current federal or state privacy laws but only to the extent that existing laws actually regulate those entities. The examples below illustrate some of the committee's options when crafting exemptions based on existing laws.

❖ Example language exempting an entity regulated by a federal law—see LD 1973, §9602(2)(E) & (F) on p. 4:

> **2. Nonapplicability.** The provisions of this chapter do not apply to:
>
> . . .
>
> E. A financial institution . . . that is subject to the federal Gramm-Leach-Bliley Act, 15 United States Code, Section 6801 et seq. (1999);
>
> F. A covered entity or business associate [Note: the bill defines these terms using their HIPAA definitions];

❖ Example language exempting data protected by a federal law—see LD 1973, §9602(H) & (R) on pp. 4-5:

> **2. Nonapplicability.** The provisions of this chapter do not apply to:
>
> . . .
>
> H. Patient-identifying information as described in 42 United States Code, Section 34290dd-2 [Note: this law protects records of "identity, diagnosis, prognosis, or treatment of any patient maintained in connection with . . . substance use disorder education, prevention, training, treatment, rehabilitation or research…."];
>
> . . .
>
> R. Personal data regulated by the federal Family Educational Rights and Privacy Act of 1974, 20 United States Code, Section 1232g et seq.;

❖ Example language exempting an entity regulated by a federal law but only to the extent that the entity is complying with that federal law's data protection provisions—see LD 1973, §9602(P) on page 5:

> **2. Nonapplicability.** The provisions of this chapter do not apply to:
>
> . . .
>
> P. The collection, maintenance, disclosure, sale, communication or use of personal information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act, 15 [U.S.C.], Section 1681 et seq.;

Additional examples of limited exemptions appear in LD 1902, § 1350-X(1)-(3) on page 10:

> This chapter does not apply to:
>
> **1. Protected health information.** Protected health information, or information treated like protected health information, collected, used or disclosed by covered entities and business associates when:
>
> A. The protected health information is collected, used or disclosed in accordance with the federal Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act and 45 Code of Federal Regulations, Parts 160 and 164 and implementing regulations; and
>
> B. The protected health information is afforded all the privacy protections and security safeguards of the federal laws and implementing regulations under paragraph A. For the purpose of this subsection, "protected health information," "covered entity" and "business associate" have the same meaning as in the federal Health Insurance Portability and Accountability Act of 1996 and its implementing regulations;
>
> **2. Patient identifying information.** Patient identifying information collected, used or disclosed in accordance with 42 Code of Federal Regulations, Part 2, established pursuant to 42 [U.S.C.], Section 290dd-2; or
>
> **3. Health care information.** Health care information collected, used or disclosed in accordance with Title 22, section 1711-C.

D. Information about other states' consumer privacy laws

❖ Connecticut law: Senator Bailey asked me to prepare a chart comparing LD 1973, LD 1977 and the Connecticut Data Privacy Act (CTDPA), which many industry stakeholders advanced as the best state model for general consumer privacy legislation. The requested comparison chart is attached.

❖ Other states: the following resource may provide a helpful overview of some other state's data privacy laws:

- Theodore P. Augustinos & Alexander R. Cox, *U.S. State Privacy Laws in 2023: California, Colorado, Connecticut, Utah & Virginia*, Privacy & Cybersecurity Newsletter (December 2022), https://www.lockelord.com/newsandevents/publications/2022/12/us-state-privacy-laws-2023.
  See also their chart comparing aspects of the California, Connecticut, Colorado, Utah and Virginia laws at https://www.lockelord.com/-/media/files/newsandevents/publications/2022/12/us-state-privacy-laws-2023.pdf?rev=20b1a066f2054c239305719f0d04947f&hash=D13B9DA670F0476799495034561A7682.

❖ Private right of action: During the October 17, 2023 work session, stakeholders informed the committee that no other state's comprehensive data privacy legislation contains a private right of action. While the Illinois Biometric Privacy Act is enforceable through a private right of action (for $1,000 per negligent violation, $5,000 per intentional or reckless violation or actual damages, whichever is greater, plus attorney's fees and injunctive relief), that law only regulates biometric data. In addition, while the Washington My Health My Data Act is enforceable through a private right of action (for actual damages, potentially treble punitive damages, attorney's fees and injunctive relief), that law only regulates consumer health data.

Moreover, although the comprehensive consumer data protection law adopted in California—the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act (CPRA)—contains a private right of action, most violations of that law are enforceable only through actions brought by the California Privacy Protection Agency. The agency may recover administrative fines of up to $2,500 for each violation or up to $7,500 for each either intentional violation or violation involving a consumer under 16 years of age. See Cal. Civ. Code §1798.155. The private right of action only applies when:

> Any consumer whose nonencrypted and nonredacted personal information…, or whose email address in combination with a password or security question and answer that would permit access to the account is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information ….

A consumer may recover statutory damages of between $100 to $750 per consumer per incident or actual damages, whichever is greater, as well as injunctive and declaratory relief. If a consumer seeks statutory damages (as opposed to actual damages), the consumer must first provide notice to the business of the specific sections of law alleged to be violated. No action may be brought if the business responds in writing within 30 days indicating that it has cured the alleged violations and that no further violations will occur (unless the consumer can prove a subsequent breach of this statement). In addition, in assessing statutory damages (as opposed to actual damages) courts are directed to consider "the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth." *See* Cal. Civ. Code §1798.150.

E. Information about state statutes enforceable under the Maine Unfair Trade Practices Act

In Chapter 3 of its *Consumer Law Guide*, the Office of the Maine Attorney General notes that the following state statutes contain language expressly providing that a violation of their provisions either constitutes a violation of the Maine Unfair Trade Practices Act (UTPA) or is *prima facie* (presumptive) evidence of a violation of UPTA.

A. Automated Telephone Solicitations [10 M.R.S. § 1498(8)]
B. Cable Television Service [30-A M.R.S. § 3010(7)]
C. Charitable Solicitations Act [9 M.R.S. § 5014]
D. Manufactured Housing Warranties [10 M.R.S. § 1406]
E. Leases (Landlord-Tenant) [14 M.R.S. § 6030]
F. Leases (Consumer Transactions) [11 M.R.S. § 2-1104]
G. Used Car Information [10 M.R.S. § 1477]
H. Insulation Contracts [10 M.R.S. § 1483]
I. Home Construction Contracts [10 M.R.S. § 1490(1)]
J. Solar Energy Equipment Warranties [10 M.R.S. § 1494]
K. Implied Warranties for Consumer Goods [11 M.R.S. § 2-316(5)(a)]
L. Pyramid Clubs [17 M.R.S. § 2305]
M. Odometers [29-A M.R.S. § 752]
N. Law Enforcement Solicitations [25 M.R.S. § 3702-C]
O. Unsolicited Telefacsimile Transmissions [10 M.R.S. § 1496(4)]
P. Motor Vehicle Dealers [29-A M.R.S. § 1754(3)]
Q. Motor Vehicle Repairs [29-A M.R.S. § 1807]
R. Mobile Home Parks [10 M.R.S. § 9100]
S. Pawnshop Transactions [30-A M.R.S. § 3963(6)]
T. Hearing Aid Dealers and Fitters [32 M.R.S. § 17305]
U. Consumer Solicitation Sales [32 M.R.S. § 4670]

V. Door-to-Door Home Repair Transient Sellers [32 M.R.S. § 14512]
W. Transient Sellers of Consumer Merchandise [32 M.R.S. § 14713]
X. Business Opportunities Sales[32 M.R.S. § 4700(1)]
Y. Membership Camping [33 M.R.S. § 589-C(1)]
Z. Time Shares [33 M.R.S. § 592(6)]
AA. New Car Lemon Law [10 M.R.S. § 1169(10)]
BB. Charges After Free Trial Period [10 M.R.S. § 1210-A]
CC. Immigration and Nationality Law Assistance Act [4 M.R.S. § 807-B]
DD. Maine Self-service Storage Act [10 M.R.S. § 1377]

See https://www.maine.gov/tools/whatsnew/attach.php?id=27921&an=1.

F. Requests for Information from Oct. 17, 2023 Committee Meeting

- *To Representative O'Neil*: Explain why LD 1977 §9604 enumerates a list of allowed purposes for collecting, processing and transferring covered data. Is there a danger the Legislature might forget to list an important purpose for collecting, processing or transferring data in this legislation?
- *To Computer & Communications Industry Association* (CCIA): How could a consumer's request for information about the covered data collected by an entity, for example under the proposal in LD 1973, require a business to reveal a trade secret?
- *To L.L. Bean*: Please provide any analysis of the Connecticut law (which L.L. Bean prefers) or any other states' consumer data privacy laws. (Not a request to create a resource, but share resources it already has.)
- *To Maine Attorney General*: How often are the complaints received by the Office regarding alleged violations of the Maine Unfair Trade Practices Act frivolous? [*Answer: This data is not tracked.*]
- *To Maine Automobile Dealers Association*: Please provide an example of a Maine law that included a private right of action that led the courts to be overwhelmed with litigation.
- *To Maine State Chamber of Commerce*:
  - Why does the chamber prefer the Connecticut/Colorado/Virginia model of consumer privacy legislation (beyond lack of a private right of action)?
  - Would any members of the Maine State Chamber of Commerce be regulated by LD 1977 (or are they all exempt under §9603(2) of the bill)?
- *To Maine Automobile Dealers Association (MADA)*: Are any of your members large enough that they would not be exempt from LD 1977 under §9603(2) of the bill?
- *To Retail Association of Maine*: [*Answers: see attached email.*]
  - Please provide data and sources for that data regarding the number of lawsuits filed against small businesses under the Illinois Biometric Information Privacy Act.
  - Please provide additional information about how the Washington My Health My Data law has unintended consequences regarding sales of products like toothpaste, aspirin and rash cream.

G. Background information about how consumer data is collected online

The following report from the Congressional Research Service contains a helpful overview of the methods used to collect information about and track consumers online. It also briefly summarizes enforcement actions taken by the Federal Trade Commission under its authority to punish "unfair or deceptive acts or practices."

- Clare Y. Cho & Kristen E. Busch, *Online Consumer Data Collection and Data Privacy*, Congress. Res. Serv. Report #R47298 (Oct. 31, 2022), available at https://crsreports.congress.gov/product/pdf/R/R47298.

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
Protected Data	❖ "**Personal data**": • Data linked or reasonably linkable to an identifiable individual (a "consumer") who is a Maine resident Excludes: "Publicly available information" (defined term [i]) and "de-identified data" (see duties listed in chart below) ❖ "**Sensitive data**": subset of personal data including: • Data revealing race, ethnicity, religion, mental or physical health, sexual orientation, citizenship or immigration status • Processing of biometric or genetic data to uniquely ID a person • Precise geolocation data (within 1,750 feet) • Personal data of a child <13 years of age **Exception (both types of data above):** • "Consumer" is defined for purposes of the bill to exclude an employee, contractor, etc. interacting with a controller solely in an employment context	❖ "**Personal data**": • Data linked or reasonably linkable to an identifiable individual (a "consumer") who is a CT resident Excludes: "Publicly available information" (defined as in LD 1973 [i]) and de-identified data (same duties as in LD 1973) ❖ "**Sensitive data**": subset of personal data including: • Data revealing race or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, citizenship or immigration status • Processing of genetic or biometric data for purposes of uniquely identifying an individual • Precise geolocation data (within 1,750 feet) • Personal data of a known child < 13 years of age • Consumer health data or CHD (see below) • Data about person's status as a victim of a crime ❖ "**Consumer health data**" (CHD): subset of sensitive data used to identify a consumer's physical or mental health condition or diagnosis, including but not limited to: • Gender-affirming health data; and • Reproductive or sexual health data (includes data on conditions, abortions, medications, symptoms etc.) **Exception (all 3 types of data above):** • "Consumer" is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context	❖ "**Covered data**": • Information linked or reasonably linkable, alone or in combination with other info., to identifiable individual or to a device that is reasonably linkable to an individual Excludes: "publicly available information" (not defined) and de-identified data (no specific duties apply to this data) ❖ "**Sensitive data":** subset of covered data including: • Data revealing race, ethnicity, religion, mental/physical health, disability, diagnosis, sexual behavior, employment history, union membership or family or social relationships • Biometric and genetic information • Location information (within 1,850 feet) • Information of person known to be a minor <18 y.o. • Social security, passport or driver's license number • Account or device log-in credentials or access codes • Private communications (email, text, DM, voicemail, mail) and information about their transmission • Calendar and address book information, phone or text logs, photos, audio recordings, and videos if those are for private use, whether on the individual's device or remotely stored • Photo or video images of naked or undergarment-clad genitals • Information about video content requested by an individual and an individual's online activities over time
Size and Maine connection requirements for regulation	❖ **Law only applies to** persons that: • Conduct business in Maine or target Maine residents • In last calendar year, controlled or processed personal data of: o ≥100,000 Maine residents (except solely for purposes of payment transactions) **or** o ≥25,000 Maine residents and derived > 25% of gross revenue from the sale of personal data	❖ **CTDPA – *non-CHD provisions* –** same requirements as in LD 1973 (except focus is on CT businesses and residents) ❖ **CTDPA – *CHD provisions* – only apply to** persons: • Conducting business in CT or targeting CT residents • (No requirement about number of residents affected)	❖ **Law only applies to** persons that for any of the prior 3 years: • Collect or process data of >75,000 individuals per year (other than solely for purpose of billing for requested product/service) • Have average annual gross revenue >$20,000,000 **or** • Receive any revenue for transferring covered data *Note: no Maine connection required*

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
Types of covered entities	❖ **Controller:** person that determines purpose and means of processing personal data ❖ **Processor:** person that processes (collects, uses, stores, discloses, analyzes or deletes) personal data for a controller	❖ **Controller:** person that, alone or jointly with others, determines purpose and means of processing personal data ❖ **Processor:** person that processes (collects, uses, stores, discloses, analyzes or deletes) personal data for a controller	❖ **Covered entity**: alone or jointly determines purposes and means of collecting, processing or transferring covered data ❖ **Service provider**: collects, processes or transfers covered data for a covered entity or federal, state, tribal or local government
Exceptions to applicability Note: *for LD 1973, see lists on pp. 4-6 and 12-14*	❖ **Law <u>not</u> applicable to (types of entities / types of data)**: • State or its political subdivisions or boards or agencies, • Certain tax-exempt organizations • Higher education institutions and data regulated by the federal Family Educational Rights and Privacy Act • Financial institutions or data subject to federal Gramm-Leach-Bliley Act • National securities associations registered under the federal Securities Exchange Act of 1934 (ex: FINRA) • Covered entities or business associates under HIPAA • HIPAA "protected health information" & intermingled information held by HIPAA-regulated entities • Info. de-identified in accordance with HIPAA • Info. for public health activities as authorized by HIPAA • Patient-identifying info. related to substance-use disorder treatment (under 42 USC §290dd-2) • Identifiable information collected as part of human subject research conducted under certain federal laws or international guidelines • Info. created, collected, processed, sold or disclosed in compliance with the following federal laws: o Health Care Quality Improvement Act of 1986 o Fair Credit Reporting Act o Driver's Privacy Protection Act of 1994 o Farm Credit Act of 1971 o Airline Deregulation Act of 1978 • Information of those applying to or employed by a controller, processor or third party or to administer benefits to employees and relatives	❖ **CTDPA – *non-CHD provisions* – are <u>not</u> applicable to (types of entities / types of data)**: • State or its political subdivisions or boards or agencies, (including contractors that process CHD for them) • Certain tax-exempt organizations (same as LD 1973) • Higher education institutions • Financial institutions or data subject to federal Gramm-Leach-Bliley Act • National securities associations registered under the federal Securities Exchange Act of 1934 (ex: FINRA) • Covered entities/business associates under HIPAA • Tribal nation government or organization • Air carrier regulated under Federal Aviation Act of 1958 and federal Airline Deregulation Act of 1978 • Any obligation otherwise required by CTDPA that would violate an evidentiary privilege under state law • Any obligation otherwise required by CTDPA that would violate freedom of speech or press ❖ **CTDPA – *all provisions, including CHD provisions* –** are also **<u>not</u> applicable to (types of entities / types of data)**: • Protected health information regulated by HIPAA and intermingled info. held by HIPAA-regulated entities • Info. de-identified in accordance with HIPAA • Info. for public health activities authorized by HIPAA or for community health or population health activities • Patient-identifying info. related to substance-use disorder treatment (under 42 USC §290dd-2) • Identifiable information collected as part of human subject research conducted under certain federal laws or international guidelines	❖ **Law <u>not</u> applicable to:** • Government entities • Service providers that exclusively and solely process information provided by government entities (except as specified below) Note: LD 1977 does not include a comprehensive list of activities unaffected by the requirements/prohibitions in the bill. **Instead, it generally limits collection, processing and transferring of covered data to specific allowed purposes** listed on pp. 6-7: • Complying with obligations under local, state, tribal or federal laws & defending legal claims • Completing transaction for a requested product or service • Fulfilling a product or service warranty • Preventing harm if have a good faith believe individual at risk of death, serious physical injury or other serious health risk • Preventing or responding to security incident (network security or physical security, including trespass, medical alert, fire alarm) • Preventing or responding to fraud, harassment or illegal activity targeted at or involving the controller or service provider

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
	• Disclosures that violate an evidentiary privilege under state law • Disclosures that violate freedom of speech or press ❖ **Controller / Processor activities <u>not</u> affected by LD 1973**: • Complying with federal, state or local laws, investigations, subpoenas or summonses • Investigating, exercising or defending legal claims • Providing product or service requested by consumer, including performing contracted services (ex: warranty) • Taking immediate steps to protect an interest essential for the life or physical safety of a consumer or other individual • Preventing or responding to security incidents, identity theft, fraud, harassment or illegal activity or report those incidents • Engaging in scientific or statistical research that adheres to all other ethics and privacy laws and is overseen by an IRB • Assisting another controller or processer with its compliance • Process personal data for public health purposes subject to confidentiality obligations of federal or state laws • Collection, use or retention of data for internal use, including R&D, product recalls, identifying and repairing technical errors • Processing of personal data by person for own household use	• Info. created, collected, processed, sold or disclosed in compliance with the following federal laws: o Health Care Quality Improvement Act of 1986 o Fair Credit Reporting Act o Driver's Privacy Protection Act of 1994 o Farm Credit Act o Airline Deregulation Act of 1978 and Federal Aviation Act of 1958 o Family Educational Rights and Privacy Act of 1974 • Data regulated by the o federal Family Educational Rights and Privacy Act o federal Patient Safety and Quality Improvement Act (and the CT analog to that act) • Information of those applying to or employed by a controller, processor or third party or to administer benefits to employees and relatives ❖ **Controller / Processor activities <u>not</u> affected by CTDPA**: • All of the activities listed as <u>not</u> affected by LD 1973 (see column to immediate left) and • Cooperating with law enforcement concerning conduct the processor or controller in good faith believes may violate federal, state or local laws	• Conducting scientific, historical or statistical research that adheres to all relevant laws and regulations • Authenticating users of product or service • Carrying out a product recall under state or federal law • Delivering non-advertisement communication to an individual that is reasonably anticipated by their interaction with the entity • Delivering commination at direction of an individual • Ensuring security and integrity of covered data • Support individuals' participation in civil engagement, including voting, petitioning, unionizing, providing indigent legal services • Transferring assets to successor in interest after notice to affected individuals and reasonable opportunity to withdraw consent or request deletion of covered data • **Previously collected data** – distinct purposes allowed, including for targeted advertising (see page 6, lines 5-24)
Data minimization requirements	❖ Controller must limit **collection** of **personal data** to: • what is **adequate, relevant and reasonably necessary** to the processing purposes disclosed to the consumer ❖ All processing (collection, use, storage, disclosure, analysis or deletion) of **personal data** must also be: • **Reasonably necessary & compatible** the processing purposes disclosed to the consumer (unless controller obtains consumer's consent)	Same data minimization requirements as LD 1973 (see column to immediate left) *Note: After Oct. 1, 2024, additional data minimization requirements apply to minors' personal data (see p.16 of this chart)*	❖ All collection, processing and transferring of **covered data** must be: • For an **allowed purpose** (See list above) • **Reasonably necessary & proportionate** to that purpose ❖ All collection or processing of **sensitive data** must be: **Strictly necessary** to achieve an **allowed purpose** (other than to promote civic engagement)

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
Consent requirements for protected data	❖ Activities permitted **without consent** • **Processing** (includes collecting, processing and disclosing but <u>not</u> selling) of **non-sensitive personal data** for any purpose except targeted advertising	Same activities permitted without consent as LD 1973 (see column to immediate left)	❖ Activities permitted **without consent** • C**ollecting, processing or transferring covered data** to service provider for allowed purpose (see list above) • **Transfer *adult's* non-sensitive covered data to 3rd party** for allowed purpose
		❖ Activities permitted only with **choice to opt-out** • Processing personal data for **targeted advertising** • **Selling** of personal data <u>Exceptions</u>: "sale" defined to exclude the same activities excluded from "sale" in LD 1973 • Process personal data for "**profiling**" ("profiling" is described similarly to the description in LD 1973 but with an additional definition that isn't in LD 1973 [ii])	❖ Activities permitted only with **choice to opt-out** (*opt-out consent appears to be the intent of §9609(5) and §9610(1))* • **Transfer *adult's* non-sensitive covered data** to 3rd party for **other than** an **allowed purpose** (See list above *but see more limited and conflicting list in §9619(1)*) • **Targeted advertising** to person (unless the person is known to be a minor, in which case targeted advertising is completely prohibited as is described below)
	❖ Activities permitted only **with consent (opt-in)** • Processing **sensitive data** for **any purpose**(recall this includes all personal data of any minor under age 13) • Processing personal data for **targeted advertising** • **Selling** personal data <u>Exceptions</u>: "sale" defined to exclude sharing personal data with (a) processor; (b) 3rd party for purpose of providing requested product or service; (c) affiliate or (d) successor in interest after merger, bankruptcy or other transaction. • Process personal data for "**profiling**" (solely automated decisions producing legal or similarly significant effects)	❖ Activities permitted only **with consent (opt-in)** • Processing **sensitive data** for **any purpose** (recall this includes all personal data of any minor under age 13) • **Selling CHD** for any purpose • For **minors known to be ages 13-15**: [*Note: after Oct. 1, 2024 this opt-in consent requirement applies to all minors*] ○ Processing personal data for **targeted advertising** ○ **Selling** personal data <u>Exceptions</u>: "sale" defined to exclude the same activities excluded from "sale" in LD 1973 *Note: After Oct. 1, 2024, additional opt-in consent requirements related to minors' personal data apply under CTDPA (see page 16 of this chart)*	❖ Activities permitted only **with consent (opt-in)** • **Transfer** any **covered data of minor** to 3rd party <u>Exception</u>: Cybertip about child victims to NCMEC • **Transfer sensitive data** to a 3rd party <u>Exceptions</u>: may transfer (a) to comply with law; (b) to prevent imminent injury; (c) to a successor in interest; (d) to transfer password to identify reused passwords; (e) to transfer genetic info. for medical diagnosis or treatment • **Transfer** info on **video content or services** <u>Exceptions</u>: same as (a) to (e) above
	n/a [*Note: My original chart comparing LD 1973 and LD 1977 had a category of activities regarding data of minors age 13-15 potentially prohibited by LD 1973, regardless of consent. After comparing LD 1973 to the CTDPA, I no longer think these activities are prohibited.*]	n/a *Note: After Oct, 1, 2024, allowing certain unsolicited direct messaging from adults to minors is prohibited by CTDPA (see page 15 of this chart)*	❖ Other **prohibited** activities (regardless of consent) • Process or transfer **SSNs** (except for limited reasons—*e.g.*, for credit extension, authentication, collection or payment of taxes, enforce a contract, prevent fraud/crime or as required by law) • Process **sensitive data** for **targeted advertising** • **Targeted advertising** to person known to be a **minor** (stricter requirements for high-impact social media companies and data holders described below)

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
Definition of targeted advertising	**21. Targeted advertising.** "Targeted advertising" means displaying advertisements to a consumer when the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated publicly accessible websites or online applications to predict that consumer's preferences or interests. "Targeted advertising" **does not include**: A. Advertisements based on activities within a controller's own publicly accessible websites or online applications; B. Advertisements based on the context of a consumer's current search query, visit to a publicly accessible website or online application; C. Advertisements directed to a consumer in response to the consumer's request for information or feedback; or D. Processing personal data solely to measure or report advertising frequency, performance or reach.	Nearly same "targeted advertising" definition as in LD 1973 (see column to immediate left) Only difference from LD 1973: • CTDPA uses the phrase "Internet web sites" instead of "publicly accessible websites"	**18. Targeted advertising.** "Targeted advertising" means presenting to an individual or device identified by a unique identifier, or groups of individuals or devices identified by unique identifiers, an online advertisement that is selected based on known or predicted preferences, characteristics or interests associated with the individual or a device identified by a unique identifier. "Targeted advertising" **does not include** advertising or marketing to an individual or an individual's device in response to the individual's specific request for information or feedback; an advertisement displayed based on the content or nature of the publicly accessible website or service in which the advertisement appears and does not vary based on who is viewing the advertisement; or processing covered data strictly necessary for the sole purpose of measuring or reporting advertising or content, performance, reach or frequency, including independent measurement.
Requirements for consent	❖ **Consent (opt-in)** requirements: • Written or electronic statement that is specific and unambiguous • Freely given (user interface may not subvert or impair decision-making) • Opt-in consent must be provided by (a) consumer, (b) designated agent, guardian or conservator; or (c) parent or legal guardian of minor consumer <13 years old	❖ **Consent (opt-in)** requirements – nearly same as LD 1973 (see column to immediate left) except no provision for an agent, guardian or conservator to provide opt-in consent ❖ **Opt-out** – see requirements on next page. Also, for opt-out: • Consumer may designate an agent to opt-out if the controller can verify the agent's identity and authority • Consumer's guardian or conservator may opt-out	❖ **Consent (opt-in)** requirements: • Affirmative act that is specific and unambiguous • Freely given (not based on material misrepresentations and user interface may not be designed to impair decision-making) • Opt-in consent must be provided by (a) individual or (b) parent or legal guardian of a minor individual ❖ **Opt-out** – requirements not specified in the bill
	• *(Not explicit)* presumably consumer must be informed of the purposes for which personal data is processed (perhaps the privacy notice is sufficient for this purpose?)	Same non-explicit requirement for disclosure of processing purposes as LD 1973 (see column to immediate left)	• Made after standalone request from covered entity that: o Is made via primary medium used by covered entity to offer product or service o Is in each covered language (top 10 per US Census) used to sell the product or service o Is reasonably accessible to individuals w/disabilities o Clearly explains, with prominent headings, categories of data collected, processed or transferred and why o Clearly explains individual's rights related to consent

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
	• **Mechanism to opt-in:** (a) must be easy to use; (b) may not have opt-in as a default setting; (c) must be consistent with similar mechanisms required by other state or federal law; and (d) must enable controller to verify the Maine residency of the consumer & legitimacy of opt-in request • **Mechanism to revoke consent** must be at least as easy as mechanism to provide consent	• **Mechanism to opt-out**: (a) must be easy to use; (c) may not have a default setting (c) must be consistent with similar mechanisms required by other state or federal law; (d) must enable controller to verify the CT residency of the consumer & legitimacy of opt-out request and (e) must have link from controller's website to the page where you can opt out ○ May deny opt-out request if good faith documented belief it is fraudulent; but must notify the requester why • **Mechanism to revoke consent** must be at least as easy as mechanism to provide opt-in consent	• **Option to refuse** consent must be as prominent as and may not take more steps than granting consent • **Mechanism to withdraw consent** must be clear and conspicuous and as easy to execute as providing consent
	❖ Consent (opt-in) may **not** be based on: • Accepting a terms of use agreement (must be separate) • Hovering over, muting, pausing or closing content	Same prohibited methods of opt-in consent as LD 1973 (see column to immediate left)	❖ Consent may **not** be based on: • Individual's inaction • Individual's mere continued use of service or product
Discrimination and retaliation prohibitions	❖ **Controller** may not process (collect, use, disclose, analyze, delete) personal data in manner that violates state and federal laws prohibiting unlawful discrimination against consumers ❖ **Controller** may not discriminate against consumer for exercising a right under this law, including by: • Denying or charging different prices for goods or services • Providing different level or quality of goods or services Exception: • Need not offer product or service without having **required** personal data • May offer different price, quality or selection of goods or services via a **voluntary consumer loyalty program**	Same discrimination and retaliation prohibitions as LD 1973 (see column to immediate left)	❖ **Covered entity and service provider** may not collect, process or transfer covered data in manner that discriminates based on race, color, religion, national origin, sex or disability Exceptions: (a) self-testing to prevent discrimination; (b) collection or processing to diversify an applicant or customer pool; (c) private clubs not open to the public ❖ **Covered entity** may not retaliate against consumer for exercising a right under this law, including by: • Denying or charging different prices for goods/services • Providing different level or quality of goods or services Exceptions: • Need not offer product or service without having **strictly necessary** covered data • May offer different price, quality or selection of goods or services via a **voluntary consumer loyalty program only if** -- only necessary covered data is transferred to 3rd parties as part of the program, data transfers are disclosed to program members and transferred data is not retained for any other purpose by 3rd party. • May condition price or level of service on provision of financial information **for billing purposes** • May offer financial incentives to participate in **marketing studies** (with certain limits on top of p. 10)

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
Consumer / individual rights	❖ A **consumer has a right**, upon making an authenticated request, to: • **Confirm** whether controller processes personal data • **Access** own personal data processed by controller • **Correct inaccuracies** in personal data • **Delete** personal data about the consumer • Obtain a **portable copy** of own personal data from a controller Exceptions: • Controller need not disclose information that reveals a trade secret • Controller need not disclose de-identified data or data the controller is not reasonably capable of associating with the consumer • If controller did not itself collect the data the consumer requested be deleted, it may retain the data deletion request and minimum data necessary to ensure data remains deleted in its system	Same consumer rights and exceptions as in LD 1973 (see column to immediate left)	❖ A **consumer has a right**, upon personally or through an agent making an authenticated request, to: • **Download own** non-archived covered data collected, processed or transferred by the covered entity or its service provider within the previous **24 months** • Be told categories of **3rd party transferees for consideration** of covered data and for what purposes, with an option to request the names of 3rd party & service provider transferees • Be told the categories of **sources** from which covered data was collected • **Correct verified substantial inaccuracy or substantially incomplete info**. with reasonable efforts to notify 3rd parties & service providers of correction • **Delete** covered data with reasonable efforts to notify 3rd party and service provider transferees of request • If technically feasible, obtain **portable copy** for self or another entity of processed covered data not including derived data Exceptions: the 3 exceptions listed for LD 1973 apply Small differences: may refuse to disclose "privileged or confidential business info." not just trade secrets and may retain all data-deletion requests to ensure data remains deleted, not just for data it didn't itself collect Additional Exceptions: (not also in LD 1973) • Need not respond if request furthers fraud, criminal activity, a data security threat or interferes w/a contract • Need not respond if responding would require covered entity to engage in unfair or deceptive practice • Need not comply if would violate state or federal law or the federal constitutional rights of another individual • Need not comply if action would require access to or correction of another individual's sensitive data • Need not delete data if one of the reasons on p. 15 applies (see description of data deletion below)

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)

	❖ **Request / appeal process**:
	• Each consumer may make one free request per year –
	  ○ Except controller may charge a reasonable fee or decline to act on technically infeasible, excessive or repetitive requests with explanation to requester
	• Request process must be secure and reliable
	• Controller need not fulfill unauthenticated request, but must notify consumer of the unauthenticated request
	• Controller must act respond or decline to act on the request within 45 days of request; if declines to act, must provide justification and info. on how to appeal
	• **Appeal:** Consumer may appeal controller's inaction within a reasonable time and decision in response to appeal (with reasoning) is required within 60 days
	• If appeal is denied, must provide mechanism for consumer to submit a complaint to the AG
		Nearly same request / appeal processes as in LD 1973 (see column to immediate left)
		
		Only difference from LD 1973:
		• Controller may extend the initial 45-day response period once by 45 days if reasonably necessary and requester is informed of reason for the extension
			❖ **Request process**:
			• Each individual may make two free requests per year –
			  ○ Except covered entity may deny demonstrably impracticable or prohibitively costly requests, with explanation to requester
			• Request process must not be materially misleading or use an interface designed to impair reasonable choice
			• Request process must be both accessible and in all covered languages in which product/service is offered
			• If it cannot reasonably verify identity or authority of requester, covered entity may request additional info. from the requester for verification purposes only
			• Covered entity must respond or decline to act on the request within 60 days of request - may extend once by 45 days if reasonably necessary and requester is informed of reason for the extension

Required privacy notice / privacy policy	❖ **Controller** must provide accessible and clear privacy notice that includes:
	• Controller's contact information (e-mail or other)
	• Categories of personal data it processes
	• Purpose for processing personal data
	• How consumers may exercise their rights (may not require creation of a new account)
	• What categories of personal data are shared with what categories of 3rd parties
		Nearly same privacy notice requirements as in LD 1973 (see column to immediate left)
		
		Differences from LD 1973:
		• Privacy notice must be "reasonably" accessible
		• Privacy notice must also "clearly and conspicuously disclose":
		  ○ Controller's sale of personal data to 3rd parties;
		  ○ Controller's processing of personal data for targeted advertising; and
		  ○ Manner for consumer to opt-out of the above
			❖ **Covered entity and service provider** must provide readily accessible and clear privacy policy in each covered language it uses to offer a product or service, stating:
			• Name and contact information of the covered entity or service provider and all entities within the same corporate structure to which it transfers data
			• Categories of covered data it collects or processes
			• Processing purpose of each category of covered data
			• How long it intends to retain each category of covered data (or criteria it uses to decide the retention period)
			• Prominent description of how individuals may exercise their rights under LD 1977
			• What categories of covered data are shared with what categories of 3rd parties and for what purposes
			• General description of its data security practices
			• Effective date of the policy
			
			❖ **Material change: covered entity** must, before materially changing its policy for prospectively collected covered data:
			• Take reasonable measures to notify affected individuals
			• Provide reasonable opportunity to withdraw consents

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
Deletion of protected data	❖ **By request**: as is explained above, controller must delete protected data within 45 days of authenticated consumer request Exceptions: • may retain data deletion request and minimum data necessary to ensure data remains deleted in its system if the data to be deleted was collected by controller from a source other than the consumer • may decline a technically infeasible, excessive or repetitive request, subject to the appeal procedures stated above	Nearly same data deletion requirements as in LD 1973 (see column to immediate left) Only difference from LD 1973: • Controller may extend the initial 45-day period once by 45 days if reasonably necessary and requester is informed of reason for the extension *Note: After Oct. 1, 2024, controllers may not process minors' personal data for longer than reasonably necessary to provide a requested product or service. It is unclear if data deletion is also required. (See chart p. 16)*	❖ **By request**, as is explained above, covered entity must delete covered data within 60 days of authenticated request (may extend this time once by 45 days if reasonably necessary) Exceptions: need not comply with deletion request that: • unreasonably interferes with providing product/service to another person the covered entity currently serves • requires deletion of data of public figure or official and the requester has no expectation of privacy in that data • requires deletion of data necessary to perform a contract with requester • requires deletion of data that must be retained to comply with professional ethical obligations • requires deletion of data covered entity reasonably believes is evidence of unlawful activity or of an abuse of the covered entity's products or services • for private school (any grade level) covered entities, requires deletion of data that would unreasonably interfere with providing education services ❖ **In general**, covered entity and service provider must delete covered data when retention is no longer necessary for purpose for which the data was collected, processed or transferred Exceptions • If have affirmative consent (opt-in) to retain data • If service provider is required to retain data by law
Previously collected data	❖ **Controller** must, by July 1, 2025, delete consumer's personal data that it has for purposes of sale or targeted advertising unless consumer opts-in to the sale or targeted advertising	❖ **Controller** must, by July 1, 2025, adhere to consumer's choice to opt out of processing personal data for targeted advertising or sale even if that choice conflicts with prior privacy setting or prior participation in voluntary loyalty program (but controller may notify consumer of the conflict and give consumer a chance to change the setting or rejoin the program)	❖ **Covered entity** may process and transfer previously collected covered data for the specific purposes set forth on p. 6, lines 5-24 (this list differs from the list of allowed purposes for newly collected covered data)

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
Data Security (and Data Security Officers)	❖ **Controller** must: • Establish and implement reasonable data security and integrity practices appropriate to the volume and nature of the data • Process sensitive data of a child <13 years old in accordance with federal Children's Online Privacy Protection Act of 1988 (generally requires parental consent)	Same **general** data security requirements as LD 1973 (see column to immediate left) Additional data security requirements for **CHD**: • No person may **transfer CHD** to a processer unless the processor complies with its duties under CTDPA • No person may provide an employee or contractor with **access to CHD** "unless the employee or contractor is subject to a contractual or statutory duty of confidentiality"	❖ **Covered entity** and **service provider** must • Establish & implement reasonable data security practices to protect against unauthorized access appropriate to volume and nature of the data; size and complexity of entity; sensitivity of the data; current state-of-the art safeguards; and costs of security tools • Identify & assess internal & external risks to its systems • Prevent and mitigate identified reasonably foreseeable risks and vulnerabilities to covered data • Train employees with access to covered data • Implement procedures to detect and respond to security breaches • Designate a **privacy officer** and a **data security officer** ▪ To implement data security policies & ▪ To facilitate compliance with this law
Data Protection / Privacy Impact Assessments	❖ **Controller** must conduct and document **data protection assessment(s)** weighing benefits to controller, consumer and public of processing the data against the risks to consumers • **When?** Not specified • **What activities must be assessed?** All activities presenting a heightened risk to consumers including: ▪ Processing personal data for targeted advertising ▪ Sale of personal data ▪ Processing of personal data for profiling that presents a foreseeable risk of unfair treatment of consumers or of physical, reputational or financial injury to consumers ▪ Processing of sensitive data • **Copy to AG:** Must provide copy of assessment to AG on request (if relevant to an investigation). Assessment is not a public record for purposes of FOAA.	Same data protection assessment requirements as LD 1973 (see column to immediate left) *Note: After Oct. 1, 2024, after conducting data protection assessments for activities that present a heightened risk to minors, the controller must establish a plan to mitigate that risk (see chart p. 15)*	❖ **Covered entity** must conduct a written **privacy impact assessment** that is reasonable and appropriate in scope given the nature, volume and potential risks to privacy of the data collected, processed or transferred by the covered entity and that weighs the benefits of the covered entity's use of data against potential material adverse consequences to individual privacy • **When?** Every other year • **Also include**? Any additional info. required by AG • **What activities must be assessed?** All activities that may cause a substantial privacy risk • **Summary:** Covered entity must make a summary of the assessment publicly accessible and available to AG on request
Algorithm Impact Assessments	n/a	n/a (same as LD 1973)	❖ **Covered entity** using an (AI) **covered algorithm** (defined p.1) "in a manner that poses a consequential risk of harm" must**:** • Conduct **annual impact assessments**—see p. 18-19—including assessing algorithm's necessity and proportionality and describing steps taken to mitigate: harm to minors; use of algorithm to determine access to

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
			or restrictions on housing, education, employment, healthcare, insurance, credit, or public accommodations; and disparate impacts based on race, color, religion, national origin, sex, disability or political party status • Conduct a pre-deployment **design evaluation** to reduce risk of potential harms listed above • **Report to AG:** Must report summary of all assessments and design evaluations to AG within 30 days • **Public access:** Must make summary of all assessments and design evaluations publicly available • May redact trade secrets from summary to AG & public
Processor/ Service Provider duties and prohibitions	❖ **Processor** must: • Assist controller with responding to consumer requests • Assist controller with meeting data-security obligations • Notify controller of any security breach in processor's system • Assist controller with data protection assessments • Act only under contract with controller requiring it to: o Ensure each person processing personal data is subject to a duty of confidentiality o Delete or return personal data at end of services o Cooperate with controller assessments and/or share independent assessments of its own services o Require all subcontractors (if any) via written contract to comply with processor's obligations related to personal data ❖ **Processor** may <u>not</u>: • Process personal data beyond directions in contract with controller (otherwise, it assumes all responsibilities and liabilities of a controller under LD 1973)	Processor duties same as in LD 1973 (see column to immediate left) <u>Except:</u> CTDPA <u>also</u> requires the processor to give the controller the opportunity to object in advance to any subcontracts the processor enters	❖ **Service Provider** (even if only for government entities) must: • Assist covered entity responding to individuals' requests • Assist covered entity with privacy impact assessments and algorithm assessments • Cooperate with assessments by covered entity and/or share independent assessments of its own services • Act only pursuant to contract with covered entity that clearly sets forth: o Types of covered data to be processed o Instructions, purposes and duration for collecting, processing or transferring each data o A prohibition on comingling data from the covered entity and other sources unless specifically allowed o Requirement to provide advance notice to covered entity of any subcontracts and to provide written contract to subcontractors requiring compliance with processor's obligations related to covered data ❖ **Service Provider** (even if only for gov't entities) may <u>not:</u> • Collect, process or transfer covered data except pursuant to contract with covered entity (otherwise, it assumes all responsibilities of covered entity in LD 1977) • Collect, process or transfer personal data if it has knowledge covered entity violated law re: that data • Retain covered data after done providing services to covered entity, unless required to retain data by law

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
Third party duties and prohibitions	n/a	n/a (same as LD 1973)	❖ **Third party** (see definition page 5 of bill): may only process • **Covered data and sensitive data**: To complete a transaction for a requested product or service; to authenticate a user; or to prevent or detect a security incident (intrusion, medical alert, trespass or fire alarm); • **Non-sensitive data:** also for purpose disclosed in covered entity's privacy notice (recall transfer of non-sensitive data to a 3rd party has an opt-out requirement) • **Sensitive data:** also for purpose for which consumer gave opt-in consent to covered entity to transfer data ❖ **Third party** (see definition page 5 of bill) must enter contract with covered entity that: • Specifies purpose(s) for which covered data may be processed by 3rd party and not permit other processing • Requires 3rd party to adhere to data security requirements and all requirements of LD 1977
Regulation of de-identified data	❖ **Controller** in possession of **de-identified data** must: • Take reasonable measures to prevent re-identifying the data and publicly commit to not attempting to re-identify the data • Contractually obligate recipients of the data to comply with law and monitor compliance with those contractual commitments	Same controller duties re: de-identified data as in LD 1973 (see column to immediate left)	n/a
Special rules for special business types	n/a	n/a (same as LD 1973) (except see note about social media platforms on pp. 14 & 15)	❖ **Small Business**—*i.e.* non-data broker that, in past 3 years, had annual revenue <$41,000,000 and processed covered data of <200,0000 individuals per year (except for billing purposes): • May delete data in response to data-correction request • Relaxed requirements re: requests for portable data • Need not conduct privacy impact assessments • Need not conduct algorithm assessments • Need not train employees with access to covered data • Need not designate data security & privacy officers • **May not be sued by a private individual** ❖ **Data broker**—a covered entity other than a service provider that, in the prior 12-month period either had >50% revenue

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
			from processing data it didn't collect or processed or transferred data it didn't collect of >5,000,000 people • Must notify public of status as data broker on website and mobile applications • Must annually register with AG and disclose: name of contact person, phone number, mailing address, email address, website, and categories of covered data it processes and transfers o Penalty: $100/day civil penalty (max. $10,000/year) ❖ **Large data holder**—covered entity or service provider that, in past calendar year, (a) had ≥ $250,000,000 annual gross revenue; and (b) collected, processed or transferred covered data >5 million people or devices/year (except for billing purposes) • Must comply with **individuals' requests** to exercise their rights within 45 days (instead of 60 days) • Must receive and investigate **unsolicited reports of vulnerabilities** in its data security systems • Must publish last 10 years' **privacy policies** on its website, clearly describe each material change to them, and, if also a covered entity, provide accessible short-form notice (<500 words) of individuals' rights and its data privacy practices, including unexpected practices • **Annual statistics** must be disclosed by July 1st of each year on its website: number of verified requests to access or delete data; number of requests to opt-out of data transfers or targeted advertising; number of requests complied with; and average days to comply • Executive officer must **certify to AG** annually entity's good faith compliance w/law (see description on p.17) • Designate a **privacy protection officer** (who reports directly to CEO) to periodically review privacy and security practices; conduct biennial comprehensive audits accessible to AG; develop training program for employees; and be the contact for enforcement • May not engage in **targeted advertising** in willful disregard of the fact the individual targeted is a **minor**

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
		Note: After Oct. 1, 2024, "social media platforms" (as defined in CTDPA) must comply with minors' requests to unpublish their accounts (see page 15 of this chart)	❖ **High-impact social media company**—service primarily to share user-generated content with ≥ $3 billion annual revenue and ≥300 million monthly active users in 3 of 12 prior months • May not engage in **targeted advertising** either if it should have known or if it is in willful disregard of – the fact that the individual targeted is a **minor**
Remedies for violations	❖ **Attorney General** may bring action under Unfair Trade Practices Act (UTPA) against a controller or processer: • Must first provide notice of violation and **30-day right to cure**; may not initiate action if controller or processor asserts in writing the alleged violations have been cured and no future violations will occur ❖ **No private right of action** ❖ No AG power to make rules interpreting LD 1973	❖ **CT Attorney General** may bring action under CT Unfair Trade Practices Act to enforce the provisions of the CTDPA • Before Dec. 31, 2024: must first provide notice and a **60-day right to cure**; if controller fails to cure the violation in that time, AG may bring an action • Beginning Jan. 1, 2025: AG has **discretion** whether to give controller or processor an **opportunity to cure**, depending on: number of violations; size and complexity of defendant and nature of its processing activities; likelihood of injury to public, safety of persons or property; whether violation was caused by human or technical error; and sensitivity of the data ❖ **No private right of action**	❖ **Attorney General, DA or Municipal Counsel** may bring an action on behalf of Maine residents against a covered entity or service provider for: • Injunctive relief to enforce compliance with law/rules • Damages, civil penalties, restitution or other compensation; and • Reasonable attorney's fees and litigation costs ❖ **Private action** by individual injured by violation of law/rules against entity committing violation (**except small business**) for: • At least a $5,000 civil penalty per individual, per violation or actual damages, whichever is greater • Punitive damages (no limit/amount stated) • Injunctive and declaratory relief • Reasonable attorney's fees and litigation costs ❖ Pre-dispute **arbitration agreements** are unenforceable
Exceptions to liability	❖ **Exceptions to liability** for all enforcement actions: • Controller not liable if processor violates LD 1973 absent knowledge that processor would violate the law • Processor not liable for controller's violations	Same exceptions to liability as in LD 1973 and LD 1977	Same exceptions to liability as in LD 1973 and CTDPA
Repeal of other laws	❖ **Repeals 35-A M.R.S. §9301**, which generally requires Internet Service Providers (ISPs) to obtain consent before using, disclosing or selling a customer's personally identifying info. **See handout showing law to be repealed*	n/a (same as LD 1977)	n/a
Geofence prohibitions	n/a	❖ **No person may create a geofence** (virtual boundary within 1750 feet of facility) to identify, track, collect data from or send notices to consumers regarding the consumer's CHD around: • A mental health facility or • A reproductive or sexual health facility	n/a

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
Effective Date	90 days after adjournment (most of bill) Exception • By July 1, 2025, consumer must opt-in to use of previously collected data for targeted advertising or sale	July 1, 2023: All except CHD-specific provisions and child online safety provisions described below October 1, 2023: All CHD provisions (including geofences) July 1, 2024: The following **additional child online safety provision** takes effect: • "**Social media platforms**" (as defined in CTDPA) must (a) "**unpublish**" (remove from public visibility) the account of a minor within 15 days of receiving an authenticated unpublishing request and (b) **delete** the account and cease processing the personal data of a minor within 45 days of receiving an authenticated deletion request; this 45-day deletion period may be extended once by up to 45 days with notice to the requester if the extension is reasonably necessary. Requests may be made by minors ages 16-17 or parents of minors under 16. The mechanism for making these requests must be described in a privacy notice. October 1, 2024: The following **additional child online safety provisions** take effect: • Controllers that offer online services, products or features to consumers with actual knowledge or in willful disregard of the fact that they are minors must: o Take **reasonable care** to avoid any "heightened risk of harm" caused by the online service, product or feature (includes unfair or deceptive treatment of or disparate impact on minors; financial, reputational or physical injury to minors; or intrusion on private affairs of minors that would be offensive to a reasonable person); o **Not offer direct messaging** without easy-to-use safeguards prohibiting adults from sending unsolicited communications to minors. This prohibition does not apply to email or text/photo/video text messaging between devices only visible to sender and recipient. o Conduct **a data protection assessment** for processing minors' data evaluating any "heightened risk of harm" and establish a plan to mitigate any heightened risk	180 days after adjournment (most of bill) Exceptions: • 1 year later: privacy impact assessment and large data holder certification requirements take effect • 2 years later: algorithm assessment requirement takes effect

Detailed comparison of LD 1973 and LD 1977 and the Connecticut Data Privacy Act (CTDPA)

	LD 1973 (Keim)	Connecticut Data Privacy Act (CTDPA)	LD 1977 (O'Neil)
		• Controllers that offer online services, products or features to consumers with actual knowledge or in willful disregard of the fact that they are minors must -- **unless the controller has voluntary consent** of a minor ages 13-17 or of a parent of a minor under age 13: o **Not process** minors' personal data **for (a) targeted advertising (b) sale or (c) profiling** o **Not process** minors' personal data unless **reasonably necessary** to provide its service, product or feature o **Not process** minors' personal data for any purpose **other than the purpose disclosed** at time of collection o **Not process** minors' personal data **longer than reasonably necessary** to provide its service, product or feature o **Not use any system to significantly prolong minors' use** of its product, service or feature o **Not** use minors' **precise geolocation data** unless this data is reasonably necessary to provide its service, product or feature and the minor is notified throughout the entire duration of the collection • **Exemptions:** similar list of exemptions to rest of CTDPA • **Enforcement:** CT Attorney General may bring action under CT Unfair Trade Practices Act. **Until Dec. 1, 2025** there is a **30-day right to cure** similar to the other right to cure provisions in the CTDPA that are described above.	

[i] Under LD 1973 (and the CTDPA) "publicly available information," which is not protected, is defined as follows:

"Publicly available information" means information that is:
A. Lawfully made available through federal, state or municipal government records or widely distributed media; and
B. Information that a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

[ii] Under the CTDPA, Conn. Gen. Stat. §42-515(30): "Profiling" means any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Info. Requested from Retail Association of Maine

11/8/23 WS
LDs 1977, 1973
1902, 1705

Stocco, Janet

From:	Curtis Picard <curtis@retailmaine.org>
Sent:	Friday, November 3, 2023 3:36 PM
To:	Carney, Anne; Moonen, Matt; Bailey, Donna; Brakey, Eric; Andrews, John; Dana, Aaron; Haggan, David; Henderson, Rachel; Kuhn, Amy; Lee, Adam; Moriarty, Steve; Poirier, Jennifer; Sheehan, Erin; Stocco, Janet; JUD
Subject:	Follow up information requested by the Committee on Consumer Data Privacy
Attachments:	One Pager on CT Data Privacy Law - Retail Obligations.pdf

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

I am writing to provide additional information that was requested by the committee at the October 17th work session, as well as additional information that has been requested since then.

1. We were asked to provide additional sourcing and data regarding the number of lawsuits that have been filed against small businesses under the Illinois biometric law. Hopefully, these links are helpful:

https://www.reuters.com/legal/legalindustry/illinois-court-decisions-acknowledge-biometric-privacy-acts-damages-potential-2023-04-17/

https://news.wttw.com/2023/09/22/illinois-supreme-court-weighs-another-biometric-privacy-lawsuit-lawmakers-consider-child

https://www.cbsnews.com/chicago/news/illinois-biometric-data-privacy-business/

Not printed

https://www.littler.com/files/wpi_rpt_bipa_white_paper_0623.pdf

2. For the benefit of our retail members, we drafted up a short document detailing the requirements of the Connecticut comprehensive privacy law which is similar to LD 1973. (See attached) → printed + attached

Some of the advocates testified that the CT law was meaningless. I would respectfully disagree. The provisions in the CT law are significant, and it will be challenging for Maine's small retailers and other consumer facing businesses to comply.

Regardless, we can support the CT framework as a viable privacy model as consistency is important, and the experience of retailers in CT as they navigate compliance will be helpful if Maine follows a similar path.

3. We were asked for additional information regarding the unintended consequence of the Washington state privacy model, and a retailer's ability to sell typical household healthcare products like toothpaste, aspirin and rash cream.

I would first point to the Washington AG website where they maintain an FAQ about the law. Questions 5 and 6 refer to this issue: https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy

→ printed + attached

Additionally, I wrote in our written testimony on October 17: It is worth noting the amendment to the Connecticut data privacy act defines "consumer health data" as ***any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis***. Examples provided include gender-affirming health data and reproductive or sexual health data. The "identify" language is critically important since selling a product, providing an advertisement or coupon for it, etc. does not mean that a retailer is trying to identify or wishes to know a consumer's physical or mental health condition. Rather, the retailer is simply trying to make available to customers the products they need and prefer. The product involved may be intended for use by the purchaser, a family member, a neighbor or other third party. Washington state made this mistake in their consumer health data law, which has resulted in retailers having to obtain consent for purchases of products as benign as aspirin and rash cream. This is why it is so important to keep these provisions focused on the areas of concern (generally, reproductive privacy) and not any product that could be tangentially related to a sweeping definition of "health."

I hope this information is helpful, and I will attend the work session next Wednesday afternoon. I am happy to answer any questions and provide additional information.

Sincerely,

Curtis Picard

Curtis Picard, CAE, *President & CEO, Retail Association of Maine*
45 Melville Street, Suite 1
Augusta, ME 04330
Tel: 207.623.1149 | Mobile: 207.240.7377
curtis@retailmaine.org | www.retailmaine.org

RETAIL ASSOCIATION OF MAINE
Voice of Maine Retail
45 Melville Street, Suite 1
Augusta, ME 04330
Phone: 207.623.1149
www.retailmaine.org

Short Summary of the Connecticut Data Privacy Act ("CTDPA")
Submitted by the Retail Association of Maine
November 2, 2023

1. Consumer Rights
    a. A business must honor consumers' rights, which include the right to access (in a portable format), correct, delete, opt-out, and appeal.
    b. The opt-out right includes, opting out of the "sale" of data, targeted advertising, and profiling (profiling means "in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer." (e.g., financial, housing, education)). (4(a))
        i. The word sale takes on the meaning given to it by the CCPA. It is defined as the "exchange of personal data for monetary or other valuable consideration." (1(26))
        ii. A business must have a clear and conspicuous link on its website to allow a consumer to opt-out. (6(e)(A)(i))
        iii. By 1/1/25, businesses must honor a preference signal that the consumer sets on their browser. (6(e)(A)(ii)
    c. Businesses must process requests received by a consumer's authorized agent. (4(b))
    d. A business must collect consent prior to processing Sensitive Data (6(a)). Sensitive Data includes certain attributes (such as race, religion, health condition/diagnosis), biometric information, information about a known child, and precise geolocation data (within 1,750 feet). (1(27))
2. Obligations
    a. Data minimization
        i. A business must only process Personal Data when it is "reasonably necessary and proportionate to the stated purpose and adequate, relevant, and limited to what is necessary to achieve the stated purpose." (10(f))
    b. Data security
        i. Processing Personal Data is subject to reasonable administrative, technical, and physical measures to protect confidentiality, integrity, and accessibility. (6(a)(3) and 10(f))
    c. Privacy policy
        i. The business' privacy notice must include the categories of Personal Data processed, the purpose for processing, the consumer's options to take advantage of their privacy rights (including how to appeal a controller's

decision), the categories of Personal Data shared with third parties, and the categories of those third parties. (6(c))

d. Agreements with processors
    i. Businesses must have a signed contract with each Service Provider/Processor that processes Personal Data. Contracts must include the purpose of processing, confidentiality obligations, destruction/return of Personal Data requirement, obligation for the Processor to have its sub processor under written contract, and audit rights. (7(b))
e. Data Protection Assessment
    i. A Data Protection Assessment must be completed and recorded internally, which documents the risks, benefits, and mitigation efforts regarding any processing activity that poses a significant risk of harm (e.g., sale of data, targeted advertising, profiling, processing of Sensitive Personal Data). (8(a))

3. Enforcement
    a. The Attorney General enforces the CT law. A 60 day right to cure period is used for the first 1 ½ years after the law is effective. If the business fails to cure within that time, then the AG may bring an action pursuant to this section.

Protecting Washingtonians' Personal Health Data and Privacy

Washington is a national leader in protecting the privacy of consumer health decisions and health data. In 2023, Attorney General Bob Ferguson requested legislation to significantly expand privacy protections for personal health data. The Washington My Health My Data Act (HB 1155 (https://app.leg.wa.gov/billsummary?BillNumber=1155&Initiative=false&Year=2023)) passed the Washington State Legislature on April 17, 2023, and was signed into law by Governor Jay Inslee on April 27, 2023. Washington My Health My Data Act, 2023 Wash. Laws 191.

The My Health My Data Act is the first privacy-focused law in the country to protect personal health data that falls outside the ambit of the Health Insurance Portability and Accountability Act, or HIPAA. The Act was developed to protect a consumer's sensitive health data from being collected and shared without that consumer's consent. Washington's concern for the urgent need to enhance privacy protections for health data is widely shared: 76% of Washingtonians express support for the My Health My Data Act.

Under the law, regulated entities must follow specific requirements about how and when they may collect and share personal health data.

Frequently Asked Questions

1: What are the effective dates for the My Health My Data Act?

The My Health My Data Act includes effective dates on a section-by-section basis.

All persons, as defined in the Act, must comply with section 10 beginning July 23, 2023. Regulated entities that are not small businesses must comply with sections 4 through 9 beginning March 31, 2024. Small businesses, as defined in the Act, must comply with sections 4 through 9 beginning June 30, 2024. For sections 4 through 9, the effective dates apply to the entirety of the section and are not limited to the subsections in which the effective dates appear.

2: What is the Attorney General's role in enforcing the My Health My Data Act?

Section 11 of the My Health My Data Act provides that any violation of the Act is a *per se* violation of the Washington Consumer Protection Act (CPA), RCW 19.86, which is enforced by the Attorney General as well as through private action.

3: How will a business located outside of the state of Washington but that stores its data in Washington be impacted?

Generally, all persons and businesses that conduct business in Washington (or provide services or products to Washington), and that collect, process, share, or sell consumer health data are impacted by the Act. Subject to some exceptions, a regulated entity is a legal entity that (a) conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington and (b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data. An entity that only stores data in Washington is not a regulated entity.

A processor is as a person that processes consumer health data on behalf of a regulated entity or a small business. Out-of-state entities that are processors for regulated entities or a small business must comply with the Act.

Sections 9 and 10 of the Act apply to persons, which generally includes natural persons, corporations, trusts, unincorporated associations, and partnerships. Out-of-state entities that fall within the definition of person must comply with sections 9 and 10 of the Act.

4: Is a business that is covered by the My Health My Data Act required to place a link to its Consumer Health Data Privacy Policy on the company's homepage?

Yes. Section 4(1)(b) of the My Health My Data Act explicitly provides that "[a] regulated entity and a small business shall prominently publish a link to its consumer health data privacy policy on its homepage."

5: Does the definition of consumer health data include the purchase of toiletry products (such as deodorant, mouthwash, and toilet paper) as these products relate to "bodily functions"?

Information that does not identify a consumer's past, present, or future physical or mental health status does not fall within the Act's definition of consumer health data. Ordinarily, information limited to the purchase of toiletry products would not be considered consumer health data. For example, while information about the purchase of toilet paper or deodorant is not consumer health data, an app that tracks someone's digestion or perspiration is collecting consumer health data.

6: If a regulated entity or small business draws inferences about a consumer's health status from purchases of products, could that information be considered consumer health data?

Yes. The definition of consumer health data includes information that is derived or extrapolated from nonhealth data when that information is used by a regulated entity or their respective processor to associate or identify a consumer with consumer health data. This would include potential inferences drawn from purchases of toiletries. For example, in 2012 the media reported that a retailer was assigning shoppers a "pregnancy prediction score" based on the purchase of certain products; this information is protected consumer health data even though it was inferred from nonhealth data. Likewise, any inferences drawn from purchases could be consumer health data.

In contrast, nonhealth data that a regulated entity collects but does not process to identify or associate a consumer with a physical or mental health status is not consumer health data.

7: How may a regulated entity or a small business comply with its obligation to retain copies of a consumer's valid authorization for sale of consumer health data under section 9 and a consumer's request to delete their consumer health data under section 6 of the Act?

Under section 9 of the My Health My Data Act, it is unlawful for anyone to sell or offer to sell consumer health data without first obtaining valid authorization from the consumer. When a consumer grants a person valid authorization to sell their consumer health data, both the seller and purchaser are required to retain a copy of the valid authorization for six years. Section 6 of the My Health My Data Act empowers consumers to have their consumer health data deleted from a regulated entity's or small business' network, including archived or backup systems.

If after executing a valid authorization, a consumer exercises their section 6 right to have their consumer health data deleted, a regulated entity or small business may meet its obligation to delete the consumer's health data and its obligation to retain a copy of the valid authorization by redacting the portion of the valid authorization that specifies the consumer health data for sale (for example, by applying a redaction that states: "REDACTED pursuant to consumer deletion request on [insert date]").

This FAQ may be periodically updated and is provided as a resource for general educational purposes and is not provided for the purpose of giving legal advice of any kind. Readers should not rely on information in this guide regarding specific applications of the law and instead should seek private legal counsel.

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

MEMORANDUM

TO: Joint Standing Committee on Judiciary

FROM: Janet Stocco, Legislative Analyst

DATE: November 8, 2023

RE: **Updated list of amendments proposed to consumer privacy bills**

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

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

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

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

This memorandum provides an updated list of the amendments to LD 1705, LD 1902, LD 1973 and LD 1977 requested either in testimony presented at the public hearings on these bills or during the work session held on October 17, 2023.

a) Technical and Drafting Issues Identified by Analyst

- *Technical drafting issues*: Each bill has multiple technical drafting issues, including ambiguous language, internal inconsistencies, and technical violations of state drafting standards. The committee may wish to authorize the analyst to work with the relevant bill sponsor or specific committee member(s) to work through these issues after a substantive vote to move forward with a bill has been taken**.**
- *More substantive issues*: The bill analysis dated October 17, 2023 list several substantive drafting issues identified by the analyst for each bill. The committee may wish to address these issues as part of any motion in favor of an amended version of any of these bills.

b) Amendments for all 4 consumer privacy bills requested by stakeholders

- *Hospitality Maine*
  - All industry sectors – *i.e.*, both the parties that collect the data and downstream parties with whom customers do not interact – should be directly regulated by privacy legislation. Legislation should not, for example, limit regulation of downstream parties to contractual obligations.
- *Maine State Police*:
  - Clarify all entities regulated by these bills must share information (including sensitive data) with law enforcement pursuant to subpoenas or search warrants validly obtained under federal or state law.
- *Multiple industry representatives*:
  - Eliminate all privates right of action
  - Require notice and opportunity to cure prior to Attorney General enforcement actions
  - Prefer opt-out consent for collecting and processing of most personal data; however, a few industry representatives are amenable to opt-in consent for certain sensitive information (biometrics, health data, data of minors, etc.) or for certain uses of personal data (sale or targeted advertising).

- Generally, prefer a comprehensive data privacy law to standalone bills for different data, especially to avoid creating conflicting definitions and conflicting regulations through different legislation

- *MaineHealth*
  - Provide entity-level exemption for entities regulated by federal HIPAA

- *Maine Grocers and Food Producers Association / Retail Association of Maine*
  - Strongly opposed to private right of action and lack of notice and opportunity to cure
  - Due to seasonal sales volumes, data privacy laws should have a July 1st not a Jan. 1st effective date;
  - Delay the effective date by at least 2 years, to allow Maine businesses to comply; and
  - Provide reduced regulation for small businesses, *e.g.*, those that employ < 50 employees.

c) Amendments to LD 1705 (Biometric identifiers) requested by stakeholders

- *AvaMed*: *See* language proposed in testimony.
  - More clearly exclude information subject to federal laws, federal regulations and state laws governing access to health care information.

- *CCIA: See* proposed language in testimony.
  - Eliminate the private right of action;
  - Add a 30-day right to cure;
  - Amend definition of "BIs" (a) to include only data generated by automated measurements of a consumer's biological characteristics; (b) to exclude all photographs or videos without qualification; and (c) to exclude publicly available and de-identified information;
  - Amend definition of "personal information" to exclude publicly available and de-identified data; and
  - Amend definition of "consent" to include electronic consent (*analyst*: electronic consent is already authorized under §9604(3) of LD 1705).

- *Center for Progress*:
  - Clarify the prohibition against discrimination based on failure to allow collection, processing or transfer of BIs, unless use of the BI is "strictly necessary" to the sale of goods or provision of the service. What if the use of BIs makes the service convenient and efficient and less risky to the entity? What if different family members have different choices but one smart device?

- *Maine Credit Union League and Maine Bankers Association*:
  - Exempt financial institutions subject to the Gramm-Leach-Bliley Act.

- *MaineHealth*. *See* language proposed in testimony dated October 17, 2023.
  - Prefers entity-level exception for health care providers regulated by HIPAA (LD 1705 currently only exempts protected health information subject to HIPAA).
  - If committee does not agree to entity-level exception for HIPAA-regulated entities, propose instead:
    - Amend definition of "biometric identifier" to exclude "information collected, used or stored for health care treatment, payment or operations under [HIPAA]"
    - Amend definition of "affirmative written consent" to allow private entities to use an employee's affirmative written consent to use the employee's biometric identifier to allow the employee to access not only secured physical locations and secure computer software and hardware (as in the bill) but also to access "medications or medical supplies" and allow the use of BIs for employee tracking.
    - Also allow "affirmative written consent" to be a default setting when it is a condition of employment.

- *Maine Grocers and Food Producers Association / Retail Association of Maine*
  - Disclosure requirements in LD 1705 are too expansive, requiring disclosure of information it may be impossible for entities to produce

- *Professor Scott Bloomberg (Maine Law):*
  - Consider amending the definition of "BIs" to include biometric data—for example, about facial characteristics like smiling, eye movements—even when it is not used to identify a specific individual, as these involuntary movements reveal consumer preferences.

d) Amendments or LD 1902 (Consumer Health Data) requested by stakeholders

- *AvaMed*: *See* language proposed in testimony.
  - More clearly exclude information subject to federal laws, federal regulations and state laws governing access to health care information.
- *Anthem & Maine Auto Dealers Association*:
  - Exempt the insurance industry, which is already subject to extensive regulation, from the provisions of the bill.
- *CCIA*:
  - More narrowly define "CHD" to avoid situations where data about purchases of feminine care products, toilet paper or undergarments is considered CHD by: (a) removing "efforts to research health care services or supplies," (b) removing info. related to "bodily functions" and (c) within the definition of "gender-affirming care services," a type of CHD, removing "products that . . . affirm an individual's gender identity";
  - Narrow the definition of "location information" to focus not on whether that data could be used to indicate a consumer's attempt to receive health care services or supplies but instead to focus on whether the company is collecting or processing the data for that purpose—*e.g.*, allow a directions app to collect location information for purposes of providing a patient with directions to a clinic;
  - Eliminate the private right of action; and
  - Include at least a 30-day right to cure period for enforcement actions by the Attorney General.
- *Consumer reports*: *See* language proposed in testimony dated Oct. 11, 2023.
  - Define the type of "discrimination" prohibited when a consumer chooses not to consent to collection or sharing of CHD—*i.e.* denying goods or services, charging different prices and providing a different level or quality of service.
- *EPIC:*
  - Limit the collection of CHD to instances where it is "strictly necessary" to provide a product or service requested by the consumer—*i.e.*, eliminate the option for a consumer to consent to the collection of CHD and strengthen the "necessary" standard for collecting CHD without consent.
- *findhelp: See* language proposed in testimony dated Oct. 11, 2023.
  - Broaden the definition of "CHD" to include "social care information"—*i.e.*, information that relates to the need for, payment for, or provision of "social care" including day care, housing, transportation, and employment services, etc.
- *MaineHealth*: *See* language proposed in testimony dated October 17, 2023.
  - Prefers entity-level exception for health care providers (LD 1902 currently only exempts protected health information when it is subject to HIPAA and all of the requirements of HIPAA are met).
  - If committee does not agree to entity-level exception for health care providers, propose instead:
    - Amend definition of "Biometric data" to exclude physical or digital photographs, videos, or audio recordings or data generated from them as well as information collected, used or stored for health care treatment, payment or operations under HIPAA
    - Amend definition of "CHD" to exempt "health care information"—as defined in 22 M.R.S. §1711-C(1)(E)—obtained for "health care"—as defined in §1711-C(1)(C)
    - Allow health care facilities to erect geofences *around their own facilities*

- *Maine Bureau of Insurance*:
  - Exempt from the bill data and information covered by the state Insurance Information and Privacy Protection Act (Title 24-A, Chapter 24 of the Maine Revised Statutes), which governs the collection, use and disclosure of information gathered in connection with insurance transactions in the State or by insurance organizations of Maine residents. (The bureau enforces this law.)
- *Maine Grocers and Food Producers Association / Retail Association of Maine*
  - Amend definition of "CHD" as personal information that a regulated entity "uses to identify" a consumer's physical or mental health condition or diagnosis, not any information that reveals such conditions or diagnoses (to avoid requiring retailers to obtain consumer consent for purchases of products theoretically linkable to health conditions)
- *National Insurance Crime Bureau*:
  - Exempt from the bill's scope information shared to prevent, detect, protect against, respond to, investigate, report or aid in the prosecution of malicious, deceptive or illegal activities, security incidents, identity theft, fraud or harassment (for example, information shared with NICB under Maine's Insurance Information and Privacy Protection Act, Title 24-A, chapter 24 to prevent insurance fraud)
  - Exempt from the bill's scope "insurance-support organizations" as defined in Maine's Insurance Information and Privacy Protection Act (Title 24-A, chapter 24 of the Maine Revised Statutes)
- *TechNet*:
  - Exempt entities subject to regulation by HIPAA, not just the "protected health information" that is subject to regulation by HIPAA;
  - Narrow the definition of "CHD" to exclude information "derived" or "extrapolated" from CHD, which if included could have unintended consequences,
  - Define the types of "medication" purchases included in the definition, to avoid situations where data on purchases of toilet paper or feminine hygiene products is considered CHD.

e) Amendments to LD 1973 (general consumer privacy; Keim) requested by stakeholders

- *ACLU of Maine and Maine Broadband Coalition*:
  - Oppose LD 1973, specifically the repeal of Maine's ISP privacy law (35-A M.R.S. 9301).
- *CCIA*:
  - Limit requirement for opt-in consent to processing or sale of sensitive data, otherwise apply an opt-out consent approach for sale and processing of non-sensitive consumer data;
  - Amend the definition of "consent" to remove the affirmative act requirement and not exclude acceptance of terms of use agreement or hovering over, muting, pausing or closing a given piece of content;
  - Amend the definition of "processor" to include not just persons but also legal entities that process data on behalf of a controller (*analyst note:* under 1 M.R.S. §72(15) when "person" is used in Maine statute it "may include a body corporate");
  - Amend definition of "sale" of personal data to include only sales for monetary consideration not sales for "other valuable consideration";
  - Expand the provisions of §9603(1)(A) and (D), which exempt controllers from confirming that they process personal data or to providing a portable copy of that personal data to consumers if doing so would reveal a "trade secret" to also exclude instances where the disclosure would reveal "sensitive business information"; and
  - Provide a delayed effective date of no earlier than January 1, 2025 to provide businesses with adequate time to comply with the law.
- *Maine Attorney General*:
  - Do not repeal Maine's ISP privacy law (35-A M.R.S. 9301)

- Do not limit the bill's applicability to entities that control or process the data of ≥100,000 Maine residents or of ≥ 25,000 Maine residents and derive > 25% of their gross revenue from selling personal data—because most Maine businesses do not reach these thresholds and would be exempt from the bill;
- Narrow the list of categorical exemptions from the bill, some of which may be inappropriate and the inclusion of which may render the bill vulnerable to constitutional challenge;
- Do not exempt sale of data to an "affiliate" from the prohibition on selling data without consent;
- Expand the definition of "targeted advertising" to include targeted advertising within the controller's own websites and applications;
- Do not prohibit the AG's office from promulgating interpretive rules;
- Allow private rights of action (AG's office has insufficient staff to ensure compliance);
- Do not require 30-day right to cure (although adding a right to cure period for a private right of action may be a compromise position);
- Do not allow companies to offer financial incentives to disclose data through consumer loyalty programs; and
- Do not allow actions in compliance with other state's laws if they violate this legislation.

- *Maine Chamber of Commerce*:
  - Supports LD 1973 if the opt-in consent requirement is limited to the processing of sensitive data only.

- *Multiple industry representatives*:
  - Support LD 1973 if opt-in consent requirements are changed to opt-out consent to match CTDPA

f) Amendments to LD 1977 (general consumer privacy; O'Neil) requested by stakeholders

- *Sponsor—Representative O'Neil*
  - Amend §9614(1) of the bill – the anti-discrimination provision – to prohibit discrimination on the basis of all characteristics protected under the Maine Human Rights Act

- *ACLU of Maine*
  - Add definitions for: "collect," "transfer," "process" and "publicly available information"
  - Require Internet Service Providers to comply with existing law in 35-A M.R.S. §9301 (*analyst note*: this could be accomplished by exempting ISPs from LD 1977 provided they are complying with 35-A M.R.S. §9301)
  - Narrow the definition of a "small business" that is exempt from the private right of action
  - Completely ban the sale or lease of biometric identifiers (even with consent)
  - Amend §9614(1) of the bill – the anti-discrimination provision – to prohibit discrimination on the basis of all characteristics protected under the Maine Human Rights Act
  - Strengthen the anti-discrimination provisions of §9607 (*analyst note*: §9607(3)(E) appears to allow entities to charge a different price or offer a different product or service to individuals who exercise their rights under the act, directly contradicting §9607(1)).
  - Amend bill to require adult customers to opt-in to targeted advertising (*analyst note:* the bill currently provides for adults to opt-out of targeted advertising but prohibits all targeted advertising to individuals known to be minors)

- *Alliance for Automotive Innovation*
  - Do not require that data generated from vehicles' onboard computer systems and sensors be included within the requirement of §9611(1)(A)(1) that, in response to a consumer request, all covered data be provided to the individual "in a format that a reasonable individual can understand and download from the Internet"

- *American Council of Life Insurers*
  - Exempt "financial institutions" (including insurers) regulated by federal Gramm-Leach-Bliley Act

- *Association of National Advertisers, American Association of Advertising Agencies, Interactive Advertising Bureau, American Advertising Federation and Digital Advertising Alliance*
  - Amend the bill to exempt "pseudonymous data"—data that cannot be attributed to a specific individual without additional information and that is kept separately from that information—from the consumer rights of access, correction, deletion and portability
  - Amend the bill to remove "information identifying an individual's online activities over time and across third party websites or online services" from the definition of "sensitive data," which the bill prohibits using for purposes of targeted advertising
  - Allow consumers to opt-out of targeted advertising rather than requiring them to opt-in (*analyst note:* it is unclear in §9610(1) of LD 1977 whether opt-in or opt-out consent is required)
  - Amend §9611(1)(A)(2) to require only disclosure of the categories of 3rd parties to whom covered entities transfer covered data, and not also the names of these service providers and 3rd parties
  - Remove the private right of action and allow enforcement only by the Attorney General
- *Consumer Healthcare Products Association (CHPA)*
  - Exempt from the bill's prohibitions the sharing of personal data with law enforcement as required under the Controlled Substances Act, 21 U.S.C. §830
    (*analyst note*: LD 1977 allows covered entities to collect, process and transfer data to comply with federal, state, local or tribal laws; however, this authorization is not an exemption from the bill's requirements related to data minimization and opt-in consent for the transferring of sensitive data)
- *Consumer Reports*:
  - Allow an authorized agent, not just the consumer, to exercise the consumer's privacy rights (*analyst note*: although the rest of the bill is unclear, language on page 14, line 38 suggests that an "individual authorized to make a request on the individual's behalf" may exercise these rights)
- *Fidelity Investments*
  - Exempt "financial institutions" subject to federal Gramm-Leach-Bliley Act and their affiliates
- *Financial Industry Regulatory Authority*: *See* language proposed in testimony dated Oct. 17, 2023.
  - Define the "government agencies" who are exempt from the bill under §9603(1) to include FINRA, which is a nonprofit regulator of the securities industry that operates under the authority of the Securities Exchange Act of 1934 but is not a federal government agency.
  - Also allow sharing of data with FINRA by covered entities and service providers under §9604(2).
- *L.L. Bean*: objects to several ways in which LD 1977 differs from other state privacy laws, including:
  - Overly broad definition of "sensitive data"—including income level, family or social relationship information and information on individual's online activities
  - Requiring covered entities to identify every service provider with which it shares personal data (*analyst note*: this appears to be a critique of §9611(1)(A)(2)(b))
  - Requiring opt-in consent for using non-sensitive covered data for targeted advertising (*analyst note*: it is unclear in §9610(1) whether opt-in or opt-out consent is required)
  - Authorizing private rights of action and statutory damages with no showing of harm
  - Not providing any reasonable exceptions to customer's right to access and/or delete data
  - Failure to exempt from the bill's scope information a business collects regarding its employees
  - Other issue (unrelated to other state laws): need to define "a consequential risk of harm" for purposes of defining which algorithms require impact assessments under §9615
- *Maine Attorney General*
  - Add definitions for: "authenticate," "collect," "transfer," "derived data," "process," "processing purpose," "publicly available information" and "reasonably understandable"
  - Amend definition of "sensitive data" to more clearly include web browsing history
  - Consider amending definition of "small business" so more businesses are included

- Consider exempting information collected by health care providers from the bill
- Permit transfer sensitive information to 3rd parties when necessary to comply with federal or Maine law at the time the sensitive data was collected, but not subsequently enacted laws or laws in other states that may differ from Maine law. Also require notice to individuals whenever sensitive data is transferred to 3rd parties under this provision.
- Clarify that privacy policies must be understandable and provide sufficient detail regarding 3rd parties to which covered data is transferred.
- Restructure §9604 (the allowed purposes provision) for clarity
- Strengthen §9607's protections against discrimination against those who exercise rights
- Amend §9611 to require a covered entity to disclose on request not only the covered data it has for the individual but also the "publicly available" information it has for that individual and to explain why it believes that this information is publicly available (ex: it must identify source of public data)
- Consider amending §9611 to establish an appeal process when a covered entity denies an individual's request to obtain access to information held by that covered entity
- Consider amending §9617(4) to require covered entities to share privacy impact assessments (not just summaries of the assessments) with the Attorney General and to retain those assessments for 5 years
- Consider authorizing an award of liquidated damages or specific monetary penalty in cases brought by individuals (*analyst note*: LD 1977 establishes a minimum $5,000 damages amount for cases brought by individuals)
- Clarify other provisions of the bill (not specified)

- *Maine Automobile Dealers Association*
  - Do not include private right of action
  - Use opt-out model of consumer consent rather than opt-in consent; and
  - Resolve conflicts between the bill and existing state laws, including (a) the requirement in 10 M.R.S. §1475(2-A)(B) that a dealer selling a used car generally must, on request, disclose the name and address of the previous owner of the vehicle (unless the car was purchased through an out-of-state auction from a non-resident of Maine); (b) requirements under other laws that dealers retain driver's license numbers (considered "sensitive data" in bill); and (c) 10 M.R.S. §1174(3)(V), which regulates when an automobile dealer may share customer information with manufacturers, distributors or wholesalers

- *Maine Bankers Association, Kennebec Savings Bank and Bangor Savings Bank*
  - Exempt "financial institutions" regulated by federal Gramm-Leach-Bliley Act

- *Maine Credit Union League*
  - Exempt "financial institutions" regulated by the federal Gramm-Leach-Bliley Act
  - Exempt information shared by financial institutions under the Fair Credit Reporting Act
  - Eliminate private right of action (preferred) or greatly reduce statutory damages from the minimum $5,000 per occurrence in the bill to $500-$750 per occurrence as in California

- *MaineHealth*: *See* language proposed in testimony dated October 17, 2023.
  - Prefers entity-level exception for health care providers
  - If committee does not agree to entity-level exception for health care providers, propose instead:
    - Exclude "protected health information collected, used or disclosed in accordance with the [HPAA] and implementing regulations" from the scope of the bill
    - Exclude "health care information"—as defined in 22 M.R.S. §1711-C(1)(E)—obtained for "health care"—as defined in §1711-C(1)(C)—from "covered data" protected by bill
    - Amend definition of "biometric information" to exclude "information collected, used or stored for health care treatment, payment or operations under [HIPAA]"

- *Maine Grocers and Food Producers Association / Retail Association of Maine*
  - Prefers Connecticut-type legislation (like LD 1973 except only require opt-out consent)

  - Prefers the language in Connecticut authorizing customer loyalty programs

- *Maine State Chamber of Commerce*
  - Prefers Connecticut-type legislation to LD 1977, especially lack of private right of action

- *National Retail Federation*: Prefers LD 1973 / Connecticut model, especially because:
  - Objects to the private right of action and lack of a notice and opportunity to cure when enforcement actions are brought by the Attorney General
  - LD 1973's language allowing opt-in, voluntary consumer loyalty programs is preferable to the additional requirements imposed in LD 1977 that don't exist in other states

- *Planned Parenthood of Northern New England*
  - Exclude "protected health information" as defined in HIPAA that is held by "covered entities" or "business associates" as those terms are defined in HIPAA

- *Restore the Fourth*
  - Include a definition of "sale" of data to include not only the exchange of data for money, but also the exchange of data for "other valuable consideration" (*analyst note*: LD 1977 does not refer to the "sale" of personal data, rather it refers only to the "transfer" of that data, an undefined term. By contrast, LD 1973 regulates the "sale" of covered data and defines "sale" to include exchange for money or other valuable consideration)
  - Do not provide extra protections for data of minors in a way that requires companies to unnecessarily collect information about whether a particular customer is a minor; alternative options: prohibit targeted advertising of individuals of all ages or require companies to accept self-attestations of customers that they are or are not minors

- *State Farm Mutual Insurance Company*
  - Exempt entities that comply with federal GLBA and HIPAA from the bill's requirements
  - Remove the private right of action
  - Prefers an opt-in approach to regulating privacy over an opt-out approach

- *State Privacy & Security Coalition*. Generally, prefers LD 1973 to LD 1977; especially because:
  - LD 1977's definitions of various business types ("covered entity," "covered high-impact social medial company," "data broker," "large data holder," "service provider," "small business" and "third party") are not only unclear but they also may be overlapping to some degree
  - LD 1977 requires additional definitions, for example what does it mean to "transfer" data?
  - LD 1977 should be limited to Maine customers or businesses operating in Maine
  - LD 1977 should not prohibit first-party advertising (see definition of "targeted advertising")
  - "Strictly necessary" test for collecting or processing sensitive data is unclear and overly restrictive
  - LD 1977's definition of "sensitive data" is overly broad
  - LD 1977 should not include a private right of action

- *Wex, Inc.*
  - Amend definition of "large data holder" or eliminate the large data holder requirements
  - Exempt data protected under HIPAA and other federal data protection laws
  - Omit private right of action – possibly by amending §9620 (enforcement) to remove authority of Attorney General or private litigants to bring enforcement actions. Instead, establish a new "Maine Privacy Protection Authority" staffed by both privacy and business experts with the power to detect, investigate and bring actions to punish violations of the law as well as the power to educate both consumers and businesses about the law's requirements.
  - Extend the effective date to allow at least 1 year for companies to comply with the law

Stocco, Janet

From: Murray, Joseph <Joseph.Murray@fmr.com>
Sent: Friday, November 3, 2023 10:46 AM
To: Stocco, Janet
Subject: Fidelity Investments / Privacy Legislation

Hi Janet,

I hope this statement from Fidelity Investments is arriving in time for consideration by the Joint Standing Committee on Judiciary. Thank you for inviting us to provide our comments below:

Fidelity Investments appreciates the opportunity to provide input on the comprehensive privacy legislation (LD 1977, LD 1973) under consideration by the Maine Legislature. Fidelity serves more than 275,000 individual customers in Maine and has 31 employees in the state, most of whom work at our investor center in Portland.

We are supportive of legislative efforts to preserve and protect consumer data privacy. As custodians of our customers' information, Fidelity upholds high standards to protect and safeguard against security breaches, unauthorized use, or sale to unaffiliated third parties. We as a firm adhere to the robust standard of data privacy principles laid out under Title V of the Gramm-Leach-Bliley Act (GLBA) for financial institutions.

Maintaining our current framework of data privacy, predicated on GLBA's requirements, across our firm's business is core to our privacy culture and to the customer experience we provide. This privacy framework that our affiliates operate under provides a seamless, coherent user experience for consumers using products with one standard of data privacy. We prioritize this transparent, familiar experience for our customers by supporting consistent application of privacy standards across all types of data. Navigating state-by-state requirements with differing data privacy standards for different types of data – for example, biometric or health data versus personal identifying information – layers additional, confusing complexity for both customers and the financial institutions they rely on.

We support efforts to create standards of accountability for consumer data for companies doing business in Maine and believe the current GLBA framework that governs our operations is complementary to that process. It is also important to clarify in legislation that GLBA-covered entities and their affiliate companies are exempt from a bill's requirements. This approach will allow us to continue to utilize the GLBA framework that provides regulatory clarity for our firm, continuity of business across affiliate entities, and ease of experience for our customers. Without any impending federal legislation regulating this issue on the horizon, aligning a consistent standard across states is paramount to avoid confusion for both consumers and companies. Please feel free to contact me with any questions.

Thank you for considering our position.

Joe

Joe Murray
VP, Government Relations & Public Affairs
Fidelity Investments | Corporate Affairs

 Fidelity Newsroom  joseph.murray@fmr.com  603-689-3301

Pending Legislation in Congress + Other States
Info from Office of Attorney General

11/8/23 WS
LDs 1977, 1973
1902, 1705

Stocco, Janet

From: Hayes, Danna <Danna.Hayes@maine.gov>
Sent: Friday, October 20, 2023 3:32 PM
To: Stocco, Janet
Subject: FW: Privacy - work session
Attachments: Californa data broker one delete legislation.pdf; SAfe Act for kids 10.4.23 3.30 PM.PDF; Child privacy law.PDF

Hey Janet,
Good seeing you this week! Here is an email from Brendan with more info he wanted you to have. Also, can we have a copy of the packet you handed out to the committee? I didn't see it online, but I may have missed it.
Thank you!
Danna

Following is information that I recommend we share with Janet Stocco, which is information about new laws/legislation at the state and federal level, which I did not get to in Tuesday's work session.

→ printed + attached

Regarding state legislation which I mentioned in my comments to the Committee, see attached:

- California (newly signed "Delete Act", SB 362, regarding a one-stop deletion request for data brokers),
- New York (newly-introduced social media and children's data legislation),
- Massachusetts (health data privacy legislation, ADPPA version – neither attached but we can get them), and others.

Regarding Question 6 and pending Congressional proposals, there has been some reporting about at least four Congressional proposals which may have bipartisan support: (Not printed, see links below)

- The "Informing Consumers About Smart Devices Act", to alert consumers when devices are equipped with a camera or microphone;
- The "Platform Accountability and Transparency Act", to require certain companies, including social media companies, to make available to independent researchers the data, metrics, and other information of the companies;
- The "DELETE (Data Elimination and Limiting Extensive Tracking and Exchange) Act" – this is the Congressional version of the California data broker one-stop deletion bill signed into law last week; and
- The "Deceptive Experiences to Online Users Reduction Act", to address website, application, and service designs that manipulate consumer consent and also to prohibit the design of online products that lead to compulsive usage by children.

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

SB-362 Data broker registration: accessible deletion mechanism. (2023-2024)

Date Published: 10/12/2023 02:00 PM

Senate Bill No. 362

CHAPTER 709

An act to amend Sections 1798.99.80, 1798.99.81, 1798.99.82, and 1798.99.84 of, and to add Sections 1798.99.85, 1798.99.86, 1798.99.87, and 1798.99.89 to, the Civil Code, relating to data brokers.

[Approved by Governor October 10, 2023. Filed with Secretary of State October 10, 2023.]

LEGISLATIVE COUNSEL'S DIGEST

SB 362, Becker. Data broker registration: accessible deletion mechanism.

The California Consumer Privacy Act of 2018 (CCPA) grants a consumer various rights with respect to personal information that is collected or sold by a business, including the right to request that a business disclose specified information that has been collected about the consumer, to request that a business delete personal information about the consumer that the business has collected from the consumer, and to direct a business not to sell or share the consumer's personal information, as specified. The CCPA defines various terms for these purposes. The California Privacy Rights Act of 2020 (CPRA), approved by the voters as Proposition 24 at the November 3, 2020, statewide general election, amended, added to, and reenacted the CCPA and establishes the California Privacy Protection Agency (agency) and vests the agency with full administrative power, authority, and jurisdiction to enforce the CCPA.

Existing law requires a data broker to register with the Attorney General, pay a registration fee, and provide specified information on or before January 31 following each year in which a business meets the definition of data broker. Existing law defines various terms for these purposes. Existing law establishes the Data Brokers' Registry Fund and requires that these registration fees be deposited into the fund, to be available for expenditure by the Department of Justice, upon appropriation, for specified purposes. Existing law provides that a data broker that fails to register as required by these provisions is liable for civil penalties, fees, and costs in an action brought by the Attorney General, as specified, and requires these moneys be deposited in the Consumer Privacy Fund with the intent that they be used to fully offset costs incurred in connection with these provisions. Existing law requires the Attorney General to create and maintain an internet website where specified information provided by data brokers is accessible to the public.

This bill would incorporate the definitions from the CCPA into the data broker provisions described above. The bill would require a data broker to register with, pay a registration fee to, and provide information to, the agency instead of the Attorney General and would require the agency to maintain the informational internet website described above. The bill would require a data broker to compile and disclose specified information relating to requests received under the CCPA. The bill would also require, on or before July 1 following each year in which a business meets the definition of a data broker, that business to provide specified information described above and make related changes. The bill would make a data broker that fails to register as required by the provisions described above liable for administrative fines and costs in an administrative action brought by the agency, as

specified, instead of in an action brought by the Attorney General.

This bill would require the agency to establish, by January 1, 2026, an accessible deletion mechanism that, among other things, allows a consumer, through a single verifiable consumer request, to request that every data broker that maintains any personal information delete any personal information related to that consumer held by the data broker or associated service provider or contractor. The bill would specify requirements for this accessible deletion mechanism, and would, beginning August 1, 2026, require a data broker to access the mechanism at least once every 45 days and, among other things, process all deletion requests, except as specified. Beginning August 1, 2026, after a consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant to the bill's provisions, the bill would require the data broker to delete all personal information of the consumer at least once every 45 days, as specified, and would prohibit the data broker from selling or sharing new personal information of the consumer, as specified. The bill would, beginning January 1, 2028, and every 3 years thereafter, require a data broker to undergo an audit by an independent third party to determine compliance with these provisions and would require the data broker to submit an audit report to the agency upon the agency's written request, as specified. The bill would authorize the agency to charge a fee to data brokers for accessing the accessible deletion mechanism, as specified.

This bill would provide that a data broker that fails to comply with the requirements pertaining to the accessible deletion mechanism described above is liable for administrative fines, fees, expenses, and costs, as specified. The bill would require that moneys collected or received by the agency and the Department of Justice under these provisions be deposited in the Data Brokers' Registry Fund, which the bill would require to be administered by the agency, instead of the Consumer Privacy Fund and would expand the specified uses of moneys in the Data Brokers' Registry Fund to include the costs incurred by the state courts and the agency in connection with enforcing these provisions and the costs of establishing, maintaining, and providing access to the accessible deletion mechanism described above.

This bill would require a data broker to provide additional information to the agency, including information related to requests received under the CCPA, whether the data broker collects specified information, and specified information regarding an audit under the provisions described above.

This bill would prohibit an administrative action pursuant to these provisions from being commenced more than 5 years after the date on which a violation occurred.

This bill would declare that it furthers the purposes and intent of the CPRA for specified reasons.

Vote: majority Appropriation: no Fiscal Committee: yes Local Program: no

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. Section 1798.99.80 of the Civil Code is amended to read:

1798.99.80. For purposes of this title:

(a) The definitions in Section 1798.140 shall apply unless otherwise specified in this title.

(b) "Authorized agent" has the same meaning as used in Chapter 1 (commencing with Section 7000) of Division 6 of Title 11 of the California Code of Regulations.

(c) "Data broker" means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. "Data broker" does not include any of the following:

(1) An entity to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

(2) An entity to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations.

(3) An entity to the extent that it is covered by the Insurance Information and Privacy Protection Act (Article 6.6 (commencing with Section 791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code).

(4) An entity, or a business associate of a covered entity, to the extent their processing of personal information is exempt under Section 1798.146. For purposes of this paragraph, "business associate" and "covered entity" have the same meanings as defined in Section 1798.146.

SEC. 2. Section 1798.99.81 of the Civil Code is amended to read:

1798.99.81. A fund to be known as the "Data Brokers' Registry Fund" is hereby created within the State Treasury. The fund shall be administered by the California Privacy Protection Agency. All moneys collected or received by the California Privacy Protection Agency and the Department of Justice under this title shall be deposited into the Data Brokers' Registry Fund, to be available for expenditure by the California Privacy Protection Agency, upon appropriation by the Legislature, to offset all of the following costs:

(a) The reasonable costs of establishing and maintaining the informational internet website described in Section 1798.99.84.

(b) The costs incurred by the state courts and the California Privacy Protection Agency in connection with enforcing this title, as specified in Section 1798.99.82.

(c) The reasonable costs of establishing, maintaining, and providing access to the accessible deletion mechanism described in Section 1798.99.86.

SEC. 3. Section 1798.99.82 of the Civil Code is amended to read:

1798.99.82. (a) On or before January 31 following each year in which a business meets the definition of data broker as provided in this title, the business shall register with the California Privacy Protection Agency pursuant to the requirements of this section.

(b) In registering with the California Privacy Protection Agency, as described in subdivision (a), a data broker shall do all of the following:

(1) Pay a registration fee in an amount determined by the California Privacy Protection Agency, not to exceed the reasonable costs of establishing and maintaining the informational internet website described in Section 1798.99.84 and the reasonable costs of establishing, maintaining, and providing access to the accessible deletion mechanism described in Section 1798.99.86. Registration fees shall be deposited in the Data Brokers' Registry Fund, created within the State Treasury pursuant to Section 1798.99.81, and used for the purposes outlined in this paragraph.

(2) Provide the following information:

(A) The name of the data broker and its primary physical, email, and internet website addresses.

(B) The metrics compiled pursuant to paragraphs (1) and (2) of subdivision (a) of Section 1798.99.85.

(C) Whether the data broker collects the personal information of minors.

(D) Whether the data broker collects consumers' precise geolocation.

(E) Whether the data broker collects consumers' reproductive health care data.

(F) Beginning January 1, 2029, whether the data broker has undergone an audit as described in subdivision (e) of Section 1798.99.86, and, if so, the most recent year that the data broker has submitted a report resulting from the audit and any related materials to the California Privacy Protection Agency.

(G) A link to a page on the data broker's internet website that does both of the following:

(i) Details how consumers may exercise their privacy rights by doing all of the following:

(I) Deleting personal information, as described in Section 1798.105.

(II) Correcting inaccurate personal information, as described in Section 1798.106.

(III) Learning what personal information is being collected and how to access that personal information, as described in Section 1798.110.

(IV) Learning what personal information is being sold or shared and to whom, as described in Section 1798.115.

(V) Learning how to opt out of the sale or sharing of personal information, as described in Section 1798.120.

(VI) Learning how to limit the use and disclosure of sensitive personal information, as described in

Section 1798.121.

(ii) Does not make use of any dark patterns.

(H) Whether and to what extent the data broker or any of its subsidiaries is regulated by any of the following:

(i) The federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

(ii) The Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations.

(iii) The Insurance Information and Privacy Protection Act (Article 6.6 (commencing with Section 791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code).

(iv) The Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or 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 federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191).

(I) Any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(c) A data broker that fails to register as required by this section is liable for administrative fines and costs in an administrative action brought by the California Privacy Protection Agency as follows:

(1) An administrative fine of two hundred dollars ($200) for each day the data broker fails to register as required by this section.

(2) An amount equal to the fees that were due during the period it failed to register.

(3) Expenses incurred by the California Privacy Protection Agency in the investigation and administration of the action as the court deems appropriate.

(d) A data broker required to register under this title that fails to comply with the requirements of Section 1798.99.86 is liable for administrative fines and costs in an administrative action brought by the California Privacy Protection Agency as follows:

(1) An administrative fine of two hundred dollars ($200) for each deletion request for each day the data broker fails to delete information as required by Section 1798.99.86.

(2) Reasonable expenses incurred by the California Privacy Protection Agency in the investigation and administration of the action.

(e) Any penalties, fines, fees, and expenses recovered in an action prosecuted under subdivision (c) or (d) shall be deposited in the Data Brokers' Registry Fund, created within the State Treasury pursuant to Section 1798.99.81, with the intent that they be used to fully offset costs incurred by the state courts and the California Privacy Protection Agency in connection with this title.

SEC. 4. Section 1798.99.84 of the Civil Code is amended to read:

1798.99.84. The California Privacy Protection Agency shall create a page on its internet website where the registration information provided by data brokers described in paragraph (2) of subdivision (b) of Section 1798.99.82 and the accessible deletion mechanism described in Section 1798.99.86 shall be accessible to the public.

SEC. 5. Section 1798.99.85 is added to the Civil Code, to read:

1798.99.85. (a) On or before July 1 following each calendar year in which a business meets the definition of a data broker as provided in this title, the business shall do all of the following:

(1) Compile the number of requests pursuant to subdivision (c) of Section 1798.99.86 and Sections 1798.105, 1798.110, 1798.115, 1798.120, and 1798.121 that the data broker received, complied with in whole or in part, and denied during the previous calendar year.

(2) Compile the median and the mean number of days within which the data broker substantively responded to requests pursuant to subdivision (c) of Section 1798.99.86 and Sections 1798.105, 1798.110, 1798.115,

1798.120, and 1798.121 that the data broker received during the previous calendar year.

(3) Disclose the metrics compiled pursuant to paragraphs (1) and (2) within the data broker's privacy policy posted on their internet website and accessible from a link included in the data broker's privacy policy.

(b) In its disclosure pursuant to paragraph (3) of subdivision (a) regarding requests made pursuant to subdivision (c) of Section 1798.99.86, a data broker shall disclose the number of requests that the data broker denied in whole or in part because of any of the following:

(1) The request was not verifiable.

(2) The request was not made by a consumer.

(3) The request called for information exempt from deletion.

(4) The request was denied on other grounds.

(c) In its disclosure pursuant to paragraph (3) of subdivision (a), a data broker shall, for each provision of Section 1798.145 or 1798.146 under which deletion was not required, specify the number of requests in which deletion was not required in whole, or in part, under that provision.

SEC. 6. Section 1798.99.86 is added to the Civil Code, to read:

1798.99.86. (a) By January 1, 2026, the California Privacy Protection Agency shall establish an accessible deletion mechanism that does all of the following:

(1) Implements and maintains reasonable security procedures and practices, including, but not limited to, administrative, physical, and technical safeguards appropriate to the nature of the information and the purposes for which the personal information will be used and to protect consumers' personal information from unauthorized use, disclosure, access, destruction, or modification.

(2) Allows a consumer, through a single verifiable consumer request, to request that every data broker that maintains any personal information delete any personal information related to that consumer held by the data broker or associated service provider or contractor.

(3) Allows a consumer to selectively exclude specific data brokers from a request made under paragraph (2).

(4) Allows a consumer to make a request to alter a previous request made under this subdivision after at least 45 days have passed since the consumer last made a request under this subdivision.

(b) The accessible deletion mechanism established pursuant to subdivision (a) shall meet all of the following requirements:

(1) The accessible deletion mechanism shall allow a consumer to request the deletion of all personal information related to that consumer through a single deletion request.

(2) The accessible deletion mechanism shall permit a consumer to securely submit information in one or more privacy-protecting ways determined by the California Privacy Protection Agency to aid in the deletion request.

(3) The accessible deletion mechanism shall allow data brokers registered with the California Privacy Protection Agency to determine whether an individual has submitted a verifiable consumer request to delete the personal information related to that consumer as described in paragraph (1) and shall not allow the disclosure of any additional personal information when the data broker accesses the accessible deletion mechanism unless otherwise specified in this title.

(4) The accessible deletion mechanism shall allow a consumer to make a request described in paragraph (1) using an internet service operated by the California Privacy Protection Agency.

(5) The accessible deletion mechanism shall not charge a consumer to make a request described in paragraph (1).

(6) The accessible deletion mechanism shall allow a consumer to make a request described in paragraph (1) in any language spoken by any consumer for whom personal information has been collected by data brokers.

(7) The accessible deletion mechanism shall be readily accessible and usable by consumers with disabilities.

(8) The accessible deletion mechanism shall support the ability of a consumer's authorized agents to aid in the

deletion request.

(9) The accessible deletion mechanism shall allow the consumer, or their authorized agent, to verify the status of the consumer's deletion request.

(10) The accessible deletion mechanism shall provide a description of all of the following:

(A) The deletion permitted by this section, including, but not limited to, the actions required by subdivisions (c) and (d).

(B) The process for submitting a deletion request pursuant to this section.

(C) Examples of the types of information that may be deleted.

(c) (1) Beginning August 1, 2026, a data broker shall access the accessible deletion mechanism established pursuant to subdivision (a) at least once every 45 days and do all of the following:

(A) Within 45 days after receiving a request made pursuant to this section, process all deletion requests made pursuant to this section and delete all personal information related to the consumers making the requests consistent with the requirements of this section.

(B) In cases where a data broker denies a consumer request to delete under this title because the request cannot be verified, process the request as an opt-out of the sale or sharing of the consumer's personal information, as provided for under Section 1798.120 and limited by Sections 1798.105, 1798.145, and 1798.146.

(C) Direct all service providers or contractors associated with the data broker to delete all personal information in their possession related to the consumers making the requests described in subparagraph (A).

(D) Direct all service providers or contractors associated with the data broker to process a request described by subparagraph (B) as an opt-out of the sale or sharing of the consumer's personal information, as provided for under Section 1798.120 and limited by Sections 1798.105, 1798.145, and 1798.146.

(2) Notwithstanding paragraph (1), a data broker shall not be required to delete a consumer's personal information if either of the following apply:

(A) It is reasonably necessary for the data broker to maintain the personal information to fulfill a purpose described in subdivision (d) of Section 1798.105.

(B) The deletion is not required pursuant to Section 1798.145 or 1798.146.

(3) Personal information described in paragraph (2) shall only be used for the purposes described in paragraph (2) and shall not be used or disclosed for any other purpose, including, but not limited to, marketing purposes.

(d) (1) Beginning August 1, 2026, after a consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant to this section, the data broker shall delete all personal information of the consumer at least once every 45 days pursuant to this section unless the consumer requests otherwise or the deletion is not required pursuant to paragraph (2) of subdivision (c).

(2) Beginning August 1, 2026, after a consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant to this section, the data broker shall not sell or share new personal information of the consumer unless the consumer requests otherwise or selling or sharing the personal information is permitted under Section 1798.145 or 1798.146.

(e) (1) Beginning January 1, 2028, and every three years thereafter, a data broker shall undergo an audit by an independent third party to determine compliance with this section.

(2) For an audit completed pursuant to paragraph (1), the data broker shall submit a report resulting from the audit and any related materials to the California Privacy Protection Agency within five business days of a written request from the California Privacy Protection Agency.

(3) A data broker shall maintain the report and materials described in paragraph (2) for at least six years.

(f) (1) The California Privacy Protection Agency may charge an access fee to a data broker when the data broker accesses the accessible deletion mechanism pursuant to subdivision (d) that does not exceed the reasonable costs of providing that access.

(2) A fee collected by the California Privacy Protection Agency pursuant to paragraph (1) shall be deposited in the Data Brokers' Registry Fund.

SEC. 7. Section 1798.99.87 is added to the Civil Code, to read:

1798.99.87. (a) Except as provided in subdivision (b), the California Privacy Protection Agency may adopt regulations pursuant to the Administrative Procedure Act (Chapter 3.5 (commencing with Section 11340) of Part 1 of Division 3 of Title 2 of the Government Code) to implement and administer this title.

(b) Notwithstanding subdivision (a), any regulation adopted by the California Privacy Protection Agency to establish fees authorized by this title shall be exempt from the Administrative Procedure Act (Chapter 3.5 (commencing with Section 11340) of Part 1 of Division 3 of Title 2 of the Government Code).

SEC. 8. Section 1798.99.89 is added to the Civil Code, to read:

1798.99.89. No administrative action brought pursuant to this title alleging a violation of any of the provisions of this title shall be commenced more than five years after the date on which the violation occurred.

SEC. 9. The Legislature finds and declares that this act furthers the purposes and intent of the California Privacy Rights Act of 2020 by ensuring consumers' rights, including the constitutional right to privacy, are protected by enabling and empowering Californians to request that data brokers delete their personal information and prohibiting data brokers from collecting consumers' personal information in the future.

Legislative Bill Drafting Commission
11334-09-3

S. --------
Senate

IN SENATE--Introduced by Sen

--read twice and ordered printed, and when printed to be committed to the Committee on

-------- A.
Assembly

IN ASSEMBLY--Introduced by M. of A.

with M. of A. as co-sponsors

--read once and referred to the Committee on

GENEBULA
(Establishes the Stop Addictive Feeds Exploitation (SAFE) for Kids act prohibiting the provision of addictive feeds to minors)

Gen Bus L. SAFE for kids act

AN ACT

to amend the general business law, in relation to enacting the Stop Addictive Feeds Exploitation (SAFE) for Kids act prohibiting the provision of an addictive feed to a minor

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

IN SENATE

Senate introducer's signature

The senators whose names are circled below wish to join me in the sponsorship of this proposal:

s15 Addabbo	s34 Fernandez	s28 Krueger	s01 Palumbo	s42 Skoufis
s43 Ashby	s60 Gallivan	s24 Lanza	s21 Parker	s11 Stavisky
s36 Bailey	s12 Gianaris	s16 Liu	s19 Persaud	s45 Stec
s57 Borrello	s59 Gonzalez	s50 Mannion	s13 Ramos	s35 Stewart-Cousins
s46 Breslin	s26 Gounardes	s04 Martinez	s05 Rhoads	
s25 Brisport	s53 Griffo	s07 Martins	s33 Rivera	s44 Tedisco
s55 Brouk	s40 Harckham	s02 Mattera	s39 Rolison	s06 Thomas
s09 Canzoneri-Fitzpatrick	s54 Helming	s48 May	s61 Ryan	s49 Walczyk
	s41 Hinchey	s37 Mayer	s18 Salazar	s52 Webb
s17 Chu	s47 Hoylman-Sigal	s03 Murray	s10 Sanders	s38 Weber
s30 Cleare		s20 Myrie	s23 Scarcella-Spanton	s08 Weik
s14 Comrie	s31 Jackson	s51 Oberacker		
s56 Cooney	s27 Kavanagh	s58 O'Mara	s32 Sepulveda	
s22 Felder	s63 Kennedy	s62 Ortt	s29 Serrano	

IN ASSEMBLY

Assembly introducer's signature

The Members of the Assembly whose names are circled below wish to join me in the multi-sponsorship of this proposal:

a078 Alvarez	a047 Colton	a034 Gonzalez-Rojas	a146 McMahon	a103 Shrestha
a031 Anderson	a140 Conrad		a137 Meeks	a016 Sillitti
a121 Angelino	a032 Cook	a150 Goodell	a017 Mikulin	a052 Simon
a037 Ardila	a039 Cruz	a116 Gray	a122 Miller	a075 Simone
a035 Aubry	a043 Cunningham	a100 Gunther	a051 Mitaynes	a114 Simpson
a120 Barclay	a021 Curran	a139 Hawley	a145 Morinello	a094 Slater
a106 Barrett	a018 Darling	a083 Heastie	a144 Norris	a005 Smith
a105 Beephan	a053 Davila	a028 Hevesi	a045 Novakhov	a118 Smullen
a107 Bendett	a072 De Los Santos	a128 Hunter	a069 O'Donnell	a022 Solages
a082 Benedetto	a003 DeStefano	a029 Hyndman	a091 Otis	a110 Steck
a027 Berger	a070 Dickens	a079 Jackson	a132 Palmesano	a010 Stern
a042 Bichotte Hermelyn	a054 Dilan	a104 Jacobson	a088 Paulin	a127 Stirpe
	a081 Dinowitz	a011 Jean-Pierre	a141 Peoples-Stokes	a102 Tague
a117 Blankenbush	a147 DiPietro	a134 Jensen		a064 Tannousis
a015 Blumencranz	a009 Durso	a115 Jones	a023 Pheffer Amato	a086 Tapia
a073 Bores	a099 Eachus	a077 Joyner		a071 Taylor
a098 Brabenec	a048 Eichenstein	a125 Kelles	a063 Pirozzolo	a001 Thiele
a026 Braunstein	a074 Epstein	a040 Kim	a089 Pretlow	a033 Vanel
a138 Bronson	a109 Fahy	a013 Lavine	a019 Ra	a055 Walker
a046 Brook-Krasny	a061 Fall	a065 Lee	a030 Raga	a143 Wallace
a020 Brown, E.	a008 Fitzpatrick	a126 Lemondes	a038 Rajkumar	a112 Walsh
a012 Brown, K.	a004 Flood	a095 Levenberg	a006 Ramos	a041 Weinstein
a093 Burdick	a057 Forrest	a060 Lucas	a062 Reilly	a024 Weprin
a085 Burgos	a124 Friend	a135 Lunsford	a087 Reyes	a059 Williams
a142 Burke	a050 Gallagher	a123 Lupardo	a149 Rivera	a113 Woerner
a119 Buttenschon	a131 Gallahan	a129 Magnarelli	a067 Rosenthal, L.	a080 Zaccaro
a133 Byrnes	a007 Gandolfo	a101 Maher	a025 Rozic	a096 Zebrowski
a044 Carroll	a068 Gibbs	a036 Mamdani	a111 Santabarbara	a056 Zinerman
a058 Chandler-Waterman	a002 Giglio, J.A.	a130 Manktelow	a090 Sayegh	
	a148 Giglio, J.M.	a108 McDonald	a076 Seawright	
a049 Chang	a066 Glick	a014 McDonough	a084 Septimo	
a136 Clark		a097 McGowan	a092 Shimsky	

1) Single House Bill (introduced and printed separately in either or both houses). Uni-Bill (introduced simultaneously in both houses and printed as one bill. Senate and Assembly introducer sign the same copy of the bill).

2) Circle names of co-sponsors and return to introduction clerk with 2 signed copies of bill and: in Assembly 2 copies of memorandum in support, in Senate 4 copies of memorandum in support (single house); or 4 signed copies of bill and 6 copies of memorandum in support (uni-bill).

LBDC 09/14/23

Section 1. This act shall be known and may be cited as the "Stop Addictive Feeds Exploitation (SAFE) for Kids act".

§ 2. The general business law is amended by adding a new article 45 to read as follows:

ARTICLE 45

SAFE FOR KIDS ACT

§ 1500. Definitions. For the purposes of this article, the following terms shall have the following meanings:

1. "Addictive feed" shall mean a website, online service, online application, or mobile application, or a portion thereof, in which multiple pieces of media generated or shared by users of a website, online service, online application, or mobile application, either concurrently or sequentially, are recommended, selected, or prioritized for display to a user based, in whole or in part, on information associated with the user or the user's device, unless any of the following conditions are met, alone or in combination with one another:

(a) the information is not persistently associated with the user or user's device, and does not concern the user's previous interactions with media generated or shared by others;

(b) the information is user-selected privacy or accessibility settings, technical information concerning the user's device, or device communications or signals concerning whether the user is a minor;

(c) the user expressly and unambiguously requested the specific media or media by the author, creator, or poster of the media, provided that the media is not recommended, selected, or prioritized for display based, in whole or in part, on other information associated with the user or the user's device that is not otherwise permissible under this subdivision;

(d) the media are direct, private communications; or

(e) the media recommended, selected, or prioritized for display is exclusively the next media in a pre-existing sequence from the same author, creator, poster, or source.

2. "Addictive social media platform" shall mean a website, online service, online application, or mobile application, that offers or provides users an addictive feed that is not incidental to the provision of such website, online service, online application, or mobile application.

3. "Covered minor" shall mean a user of a website, online service, online application, or mobile application in New York when the operator has actual knowledge the user is a minor.

4. "Covered user" shall mean a user of a website, online service, online application, or mobile application in New York.

5. "Media" shall mean text, an image, or a video.

6. "Minor" shall mean an individual under the age of eighteen.

7. "Operator" shall mean any person who operates or provides a website on the internet, an online service, an online application, or a mobile application.

8. "Parent" shall mean parent or legal guardian.

9. "User" shall mean a person not acting as an agent of an operator.

§ 1501. Prohibition of addictive feeds. 1. It shall be unlawful for the operator of an addictive social media platform to provide an addictive feed to a covered user unless:

(a) the operator has used commercially reasonable methods to determine that the covered user is not a covered minor; or

(b) the operator has obtained verifiable parental consent to provide an addictive feed to the covered user.

2. Information collected for the purpose of determining a covered user's age under paragraph (a) of subdivision one of this section shall not be used for any purpose other than age determination.

3. Nothing in this section shall be construed as requiring the operator of an addictive social media platform to give a parent who grants verifiable parental consent any additional or special access to or control over the data or accounts of their child.

4. Nothing in this section shall be construed as preventing any action taken in good faith to restrict access to or availability of media that the operator of an addictive social media platform considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.

§ 1502. Time controls. 1. It shall be unlawful for the operator of an addictive social media platform to, between the hours of 12 AM Eastern and 6 AM Eastern, send notifications concerning an addictive social media platform to a covered minor unless the operator has obtained verifiable parental consent to send such nighttime notifications.

2. The operator of an addictive social media platform shall provide a mechanism through which the verified parent of a covered minor may:

(a) prevent their child from accessing the addictive social media platform between the hours of 12 AM Eastern and 6 AM Eastern; and

(b) limit their child's access to the addictive social media platform to a length of time per day specified by the verified parent.

3. Nothing in this section shall be construed as requiring the operator of an addictive social media platform to give a parent any additional or special access to or control over the data or accounts of their child.

§ 1503. Age flags. For the purposes of this article, the operator of an addictive social medial platform shall treat a user as a minor if the user's device communicates or signals that the user is or shall be treated as a minor, including through a browser plug-in or privacy setting, device setting, or other mechanism.

§ 1504. Nondiscrimination. An operator of an addictive social media platform shall not withhold, degrade, lower the quality, or increase the price of any product, service, or feature, other than as required by this article, to a covered user due to the operator not being permitted to provide an addictive feed to such covered user under subdivision one of section fifteen hundred one of this article or not being permitted to provide such covered user access to or send notifications concerning an addictive social media platform between the hours of 12 AM Eastern and 6 AM Eastern under section fifteen hundred two of this article.

§ 1505. Rulemaking authority. The attorney general may promulgate such rules and regulations as are necessary to effectuate and enforce the provisions of this article.

§ 1506. Scope. 1. This article shall apply to conduct that occurs in whole or in part in New York. For purposes of this article, conduct takes place wholly outside of New York if the addictive social media platform is accessed by a user who is physically located outside of New York.

2. Nothing in this article shall be construed to impose liability for commercial activities or actions by operators subject to 15 U.S.C. § 6501 that is inconsistent with the treatment of such activities or actions under 15 U.S.C. § 6502.

§ 1507. Remedies. 1. Whenever it appears to the attorney general, either upon complaint or otherwise, that any person, within or outside the state, has engaged in or is about to engage in any of the acts or practices stated to be unlawful in this article, the attorney general may bring an action or special proceeding in the name and on behalf of the people of the state of New York to enjoin any violation of this article, to obtain restitution of any moneys or property obtained directly or indirectly by any such violation, to obtain disgorgement of any profits or gains obtained directly or indirectly by any such violation, including but not limited to the destruction of unlawfully obtained data and algorithms trained on such data, to obtain damages caused directly or indirectly by any such violation, to obtain civil penalties of up to five thousand dollars per violation, and to obtain any such other and further relief as the court may deem proper, including preliminary relief.

2. Any covered user, or the parent of a covered minor may bring an action for a violation of section fifteen hundred one or section fifteen hundred two of this article, to obtain:

(a) damages of up to five thousand dollars per covered user per incident or actual damages, whichever is greater;

(b) injunctive or declaratory relief; and/or

(c) any other relief the court deems proper.

3. Actions brought pursuant to this section may be brought on a class-wide basis.

4. The court shall award reasonable attorneys' fees to a prevailing plaintiff.

5. Prior to bringing any action for a violation of section fifteen hundred one or fifteen hundred two of this article, a covered user shall provide the business thirty days' written notice identifying the specific provisions of this article the covered user alleges have been or are being violated. In the event a cure is possible, if within the thirty days the business cures the noticed violation and provides the covered user an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this article. If a business continues to violate this article in breach of an express written statement provided to the covered user pursuant to this section, the covered user may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the article that postdates the written statement.

§ 3. Severability. If any clause, sentence, paragraph, subdivision, section or part of this act shall be adjudged by any court of competent

jurisdiction to be invalid, such judgment shall not affect, impair, or invalidate the remainder thereof, but shall be confined in its operation to the clause, sentence, paragraph, subdivision, section or part thereof directly involved in the controversy in which such judgment shall have been rendered. It is hereby declared to be the intent of the legislature that this act would have been enacted even if such invalid provisions had not been included herein.

§ 4. This act shall take effect on the one hundred eightieth day after the office of the attorney general shall promulgate rules and regulations necessary to effectuate the provisions of this act; provided that the office of the attorney general shall notify the legislative bill drafting commission upon the occurrence of the enactment of the rules and regulations necessary to effectuate and enforce the provisions of section two of this act in order that the commission may maintain an accurate and timely effective data base of the official text of the laws of the state of New York in furtherance of effectuating the provisions of section 44 of the legislative law and section 70-b of the public officers law. Effective immediately, the addition, amendment and/or repeal of any rule or regulation necessary for the implementation of this act on its effective date are authorized to be made and completed on or before such effective date.

Legislative Bill Drafting Commission
13150-04-3

S. --------
Senate

IN SENATE--Introduced by Sen

--read twice and ordered printed, and when printed to be committed to the Committee on

-------- A.
Assembly

IN ASSEMBLY--Introduced by M. of A.

with M. of A. as co-sponsors

--read once and referred to the Committee on

GENEBULA
(Establishes the New York child data protection act)

Gen Bus L. child data protection

AN ACT

to amend the general business law, in relation to establishing the New York child data protection act

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

IN SENATE

Senate introducer's signature

The senators whose names are circled below wish to join me in the sponsorship of this proposal:

s15 Addabbo	s34 Fernandez	s28 Krueger	s01 Palumbo	s42 Skoufis
s43 Ashby	s60 Gallivan	s24 Lanza	s21 Parker	s11 Stavisky
s36 Bailey	s12 Gianaris	s16 Liu	s19 Persaud	s45 Stec
s57 Borrello	s59 Gonzalez	s50 Mannion	s13 Ramos	s35 Stewart-Cousins
s46 Breslin	s26 Gounardes	s04 Martinez	s05 Rhoads	
s25 Brisport	s53 Griffo	s07 Martins	s33 Rivera	s44 Tedisco
s55 Brouk	s40 Harckham	s02 Mattera	s39 Rolison	s06 Thomas
s09 Canzoneri-Fitzpatrick	s54 Helming	s48 May	s61 Ryan	s49 Walczyk
	s41 Hinchey	s37 Mayer	s18 Salazar	s52 Webb
s17 Chu	s47 Hoylman-Sigal	s03 Murray	s10 Sanders	s38 Weber
s30 Cleare		s20 Myrie	s23 Scarcella-Spanton	s08 Weik
s14 Comrie	s31 Jackson	s51 Oberacker		
s56 Cooney	s27 Kavanagh	s58 O'Mara	s32 Sepulveda	
s22 Felder	s63 Kennedy	s62 Ortt	s29 Serrano	

IN ASSEMBLY

Assembly introducer's signature

The Members of the Assembly whose names are circled below wish to join me in the multi-sponsorship of this proposal:

a078 Alvarez	a047 Colton	a034 Gonzalez-Rojas	a146 McMahon	a103 Shrestha
a031 Anderson	a140 Conrad		a137 Meeks	a016 Sillitti
a121 Angelino	a032 Cook	a150 Goodell	a017 Mikulin	a052 Simon
a037 Ardila	a039 Cruz	a116 Gray	a122 Miller	a075 Simone
a035 Aubry	a043 Cunningham	a100 Gunther	a051 Mitaynes	a114 Simpson
a120 Barclay	a021 Curran	a139 Hawley	a145 Morinello	a094 Slater
a106 Barrett	a018 Darling	a083 Heastie	a144 Norris	a005 Smith
a105 Beephan	a053 Davila	a028 Hevesi	a045 Novakhov	a118 Smullen
a107 Bendett	a072 De Los Santos	a128 Hunter	a069 O'Donnell	a022 Solages
a082 Benedetto	a003 DeStefano	a029 Hyndman	a091 Otis	a110 Steck
a027 Berger	a070 Dickens	a079 Jackson	a132 Palmesano	a010 Stern
a042 Bichotte Hermelyn	a054 Dilan	a104 Jacobson	a088 Paulin	a127 Stirpe
	a081 Dinowitz	a011 Jean-Pierre	a141 Peoples-Stokes	a102 Tague
a117 Blankenbush	a147 DiPietro	a134 Jensen		a064 Tannousis
a015 Blumencranz	a009 Durso	a115 Jones	a023 Pheffer Amato	a086 Tapia
a073 Bores	a099 Eachus	a077 Joyner		a071 Taylor
a098 Brabenec	a048 Eichenstein	a125 Kelles	a063 Pirozzolo	a001 Thiele
a026 Braunstein	a074 Epstein	a040 Kim	a089 Pretlow	a033 Vanel
a138 Bronson	a109 Fahy	a013 Lavine	a019 Ra	a055 Walker
a046 Brook-Krasny	a061 Fall	a065 Lee	a030 Raga	a143 Wallace
a020 Brown, E.	a008 Fitzpatrick	a126 Lemondes	a038 Rajkumar	a112 Walsh
a012 Brown, K.	a004 Flood	a095 Levenberg	a006 Ramos	a041 Weinstein
a093 Burdick	a057 Forrest	a060 Lucas	a062 Reilly	a024 Weprin
a085 Burgos	a124 Friend	a135 Lunsford	a087 Reyes	a059 Williams
a142 Burke	a050 Gallagher	a123 Lupardo	a149 Rivera	a113 Woerner
a119 Buttenschon	a131 Gallahan	a129 Magnarelli	a067 Rosenthal, L.	a080 Zaccaro
a133 Byrnes	a007 Gandolfo	a101 Maher	a025 Rozic	a096 Zebrowski
a044 Carroll	a068 Gibbs	a036 Mamdani	a111 Santabarbara	a056 Zinerman
a058 Chandler-Waterman	a002 Giglio, J.A.	a130 Manktelow	a090 Sayegh	
	a148 Giglio, J.M.	a108 McDonald	a076 Seawright	
a049 Chang	a066 Glick	a014 McDonough	a084 Septimo	
a136 Clark		a097 McGowan	a092 Shimsky	

1) Single House Bill (introduced and printed separately in either or both houses). Uni-Bill (introduced simultaneously in both houses and printed as one bill. Senate and Assembly introducer sign the same copy of the bill).

2) Circle names of co-sponsors and return to introduction clerk with 2 signed copies of bill and: in Assembly 2 copies of memorandum in support, in Senate 4 copies of memorandum in support (single house); or 4 signed copies of bill and 6 copies of memorandum in support (uni-bill).

LBDC 09/14/23

Section 1. The general business law is amended by adding a new article 39-FF to read as follows:

ARTICLE 39-FF

NEW YORK CHILD DATA PROTECTION ACT

§ 899-ee. Definitions. For purposes of this article, the following terms shall have the following meanings:

1. "Covered user" shall mean a user of a website, online service, online application, mobile application, or connected device, or portion thereof, in the state of New York who is:

(a) actually known by the operator of such website, online service, online application, mobile application, or connected device to be a minor; or

(b) a user of a website, online service, online application, mobile application, or connected device primarily directed to minors.

2. "Minor" shall mean a natural person under the age of eighteen.

3. "Operator" shall mean any person:

(a) who operates or provides a website on the internet, online service, online application, mobile application, or connected device; and

(b) who:

(i) collects or maintains, either directly or through another person, personal data from or about the users of such website, service, application, or connected device;

(ii) integrates with another website, service, application, or connected device and directly collects personal data from the users of such website, service, application, or connected device;

(iii) allows another person to collect personal data directly from users of such website, service, application, or connected device; or

(iv) allows users of such website, service, application, or connected device to publicly disclose personal data.

4. "Personal data" shall mean any data that identifies or could reasonably be linked, directly or indirectly, with a specific natural person or device.

5. "Process" or "processing" shall mean an operation or set of operations performed on personal data, including but not limited to the collection, use, access, sharing, sale, monetization, analysis, retention, creation, generation, derivation, recording, organization, structuring, storage, disclosure, transmission, disposal, licensing, destruction, deletion, modification, or deidentification of personal data.

6. "Primarily directed to minors" shall mean a website, online service, online application, mobile application, or connected device, or a portion thereof, that is targeted to minors. A website, online service, online application, mobile application, or connected device, or portion thereof, shall not be deemed directed primarily to minors solely because such website, online service, online application, mobile application, or connected device, or portion thereof refers or links to any

other website, online service, online application, mobile application, or connected device directed to minors by using information location tools, including a directory, index, reference, pointer, or hypertext link. A website, online service, online application, mobile application, or connected device, or portion thereof, shall be deemed directed to minors when it has actual knowledge that it is collecting personal data of users directly from users of another website, online service, online application, mobile application, or connected device primarily directed to minors.

7. "Sell" shall mean to share personal data for monetary or other valuable consideration. "Selling" shall not include the sharing of personal data for monetary or other valuable consideration to another person as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which that person assumes control of all or part of the operator's assets.

8. "Third party" shall mean any person who is not any of the following:

(a) the operator with whom the user intentionally interacts and who collects personal data from the user as part of the user's current interaction with the operator;

(b) the user whose personal data the operator processes; or

(c) the parent or legal guardian of a user under thirteen years old whose personal data the operator processes.

§ 899-ff. Privacy protection by default. 1. Except as provided for in subdivision six of this section and section eight hundred ninety-nine-jj of this article, an operator shall not process, or allow a third party to process, the personal data of a covered user collected through the

use of a website, online service, online application, mobile application, or connected device unless and to the extent:

(a) the covered user is twelve years of age or younger and processing is permitted under 15 U.S.C. § 6502 and its implementing regulations; or

(b) the covered user is thirteen years of age or older and processing is strictly necessary for an activity set forth in subdivision two of this section, or informed consent has been obtained as set forth in subdivision three of this section.

2. For the purposes of paragraph (b) of subdivision one of this section, the processing of personal data of a covered user is permissible where it is strictly necessary for the following activities:

(a) providing or maintaining a specific product or service requested by the covered user;

(b) conducting the operator's internal business operations. For purposes of this paragraph, such internal business operations shall not include any activities related to marketing, advertising, or providing products or services to third parties, or prompting covered users to use the website, online service, online application, mobile application, or connected device when it is not in use;

(c) identifying and repairing technical errors that impair existing or intended functionality;

(d) protecting against malicious, fraudulent, or illegal activity;

(e) investigating, establishing, exercising, preparing for, or defending legal claims;

(f) complying with federal, state, or local laws, rules, or regulations;

(g) complying with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(h) detecting, responding to, or preventing security incidents or threats; or

(i) protecting the vital interests of a natural person.

3. (a) For the purposes of paragraph (b) of subdivision one of this section, to process personal data of a covered user where such processing is not strictly necessary under subdivision two of this section, informed consent must be obtained from the covered user either through a device communication or signal pursuant to the provisions of subdivision two of section eight hundred ninety-nine-ii of this article or through a request. Requests for such informed consent shall:

(i) be made separately from any other transaction or part of a transaction;

(ii) be made in the absence of any mechanism that has the purpose or substantial effect of obscuring, subverting, or impairing a covered user's decision-making regarding authorization for the processing;

(iii) if requesting informed consent for multiple types of processing, allow the covered user to provide or withhold consent separately for each type of processing;

(iv) clearly and conspicuously state that the processing is optional, and that the covered user may decline without preventing continued use of the website, online service, online application, mobile application, or connected device; and

(v) clearly present an option to refuse to provide consent as the most prominent option.

(b) Such informed consent, once given, shall be freely revocable at any time, and shall be at least as easy to revoke as it was to provide.

(c) If a covered user declines to provide or revokes informed consent for processing, another request may not be made for such processing for the following calendar year.

(d) If a covered user's device communicates or signals that the covered user declines to provide informed consent for processing pursuant to the provisions of subdivision two of section eight hundred ninety-nine-ii of this article, an operator shall not request informed consent for such processing.

4. Except where processing is strictly necessary to provide a product, service, or feature, an operator may not withhold, degrade, lower the quality, or increase the price of any product, service, or feature to a covered user due to the operator not obtaining verifiable parental consent under 15 U.S.C. § 6502 and its implementing regulations or informed consent under subdivision three of this section.

5. Except as provided for in section eight hundred ninety-nine-jj of this article, an operator shall not purchase or sell, or allow a third party to purchase or sell, the personal data of a covered user.

6. Within fourteen days of determining that a user is a covered user, an operator shall:

(a) dispose of, destroy, or delete all personal data of such covered user that it maintains, unless processing such personal data is permitted under 15 U.S.C. § 6502 and its implementing regulations, is strictly necessary for an activity listed in subdivision two of this section, or informed consent is obtained as set forth in subdivision three of this section; and

(b) notify any third parties to whom it disclosed the personal data, and any third parties it allowed to process the personal data, that the user is a covered user.

§ 899-gg. Third parties. 1. Except as provided for in section eight hundred ninety-nine-jj of this article, no operator shall disclose the personal data of a covered user to a third party, or allow the processing of the personal data of a covered user by a third party, without a written, binding agreement governing such disclosure or processing. Such agreement shall clearly set forth instructions for the nature and purpose of the third-party's processing of the personal data, instructions for using or further disclosing the personal data, and the rights and obligations of both parties.

2. Except as provided for in section eight hundred ninety-nine-jj of this article, prior to disclosing personal data to a third party, the operator shall inform the third party if such data is the personal data of a covered user.

3. An agreement pursuant to subdivision one of this section shall require that the third party:

(a) process the personal data of covered users only when and to the extent strictly necessary for an activity listed pursuant to subdivision two of section eight hundred ninety-nine-ff of this article, or where informed consent was obtained pursuant to subdivision three of section eight hundred ninety-nine-ff of this article;

(b) delete or return to the operator all personal data of covered users at the end of its provision of services, unless retention of the personal data is required by law;

(c) upon reasonable request of the operator, make available to the operator all data in its possession necessary to demonstrate the third-party's compliance with the obligations in this section;

(d) allow, and cooperate with, reasonable assessments by the operator or the operator's designated assessor for purposes of evaluating compliance with the obligations of this article. Alternatively, the third party may arrange for a qualified and independent assessor to conduct an assessment of the third-party's policies and technical and organizational measures in support of the obligations under this article using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The third party shall provide a report of such assessment to the operator upon request; and

(e) notify the operator a reasonable time in advance before disclosing or transferring the personal data of covered users to any further third parties, which may be in the form of a regularly updated list of further third parties that may access personal data of covered users.

§ 899-hh. Ongoing safeguards. Upon learning that a user is no longer a covered user, an operator may not process the personal data of such person in a manner not previously permitted unless and until it receives informed consent pursuant to subdivision three of section eight hundred ninety-nine-ff of this article.

§ 899-ii. Respecting user-provided age flags. 1. For the purposes of this article, an operator shall treat a user as a covered user if the user's device communicates or signals that the user is or shall be treated as a minor, including through a browser plug-in or privacy setting, device setting, or other mechanism.

2. For the purposes of subdivision three of section eight hundred ninety-nine-ff of this article, an operator shall adhere to any clear

and unambiguous communications or signals from a covered user's device, including through a browser plug-in or privacy setting, device setting, or other mechanism, concerning processing that the covered user consents to or declines to consent to. An operator shall not adhere to unclear or ambiguous communications or signals from a covered user's device, and shall instead request informed consent pursuant to the provisions of paragraph a of subdivision three of section eight hundred ninety-nine-ff of this article.

§ 899-jj. Protections for third-party operators. Sections eight hundred ninety-nine-ff and eight hundred ninety-nine-gg of this article shall not apply to an operator processing the personal data of a covered user of another website, online service, online application, mobile application, or connected device, or portion thereof, where the operator received reasonable written representations that the covered user provided informed consent for such processing, or:

1. the operator does not have actual knowledge that the covered user is a minor; and

2. the operator does not have actual knowledge that the other website, online service, online application, mobile application, or connected device, or portion thereof, is primarily directed to minors.

§ 899-kk. Rulemaking authority. The attorney general may promulgate such rules and regulations as are necessary to effectuate and enforce the provisions of this article.

§ 899-ll. Scope. 1. This article shall apply to conduct that occurs in whole or in part in the state of New York. For purposes of this article, commercial conduct takes place wholly outside of the state of New York if the business collected such information while the covered user was outside of the state of New York, no part of the use of the covered

user's personal data occurred in the state of New York, and no personal data collected while the covered user was in the state of New York is used.

2. Nothing in this article shall be construed to prohibit an operator from storing a covered user's personal data that was collected pursuant to section eight hundred ninety-nine-ff of this article when such covered user is in the state.

3. Nothing in this article shall be construed to impose liability for commercial activities or actions by operators subject to 15 U.S.C. 6501 that is inconsistent with the treatment of such activities or actions under 15 U.S.C. 6502.

§ 899-mm. Remedies. 1. Whenever it appears to the attorney general, either upon complaint or otherwise, that any person, within or outside the state, has engaged in or is about to engage in any of the acts or practices stated to be unlawful in this article, the attorney general may bring an action or special proceeding in the name and on behalf of the people of the state of New York to enjoin any violation of this article, to obtain restitution of any moneys or property obtained directly or indirectly by any such violation, to obtain disgorgement of any profits or gains obtained directly or indirectly by any such violation, including but not limited to the destruction of unlawfully obtained data and algorithms trained on such data, to obtain damages caused directly or indirectly by any such violation, to obtain civil penalties of up to five thousand dollars per violation, and to obtain any such other and further relief as the court may deem proper, including preliminary relief.

2. Any covered user who has been injured by a violation of section eight hundred ninety-nine-ff of this article, or the parent or legal

guardian of a covered minor who has been injured by a violation of section eight hundred ninety-nine-ff of this article, may bring an action to obtain:

(a) Damages of up to five thousand dollars per covered user per incident or actual damages, whichever is greater;

(b) Injunctive or declaratory relief; and/or

(c) Any other relief the court deems proper.

3. Actions pursuant to this section may be brought on a class-wide basis.

4. The court may award reasonable attorneys' fees to a prevailing plaintiff.

5. Prior to bringing any action for violations of this article pursuant to subdivision two of this section, a covered user shall provide the operator thirty days' written notice identifying the specific provisions of this article the covered user alleges have been or are being violated. In the event a cure is possible, if within the thirty days the operator actually cures the noticed violation and provides the covered user an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the operator. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this article in breach of the express written statement provided to the covered user under this section, the covered user may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the

express written statement, as well as any other violation of the article that postdates such written statement.

§ 2. Severability. If any clause, sentence, paragraph, subdivision, section or part of this act shall be adjudged by any court of competent jurisdiction to be invalid, such judgment shall not affect, impair, or invalidate the remainder thereof, but shall be confined in its operation to the clause, sentence, paragraph, subdivision, section or part thereof directly involved in the controversy in which such judgment shall have been rendered. It is hereby declared to be the intent of the legislature that this act would have been enacted even if such invalid provisions had not been included herein.

§ 3. This act shall take effect one year after it shall have become a law. Effective immediately, the addition, amendment and/or repeal of any rule or regulation necessary for the implementation of this act on its effective date are authorized to be made and completed on or before such effective date.

October 13, 2023

The Honorable Anne Carney, Chair
The Honorable Matt Moonen, Chair
Joint 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 Chairs Carney and Moonen:

The Financial Industry Regulatory Authority ("FINRA")[1] appreciates the opportunity to provide feedback on LD 1977 / HP 1270 ("the proposal"), which would provide data privacy protections for Maine residents and place certain privacy-related obligations on a wide variety of entities. FINRA generally supports increased privacy protections but seeks an exemption from the bill to allow FINRA to continue protecting Maine investors and overseeing the brokerage industry in Maine.

FINRA's Role in Protecting Maine Investors

FINRA is a not-for-profit regulator of the securities industry that operates under authority granted to it by the Securities Exchange Act of 1934 ("Exchange Act").[2] FINRA is overseen by the Securities and Exchange Commission ("SEC")[3] and works closely with the SEC and the Maine Office of Securities in executing its regulatory responsibilities. FINRA's mission is to protect investors and safeguard market integrity in a manner that facilitates vibrant capital markets. As part of this mission, FINRA examines brokerage firms, examines for and enforces compliance with FINRA rules and federal securities laws and provides information to the investing public. FINRA also works with state securities regulators nationwide to register broker-dealers and their agents and operates the electronic system through which both FINRA and state registrations flow.

FINRA's regulatory work includes oversight of the more than 150,000 persons registered to do business in Maine, and the nearly 600 broker-dealer offices in the state. FINRA also conducts cross-market oversight of trading on the nation's top exchanges and off-exchange venues for securities and options, administers a specialized arbitration forum with a focus on investor protection and administers licensing qualification examinations.[4]

[1] For more information, please visit www.FINRA.org.
[2] *See* Section 15A of the Securities Exchange Act of 1934 (15 U.S.C. Section 78o-3).
[3] SEC oversight is facilitated through the "FINRA and Securities Industry Oversight Examination Program," which conducts examinations of FINRA and the Municipal Securities Rulemaking Board.
[4] FINRA develops and administers qualifying examinations to securities industry professionals, which serve as a prerequisite to FINRA registration. FINRA also administers state law examinations on behalf of the North American Securities Administrators Association ("NASAA"), which Maine uses for state licensing purposes.

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

FINRA data is used for regulatory and transparency purposes only,[5] but due to our work with state securities regulators and our unique regulatory structure, we are concerned that FINRA could unintentionally be impacted by the proposal. If FINRA were to be covered, it would become subject to restrictions that could interfere with its ability to regulate broker-dealers and protect Maine investors.

Regulatory Activities Restricted by the Proposal

The proposal would prohibit an entity from collecting or processing covered data outside of the specific purposes listed in Section 9604-2 of the bill. However, subsection 2 does not contemplate the regulatory activity of a non-governmental regulator acting pursuant to statutory authority. Without such allowances, the proposal could negatively impact FINRA's mandate to protect investors and ensure the integrity of the U.S. capital markets. As you work on this bill, we urge you to consider the following FINRA regulatory activities, which we anticipate would be negatively impacted by the proposal:

- As part of our regulatory oversight work, FINRA often shares information with law enforcement and government regulators – including the SEC and the Maine Office of Securities. Such information could include investor data (including covered data) obtained as part of FINRA's market oversight activities, or our investigations into violations of FINRA rules and federal securities laws. This could also include information related to potential violations of insider trading laws or information on the completion of qualifying examinations for registration with FINRA and the State of Maine.

- FINRA may also collect a variety of investor information, including covered data, as part of an enforcement investigation or action. Such information is critical to finding wrongdoing, as well as ensuring investors receive any restitution ordered in a FINRA enforcement action for compensation of investor loses.[6]

- Similarly, FINRA collects information as part of our cross-market regulatory oversight of the capital markets. FINRA operates a robust regulatory oversight program that processes billions of electronic records per day connected to market events. This is a key component of FINRA's mission to protect investors and ensure market integrity and may involve the collection of data covered by the proposal.

- FINRA administers a securities arbitration forum in the United States to assist in the resolution of disputes involving investors, brokerage firms and their registered employees ("FINRA Arbitration Forum").[7] All rules related to the FINRA Arbitration Forum have been filed

[5] FINRA is also subject to SEC's Regulation Systems Compliance and Integrity ("Reg SCI"), which regulates the technology infrastructure and security of FINRA and other critical portions of the securities industry. (17 CFR Section 242.1000.)

[6] In 2022, FINRA secured roughly $26 million in restitution for investors across the country.

[7] During the past 10 years alone, the FINRA Arbitration Forum has helped resolve over 41,000 intra-industry and customer disputes through arbitration. One advantage of having a forum run by the industry's regulator is that FINRA has the ability to support enforcement of awards against firms by suspending or cancelling a firm's or salesperson's license for failure to pay

> with and reviewed by the SEC and include important investor protection safeguards. Because the forum deals with investors acting in their individual capacities, much of the information related to arbitration cases could be subject to the proposal, which could create significant operational challenges or conflict with the forum's SEC-approved rules.

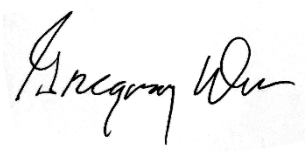
These are just a few examples of the important FINRA regulatory activities that could be impacted by the proposed restrictions. For these reasons, we respectfully request that you consider including the below language in the bill. This language is substantially similar to laws enacted in other states that provide data privacy protections to state residents while allowing FINRA to continue to protect investors and oversee broker-dealers.

We respectfully request that you add the following language to Section 9603-1:

> "For the purposes of this Act, "government agencies" includes a national securities association registered pursuant to § 15A of the Securities Exchange Act of 1934 (15 U.S.C. § 78a, et seq., as amended) and the rules and implementing regulations promulgated thereunder, or a registered futures association so designated pursuant to § 17 of the Commodity Exchange Act (7 U.S.C. § 1, et seq., as amended) and the rules and implementing regulations promulgated thereunder."

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

Sincerely,



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

CC: The Honorable Margaret O'Neil

---

arbitration awards or agreed-upon settlements. More information regarding the FINRA Arbitration Forum is available at http://www.finra.org/arbitration-and-mediation.

October 26, 2023

Via Electronic Submission
Senator Anne Carney, Chair
Representative Matthew Moonen, Chair
Members of the Judiciary Committee
Maine State Legislature
Augusta, ME 04333

RE: Additional Testimony for Consideration following the Judiciary Committee's Hearing on LD 1977 (Data Privacy) & Work Session held on October 17, 2023

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

The National Retail Federation appreciates your consideration of our views in your efforts to develop statewide privacy legislation, the subject of the Judiciary Committee's public hearing on LD 1977 and work session held on October 17, 2023. I participated in both and was invited to testify via Zoom in light of my subject matter expertise on federal and state privacy legislation in the United States. In follow up to my oral testimony last week, and after consultation with our members and other stakeholders in the retail industry, I am submitting to the Committee some additional observations to both support and augment my remarks made during the legislative hearing on LD 1977 and the work session that immediately followed it.

NRF, the world's largest retail trade association, passionately advocates for the people, brands, policies and ideas that help retail succeed. NRF empowers the industry that powers the economy. Retail is the nation's largest private-sector employer, contributing $3.9 trillion to annual GDP and supporting one in four U.S. jobs — 52 million working Americans. For over a century, NRF has been a voice for every retailer and every retail job, educating, inspiring and communicating the powerful impact retail has on local communities and global economies.

NRF believes federal privacy legislation is necessary to establish uniform, national standards that protect all Americans' personal data wherever it is collected and used, regardless of the state where a consumer resides or a business is located. Until Congress enacts preemptive federal privacy legislation, we have been supporting and will continue to support adoption of consistent data privacy laws by states to ensure the level of consumer protection and enforcement of these laws are substantially equivalent for consumers and businesses across the United States.

We believe it is critically important for the American economy and free-flowing interstate commerce that states model any new comprehensive privacy laws on the workable and non-controversial privacy frameworks successfully established by other states and implemented by covered businesses in recent years. This will help maintain substantially similar privacy laws across the United States that protect consumers' data comprehensively, do not overly burden interstate commerce, and ensure that legitimate businesses may continue to use that data to serve their customers in ways that they now expect. To this end, we have worked with and supported

NATIONAL RETAIL FEDERATION
1101 New York Avenue, NW, Suite 1200
Washington, DC 20005
www.nrf.com

our partners at state retail associations, including the Retail Association of Maine, to provide substantive policy expertise and additional support in this complex area of law and legislation.

With respect to the development of a comprehensive privacy law for Maine (including LD 1973 and LD 1977, which are bills that propose to cover all personal data and are not limited to covering only biometric information and/or consumer health data), my additional observations provided below are limited to just two of the issues discussed by other witnesses and in my personal testimony during last week's hearing and follow-on work session: 1) private rights of action; and 2) customer loyalty programs. *(While not offered here, NRF may offer comments on other issues in proposed privacy legislation for Maine in future or supplemental testimony.)*

Private Rights of Action

Setting aside certain specialized data privacy bills that do not cover all consumer data generally but are narrowly focused on biometric information and/or consumer health data (where two states have authorized private rights of action that remain controversial provisions there), it is important to reiterate that no state's enacted comprehensive privacy law has authorized private rights of action to enforce the privacy provisions of that law. Notably, California limited the private right of action in the California Consumer Privacy Act (CCPA) to apply only to the CCPA's data security provisions, so they are not used to enforce the CCPA's privacy provisions.

In lieu of relying on private rights of action, states that enacted *comprehensive* privacy laws instead adopted exclusive attorney general (AG) and/or government agency enforcement, typically coupled with notice-and-cure rights for alleged violations as further described below. The principal reason for this is that many of the obligations to protect personal data are subject to complex rules and subjective standards. Most privacy laws, for instance, use standards of "reasonability" when setting the level of protection businesses should apply to personal data based on a range of factors from the sensitivity of the data to its intended use or sharing.

Naturally, because legislatures cannot predetermine every data-use case across a broad range of industry sectors and precisely calibrate a one-size-fits-all law to cover all potential uses, most states have found an effective way to ensure the greatest compliance with their laws is to encourage robust dialogue between covered businesses handling customer data and an exclusive state enforcement authority, such as the AG or a state privacy agency. For that reason, nearly all comprehensive state privacy laws couple the AG enforcement provision with a notice-and-cure period in which businesses have the ability to work with the AG for 30 or 60 days after being notified of any potential non-compliance with the law to explain, correct, or "cure" any data practices to the satisfaction of the AG in order to avoid legal enforcement proceedings. This approach is valuable in addressing innovative data use cases lawmakers could not anticipate.

This enforcement model, which is the national standard for comprehensive state privacy laws that contain complex rules and subjective standards, helps achieve the state legislature's primary goal of driving robust data privacy law compliance across the greatest range of businesses in order to comprehensively protect state residents from data privacy violations. This model also avoids unintentionally subjecting covered businesses to "gotcha" rules alleged to apply to data in ways never intended, and where avoiding litigation may be impossible despite a legitimate business's best efforts to comply with a complicated law with subjective standards.

For these and additional reasons, *every* state that has successfully enacted *comprehensive* privacy legislation – laws covering all personal data collected and processed by covered entities – has considered and rejected private rights of action to enforce their law's privacy provisions.

Customer Loyalty Programs

A critically important area where one of the proposed privacy bills you are reviewing, LD 1977, proposes a rule that would be a significant outlier among all state privacy laws is in its potential regulation of customer loyalty plans. Retailers believe Maine consumers have the capacity to make intelligent and informed decisions about whether to voluntarily participate in customer loyalty programs offered by trusted companies with whom they do business. These programs include retail loyalty plans under which customers receive discounts and other benefits they want. Sometimes providing a benefit requires the retailer to share customer data with business partners in other industry sectors, such as gas stations who provide discounts on the price per gallon of gas once partnered grocery store customers reach certain levels of purchases.

Offering benefits like these to customers from valued business partners does not make a retailer a "data broker." Unlike the situation with data brokers, retail customers know who they are providing their personal information to – the retailer with whom they are shopping – and they voluntarily participate in these programs – that is, they opt into them after determining whether or not they'd like to participate in the plan to receive the offered benefits from that retailer or their business partners. By contrast, data brokers are unknown to consumers, and they collect and share consumer data often without providing consumers either notice or choice.

It is important to note that some text in LD 1977's section 9607 subsection 3.B. (starting on p. 9, line 27) is consistent with other state privacy laws' provisions that require participation in qualifying loyalty plans to be "voluntary." We support this requirement of voluntariness as it provides a higher level of protection (an opt-in), meaning that a consumer who takes no action to join would not be part of a loyalty program covered by this section's savings clause language. Furthermore, this requirement has teeth and provides a powerful incentive to offer loyalty plans *only* on an opt-in basis, because a plan that does not require participants to opt in could be found to violate the bill's prohibition on discriminating against consumers exercising privacy rights.[1]

Although we have supported similar voluntariness language in all other state privacy laws, LD 1977 is an outlier due to the *additional* language that appears in subsection 3.B. after the standard language noted above. This additional text, found in prongs (1)-(3) (on p. 9, lines 33-39), is legislative language that does not exist in any other state privacy law nor in federal proposals, and here's why. After the standard opt-in requirement above, the text of (1)-(3) is unnecessary to protect consumers and would only serve to overly restrict customer loyalty plan operations in ways that no other state privacy law does now and no federal privacy bill proposes.

[1] Subsection 3 of Section 9607 of LD 1977 interprets the meaning of the bill's prohibition on retaliation against consumers who exercise a privacy right, including *"charging different prices or rates for goods or services or providing a different level of quality of goods or services."* Because this text could inadvertently treat all customer loyalty programs as *de facto* violations of the law for providing some customers better prices or levels of service than those exercising privacy rights who do not participate in these programs, the subsection correctly includes a savings clause intended to preserve the operation of bona fide customer loyalty plans offered by retailers and other businesses to customers who voluntarily opt in to participate in them.

For comparative purposes it is also highly relevant that LD 1977's opt-in for data transfers of sensitive data to third parties, found in section 9605 subsection 3.A. (on p. 7 line 38), does not have *any* additional restrictions like those in prongs (1)-(3). This raises the public policy question as to why the bill would regulate popular customer loyalty plans that consumers already opt into more severely than transfers to third parties of consumers' most sensitive information.

We believe Maine should avoid enacting novel customer loyalty plan regulations that jeopardize the continued availability of popular loyalty plan benefits to Mainers, especially from programs that would continue to offer those benefits in nearby states. As explained in my oral testimony last week, Connecticut considered and rejected the same *additional* language before enacting its comprehensive privacy law containing the standard loyalty savings text that retail and other sectors fully supported. If Maine were to now adopt the outlier *additional* regulation that Connecticut and other states rejected, it will create disparities in the regulation of loyalty plans within New England that hurts Maine retailers, Maine consumers, and Maine's economy.

In conclusion, we support the old retail adage that the "customer is always right." By extension, we also believe that Maine consumers expect the public policy and laws of the state to preserve their current rights to choose whether to receive benefits offered in customer loyalty programs from trusted businesses that they decide to voluntarily join. For this reason, we ask you to reject the *additional* language regulating customer loyalty plans in LD 1977 that is an outlier among all enacted state privacy laws.

Thank you for your consideration of our views, and we appreciate the opportunity to continue participating in future work sessions to address these and other areas of interest to retailers in proposed privacy legislation. We also look forward to working with you and your staff to help develop a comprehensive, workable, and effective privacy law for Maine.

Sincerely,

Paul Martino
Vice President & Senior Policy Counsel

Paul Martino
National Retail Federation
LD 1977

Please see attached supplemental testimony in support of the oral testimony provided via Zoom by Paul Martino, Vice President & Senior Policy Counsel for the National Retail Federation, during the public hearing on LD 1799 and follow-on work session held on October 17, 2023.

November 7, 2023

Senator Anne Carney
Senate Chair of the Joint Standing Committee on Judiciary
21 Angell Point Road
Cape Elizabeth, ME 04107

Representative Matt Moonen
House Chair of the Joint Standing Committee on Judiciary
53 Thomas St., #3
Portland, ME 04102

Representative Margaret O'Neil
21 Sheila Circle
Saco, ME 04072

RE: LD 1977 – Oppose

Dear Senator Carney, Representative Moonen, and Representative O'Neil:

On behalf of the advertising industry, we write to oppose LD 1977, the "Data Privacy and Protection Act."[1] As presently drafted, LD 1977 contains provisions that are significantly out-of-step with privacy laws in other states. The bill's terms are so onerous that they threaten to completely outlaw routine and beneficial data processing practices, such as data processing for legitimate and responsible advertising. Instead of proceeding with the divergent approach represented in LD 1977, we ask the legislature to harmonize its approach with other state privacy laws.

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country. These companies range from small businesses to household brands, long-standing and emerging publishers, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product ("GDP") in 2020.[2] By one estimate, over 20,000 jobs in Maine are related to the ad-subsidized Internet.[3] Below we provide a non-exhaustive list of concerns with LD 1977. We would welcome the opportunity to engage with you further on the issues with the bill and the benefits of data-driven digital advertising we outline here:

- **Maine Should Take Steps to Harmonize its Approach to Privacy with Other State Laws**
- **The Bill Would Ban Commercial Speech in the Form of Targeted Advertising by Prohibiting the Use of the Very Data Needed for that Type of Advertising**
- **The Bill Diverges from Existing Privacy Laws Because It Requires Controllers to Disclose the Names of Specific Third-Party Partners**

[1] Maine LD 1977 (131st Leg., Second Reg. Sess., 2023), located here
[2] John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located here (hereinafter, "Deighton & Kornfeld 2021").
[3] *Id*. at 127.

- **A Private Right of Action Is an Inappropriate Form of Enforcement for Privacy Legislation**
- **The Data-Driven and Ad-Supported Online Ecosystem Benefits Maine Residents and Fuels Economic Growth.**

We and the companies we represent, many of whom do substantial business in Maine, strongly believe consumers deserve meaningful privacy protections supported by reasonable laws and responsible industry policies, which is why we support a national, preemptive standard for data privacy at the federal level. In the absence of such a preemptive federal law, it is imperative for states to work to harmonize privacy standards to provide even protections for consumers and ease costs of operationalizing privacy requirements. Adopting a deviating approach, like that contained in LD 1977, would significantly impede Maine consumers from reaching products and services they rely upon and expect and would decimate the small and mid-size business community in the state.

I. Maine Should Take Steps to Harmonize its Approach to Privacy with Other State Laws

In the current absence of a national standard for data privacy at the federal level, it is critical for legislators to seriously consider the costs to both consumers and businesses that will accrue from a patchwork of differing privacy standards across the states. Harmonization with existing privacy laws is critical to minimizing costs of compliance and fostering similar consumer privacy rights for consumers. One way that LD 1977 presently diverges from existing state privacy laws is that it does not address the concept of pseudonymous data. Most state privacy laws recognize the privacy benefits of "pseudonymous data," which is typically defined to include personal data that cannot be attributed to a specific natural person without the use of additional information. These other laws exempt this data from consumer rights to access, delete, correct, and port personal data, provided that this data is kept separately from information necessary to identify a consumer and is subject to effective technical and organizational controls to prevent the controller from accessing such information. We ask you to amend LD 1977 and harmonize it with other privacy laws to exempt pseudonymous data from consumer rights of access, correction, deletion, and portability.

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

---

[4] *See* State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations*, 11 (Aug. 2019), located here.

[5] *See* Florida Tax Watch, *Who Knows What? An Independent Analysis of the Potential Effects of Consumer Data Privacy Legislation in Florida*, 2 (Oct. 2021), located here.

[6] Daniel Castro, Luke Dascoli, and Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws* (Jan. 24, 2022), located here (finding that small businesses would bear approximately $20-23 billion of the out-of-state cost burden associated with state privacy law compliance annually).

II. The Bill Would Ban Commercial Speech in the Form of Targeted Advertising by Prohibiting the Use of the Very Data Needed for that Type of Advertising

The bill flatly prohibits use of sensitive data for targeted advertising.[7] "Sensitive data" under the bill includes "information identifying an individual's online activities over time and across 3rd party websites or online services," which is the very data that permits targeted advertising to function.[8] By banning use of such data in targeted advertising, the bill would impermissibly burden commercial speech by flatly outlawing targeted advertising entirely, without exceptions.

The bill's proposed ban of targeted advertising is likely unintended, however, because it also attempts to permit targeted advertising and transfers of covered data to third parties upon a consumer's opt in consent to such activity. As discussed in more detail in Section V below, the data-driven and ad-supported online ecosystem is powered by targeted advertising. This ecosystem benefits consumers and fuels economic growth and competition. Companies, nonprofits, and government agencies alike use data to send varying groups of individuals specific, relevant messages through targeted advertising functionalities. Tailored messaging provides immense public benefit by reaching individual consumers with information that is relevant to them in the right time and place. Legal requirements that limit entities' ability to use data responsibly to reach consumers with important and pertinent messaging, such as those set forth in LD 1977's opt-in consent requirements, can have unintended consequences and, ultimately, serve as a detriment to consumers' health and welfare.

Ad-technology systems and processes enable everything from public health messaging to retailer messaging. They allow timely wildfire warnings to reach local communities and facilitate the dissemination of missing children alerts, among a myriad of other beneficial uses with the very same technology and techniques used for targeted advertising.[9] In accordance with responsible data use, uses of data for targeted advertising should be subject to notice requirements and effective opt out controls. Opt-in consent requirements tend to work to the advantage of large, entrenched market players at the expense of smaller businesses and start-up companies. To ensure uses of data to benefit Maine residents can persist, and to help maintain a competitive business marketplace, we ask you amend the bill to: (1) remove "information identifying an individual's online activities over time and across 3rd party websites or online services" from the bill's "sensitive data" definition, and (2) permit consumers to opt out of targeted advertising rather than requiring them to opt in to such activity, an approach that reflects the requirements of a majority of states with privacy laws across the nation.[10]

III. The Bill Diverges from Existing Privacy Laws Because It Requires Controllers to Disclose the Names of Specific Third-Party Partners

Another way LD 1977 diverges from existing state privacy laws is that it would require covered entities and service providers to disclose "the name of each data broker to which the covered entity or service provider transfers covered data" in a privacy policy.[11] In addition, the bill would require covered entities to give consumers the option to obtain the names of third parties or service providers to which covered data was transferred in exchange for consideration in response to an access request.[12] Other state privacy laws require companies to disclose the *categories* of third parties to

---

[7] LD 1977 at § 9605(5).
[8] *Id.* at § 9602(13)(O).
[9] *See* Digital Advertising Alliance, *Summit Snapshot: Data 4 Good – The Ad Council, Federation for Internet Alerts Deploy Data for Vital Public Safety Initiatives* (Sept. 1, 2021), located here.
[10] *See, e.g.*, Cal. Civ. Code § 1798.135; Va. Code Ann. § 57.1-577(A)(5); Colo. Rev. Stat 6-1-1306(1)(a); Conn. Gen. Stat. § 42-518(a)(5); Utah Rev. Stat § 16-61-201(4) (effective Dec. 31, 2023).
[11] LD 1977 at § 9608(1)(D).
[12] *Id.* at § 9611(1)(A)(2)(b).

whom they transfer personal data rather than the specific names of such third parties themselves.[13] Requiring documentation or disclosure of names of entities would be operationally burdensome, as covered entities change business partners frequently, and companies regularly merge with others and change names.

For instance, a covered entity or service provider may engage in a data exchange with a new business-customer on the same day it responds to a consumer disclosure request. This requirement would either force the covered entity to refrain from engaging in commerce with the new business-customer until its privacy policy is updated or risk violating the law. This is an unreasonable restraint. From an operational standpoint, constantly updating a list of all data brokers a covered entity works with would take significant resources and time away from companies' efforts to comply with other new privacy directives in LD 1977. Covered entities and service providers may be forced to jeopardize new business opportunities and relationships just to compile, maintain, update, and distribute these ephemeral lists.

International privacy standards like the European Union's General Data Protection Regulation ("GDPR") also do not require burdensome disclosures of specific third parties in response to data subject access requests, according to the text of the law. Mandating that companies disclose the names of their third-party partners could obligate companies to abridge confidentiality clauses they maintain in their contracts with partners and expose proprietary business information to their competitors. Finally, the consumer benefit that would accrue from their receipt of a list of data brokers to whom a covered entity or service provider discloses data would be minimal at best. The benefit would be especially insignificant given LD 1977 already requires controllers to disclose *categories* of third-party partners in privacy notices for consumers.[14] For these reasons, we encourage you to reconsider this onerous language, which severely diverges from the approach to disclosures taken in existing state privacy laws. To align LD 1977 with other state privacy laws, the bill should require disclosures of the categories of third parties rather than the names of such entities themselves.

IV. A Private Right of Action Is an Inappropriate Form of Enforcement for Privacy Legislation

As presently drafted, LD 1977 allows for private litigants to bring lawsuits.[15] We strongly believe private rights of action should have no place in privacy legislation. Instead, enforcement should be vested with the Maine Attorney General ("AG") alone, because such an enforcement structure would lead to stronger outcomes for Maine residents while better enabling businesses to allocate resources to developing processes, procedures, and plans to facilitate compliance with new data privacy requirements. AG enforcement, instead of a private right of action, is in the best interests of consumers and businesses alike.

The private right of action in LD 1977 will create a complex and flawed compliance system without tangible privacy benefits for consumers. Allowing private actions will flood Maine's courts with frivolous lawsuits driven by opportunistic trial lawyers searching for technical violations, rather than focusing on actual consumer harm.[16] Private right of action provisions are completely divorced

[13] *See, e.g.,* Cal. Civ. Code § 1798.110; Va. Code Ann. § 59.1-578(C); Colo. Rev. Stat. § 6-1-1308(1)(a); Conn. Gen. Stat. § 42-520(c)(5); Utah Rev. Stat § 16-61-302(1)(a) (effective Dec. 31, 2023).
[14] LD 1977 at § 9608(1)(D).
[15] *Id.* at § 9620(2).
[16] A select few attorneys benefit disproportionately from private right of action enforcement mechanisms in a way that dwarfs the benefits that accrue to the consumers who are the basis for the claims. For example, a study of 3,121 private actions under the Telephone Consumer Protection Act ("TCPA") showed that approximately 60 percent of TCPA lawsuits were brought by just forty-four law firms. Amounts paid out to consumers under such lawsuits proved to be insignificant,

from any connection to actual consumer harm and provide consumers little by way of protection from detrimental data practices.

Additionally, a private right of action will have a chilling effect on the state's economy by creating the threat of steep penalties for companies that are good actors but inadvertently fail to conform to technical provisions of law. Private litigant enforcement provisions and related potential penalties for violations represent an overly punitive scheme that do not effectively address consumer privacy concerns or deter undesired business conduct. They expose businesses to extraordinary and potentially enterprise-threatening costs for technical violations of law rather than drive systemic and helpful changes to business practices. A private right of action will also encumber businesses' attempts to innovate by threatening companies with expensive litigation costs, especially if those companies are visionaries striving to develop transformative new technologies. The threat of an expensive lawsuit may force smaller companies to agree to settle claims against them, even if they are convinced they are without merit.[17]

Beyond the staggering cost to Maine businesses, the resulting snarl of litigation could create a chaotic and inconsistent enforcement framework with conflicting requirements based on differing court outcomes. Overall, a private right of action would serve as a windfall to the plaintiff's bar without focusing on the business practices that actually harm consumers. We therefore encourage legislators to remove the private right of action from the bill and replace it with a framework that makes enforcement responsibility the purview of the AG alone.

V. The Data-Driven and Ad-Supported Online Ecosystem Benefits Maine Residents and Fuels Economic Growth

Over the past several decades, data-driven advertising has created a platform for innovation and tremendous growth opportunities. A recent study found that the Internet economy's contribution to the United States' GDP grew 22 percent per year since 2016, in a national economy that grows between two to three percent per year.[18] In 2020 alone, it contributed $2.45 trillion to the U.S.'s $21.18 trillion GDP, which marks an eightfold growth from the Internet's contribution to GDP in 2008 of $300 billion.[19] Additionally, more than 17 million jobs in the U.S. were generated by the commercial Internet in 2020, 7 million more than four years prior.[20] More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest Internet companies, which generated 34 percent.[21] The same study found that the ad-supported Internet supported 21,371 full-time jobs across Maine, more than double the number of Internet-driven jobs from 2016.[22]

---

as only 4 to 8 percent of eligible claim members made themselves available for compensation from the settlement funds. U.S. Chamber Institute for Legal Reform, *TCPA Litigation Sprawl* at 2, 4, 11-15 (Aug. 2017), located here.

[17] For instance, in the early 2000s, private actions under California's Unfair Competition Law ("UCL") "launched an unending attack on businesses all over the state." American Tort Reform Foundation, *State Consumer Protection Laws Unhinged: It's Time to Restore Sanity to the Litigation* at 8 (2003), located here. Consumers brought suits against homebuilders for abbreviating "APR" instead of spelling out "Annual Percentage Rate" in advertisements and sued travel agents for not posting their phone numbers on websites, in addition to initiating myriad other frivolous lawsuits. These lawsuits disproportionately impacted small businesses, ultimately resulting in citizens voting to pass Proposition 64 in 2004 to stem the abuse of the state's broad private right of action under the UCL. *Id.*

[18] Deighton & Kornfeld 2021 at 5.

[19] *Id*.

[20] *Id*.

[21] *Id*. at 6.

[22] *Compare id.* at 127 (Oct. 18, 2021) *with* John Deighton, Leora Kornfeld, and Marlon Gerra, *Economic Value of the Advertising-Supported Internet Ecosystem,* INTERACTIVE ADVERTISING BUREAU, 106 (2017), located here (finding that Internet employment contributed 9,850 full-time jobs to the Maine workforce in 2016 and 21,371 jobs in 2020).

A. Advertising Fuels Economic Growth

Data-driven advertising supports a competitive online marketplace and contributes to tremendous economic growth. Overly restrictive legislation that significantly hinders certain advertising practices, such as third-party tracking, could yield tens of billions of dollars in losses for the U.S. economy—and, importantly, not just in the advertising sector.[23] One recent study found that "[t]he U.S. open web's independent publishers and companies reliant on open web tech would lose between $32 and $39 billion in annual revenue by 2025" if third-party tracking were to end "without mitigation."[24] That same study found that the lost revenue would become absorbed by "walled gardens," or entrenched market players, thereby consolidating power and revenue in a small group of powerful entities.[25] Smaller news and information publishers, multi-genre content publishers, and specialized research and user-generated content would lose more than an estimated $15.5 billion in revenue.[26] According to one study, "[b]y the numbers, small advertisers dominate digital advertising, precisely because online advertising offers the opportunity for low cost outreach to potential customers."[27] Absent cost-effective avenues for these smaller advertisers to reach the public, businesses focused on digital or online-only strategies would suffer immensely in a world where digital advertising is unnecessarily encumbered by overly-broad regulations.[28] Data-driven advertising has thus helped to stratify economic market power and foster competition, ensuring that smaller online publishers can remain competitive with large global technology companies.

B. Advertising Supports Maine Residents' Access to Online Services and Content

In addition to providing economic benefits, data-driven advertising subsidizes the vast and varied free and low-cost content publishers offer consumers through the Internet, including public health announcements, news, and cutting-edge information. Advertising revenue is an important source of funds for digital publishers,[29] and decreased advertising spends directly translate into lost profits for those outlets. Revenues from online advertising based on the responsible use of data support the cost of content that publishers provide and consumers value and expect.[30] And, consumers tell us that. In fact, consumers valued the benefit they receive from digital advertising-subsidized online content at $1,404 per year in 2020—a 17% increase from 2016.[31] Another study found that the free and low-cost goods and services consumers receive via the ad-supported Internet amount to approximately $30,000 of value per year, measured in 2017 dollars.[32] Legislative frameworks that inhibit or restrict digital advertising can cripple news sites, blogs, online encyclopedias, and other vital information repositories, and these unintended consequences also translate into a new tax on consumers. The effects of such legislative frameworks ultimately harm consumers by reducing the availability of free or low-cost educational content that is available online.

---

[23] *See* John Deighton, *The Socioeconomic Impact of Internet Tracking* 4 (Feb. 2020), located here.
[24] *Id*. at 34.
[25] *Id*. at 15-16.
[26] *Id*. at 28.
[27] J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 9 (2022), located here.
[28] *See id.* at 8.
[29] *See* Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located here.
[30] *See* John Deighton & Peter A. Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the US Economy* (2015), located here.
[31] Digital Advertising Alliance, *Americans Value Free Ad-Supported Online Services at $1,400/Year; Annual Value Jumps More Than $200 Since 2016* (Sept. 28, 2020), located here.
[32] J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 2 (2022), located here.

C. Consumers Prefer Personalized Ads & Ad-Supported Digital Content and Media

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. One study found more than half of consumers (53 percent) desire relevant ads, and a significant majority (86 percent) desire tailored discounts for online products and services.[33] Additionally, in a recent Zogby survey conducted by the Digital Advertising Alliance, 90 percent of consumers stated that free content was important to the overall value of the Internet and 85 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.[34]

Unreasonable restraints on advertising create costs for consumers and thwart the economic model that supports free services and content online. For example, in the wake of Europe's General Data Protection Regulation, and the opt-in consent requirements under that regime, platforms that have historically provided products and services for free have announced proposals to start charging consumers for access to their offerings.[35] LD 1977, which would outlaw the use of data collected across websites over time for targeted advertising, would create a similar environment where many companies could be forced to charge for services and products that were once free to Maine residents. Indeed, as the Federal Trade Commission noted in one of its submissions to the National Telecommunications and Information Administration, if a subscription-based model replaces the ad-based model of the Internet, many consumers likely will not be able to afford access to, or will be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.[36] A subscription model will diminish the number of channels available to access information, increase costs to consumers, curtail access to a diversity of online voices, and create an overall Internet environment where consumers with means can afford to access content, while consumers with less expendable income will be forced to go without access to online resources.

Laws that restrict access to information and economic growth can have lasting and damaging effects. The ability of consumers to provide, and companies to responsibly collect and use, consumer data has been an integral part of the dissemination of information and the fabric of our economy for decades. The collection and use of data are vital to our daily lives, as much of the content we consume over the Internet is powered by open flows of information that are supported by advertising. We therefore respectfully ask you to carefully consider LD 1977's potential impact on advertising, the consumers who reap the benefits of such advertising, and the overall economy before advancing it through the legislative process.

* * *

[33] Mark Sableman, Heather Shoenberger & Esther Thorson, *Consumer Attitudes Toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates* (2013), located here.
[34] Digital Advertising Alliance, *Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet Summary Report* (May 2016), located here.
[35] *See, e.g.* Megan Cerullo, *Meta proposes charging monthly fee for ad-free Instagram and Facebook in Europe*, CBS NEWS (Oct. 3, 2023), located here; *see also* Ismail Shakil, *Google to block news in Canada over law on paying publishers*, REUTERS (Jun. 29, 2023), located here.
[36] Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located here.

We and our members support protecting consumer privacy. We believe, however, that LD 1977 would impose particularly onerous requirements on entities doing business in the state and would unnecessarily impede Maine residents from receiving helpful services and accessing useful information online. We therefore respectfully ask you to reconsider LD 1977 or amend it to reflect the recommendations set forth in this letter. Thank you in advance for consideration of this letter.

Sincerely,

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

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
202-355-4564

Lartease Tiffith
Executive Vice President for Public Policy
Interactive Advertising Bureau
212-380-4700

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

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
347-770-0322

CC: Bill Co-Sponsors
Members of the Maine Joint Standing Committee on Judiciary

Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP

MAINE STATE CHAMBER of COMMERCE

The voice of Maine business

October 17, 2023

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

RE: LD 1705, LD 1902, LD 1973, LD 1977 - Privacy Legislation Work Session

Senator Carney, Representative Moonen, and members of the Judiciary Committee:
My name is Ashley Luszczki and I represent the Maine State Chamber of Commerce, which is the voice of more than 5,000 Maine businesses. Echoing the concerns you have heard from others today, we would like to provide input as an interested participant in the data privacy conversation. With regard to the questions asked by members of the Judiciary Committee for today's work session, please see our responses to those questions provided below in bold.

(1) What are the benefits and drawbacks of including a private right of action in consumer data privacy legislation?
Private Right of Action gives concern to the business community as it could drive up the cost of doing business and create a more litigious environment.

(2) Should the Legislature enact standalone bills addressing biometric identifiers and health data in addition to enacting a comprehensive data privacy bill or should the Legislature address all types of consumer personal data in a single bill? Why?
When there are various pieces of legislation being debated that seek to address some of the same issues with multiple moving parts, we believe it makes the most sense for the purpose of consistency to have one comprehensive bill dealing with data privacy that works for as many interested parties as possible.

(3) How does the choice between an opt-in or an opt-out model for consumer consent to the collection/sharing/sale of personal data impact consumers?
The Chamber is supportive of an opt-out approach as we believe it will be easier for businesses to comply.

(4) Are there particular approaches to consumer data privacy in other states that you consider particularly valuable or problematic?
The Chamber believes that the Connecticut Data Privacy Act is a valuable law to model. Of the proposed legislation before you, the Chamber feels that LD 1973 is most closely modeled after CT's law. As previously mentioned, we do find the Private Right of Action in LD 1977 to be problematic for Maine's business community.

28 State Street, Suite 101 ◆ Augusta, Maine 04330-5630 ◆ tel (207) 623-4568 ◆ fax (207) 622-7723 ◆ website: www.mainechamber.org ◆ e-mail: info@mainechamber.org

(5) What existing federal laws protect consumer personal data in your industry (or the industry of concern to you) – what types of data do those laws protect (or not protect) and what types of companies do they regulate (or not regulate)?
The Maine State Chamber of Commerce focuses most closely on policy being proposed and adopted in Maine; however, we recognize that some federal laws around data privacy apply to our members. For example, the Gramm-Leach-Bliley Act protects consumer data collected by financial institutions and HIPPA protects patient data collected by healthcare entities.

(6) Are there any pending Congressional proposals regarding consumer data privacy of which the Maine Legislature should be aware?
Aside from the American Data Privacy and Protection Act, the Chamber would defer to others on what additional bills are being considered by Congress regarding data privacy.

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

Overview of the Gramm-Leach- Bliley Act

Presented by Gordon Laurendeau, Attorney
Bureau of Financial Institutions
Before the Joint Standing Committee on the Judiciary
November 8, 2023

1

GLBA Legislative History

- Gramm-Leach Bliley Act (GLBA) was enacted on November 12, 1999
- Reformed financial services industry, with privacy as a core concept
- FTC enforces GLBA as applied to covered entities in conjunction with other government regulators (for financial institutions, this may include the FDIC, NCUA, OCC, Federal Reserve, CFPB)
- Statute: 15 U.S.C. § 6801 et. seq.
- Regulations: 12 C.F.R Part 332 (FDIC-insured banks); 12 C.F.R. Part 716/1016 (NCUA-insured credit unions)

2

Purpose of GLBA

A financial institution may not disclose nonpublic personal information about a customer unless that financial institution first provides the customer an opportunity to opt-out of some information sharing.

3

What entities are covered by GLBA?

- **Organization is subject to GLBA if it is "significantly engaged" in "financial activities"**
- "Significantly engaged" standard
  - Formal arrangement?
  - Frequency
- Financial activities include:
  - Lending, exchanging, transferring, investing for others, or safeguarding money or securities
  - Providing financial, investment, or economic advisory services
  - Brokering loans
  - Servicing loans
  - Debt collection
  - Real estate settlement services
  - Career counseling for individuals seeking employment in the financial services industry

- Entities covered by GLBA include:
  - Lenders and financial institutions
  - Check cashers
  - Wire transfer services
  - Sellers of money orders

4

Information covered by GLBA - NPI

- **GLBA protects "nonpublic personal information" (NPI)**
- NPI includes "any personally identifiable information" collected in connection with providing a financial product or service, unless that information is publicly available
- NPI examples:
  - Name, address, income, SSN (information collected on applications)
  - Account numbers, payment history, loan or deposit balances, credit and debit card purchases (information collected from transactions involving financial products
  - Court records, credit scores, and other additional information (i.e. data collected when providing financial product or service)
- Publicly available information examples:
  - Federal, state , local government records (i.e. deeds, mortgage recording)
  - Information widely distributed and available to general public through media, news, etc.

5

Financial Institutions' obligations under GLBA

- Provide customers a "clear and conspicuous" written notice on institutions' privacy policies and practices
- Initial notice provided at the time customer relationship is established
- If NPI is shared with non-affiliated third parties, notice must also provide customers
  - "Opt-out" notice explaining customers right to direct financial institution not to share NPI with third party
  - Notice must provide a reasonable means to opt-out
  - Notice must be given so customer has reasonable time to opt-out before information is shared
- Safeguard security - Interagency Guidelines Establishing Information Security Standards

6

Interagency Guidelines Establishing Information Security Standards

- 12 CFR Part 364 Appendix B
  - Address standards for developing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information
    - Implement comprehensive information security program – objectives:
      - Ensure confidentiality of customer information
      - Protect against anticipated threats or hazards to the security and integrity of information
      - Protect against unauthorized access that could result in substantial harm or inconvenience to the customer
      - Ensure proper disposal of customer information
  - Security programs developed by institution, approved by Board of Directors; focused on risk assessment and mitigation

7

Who gets a GLBA privacy notice?

Consumers and customers

- Consumer
  - Individual who obtains or has obtained a financial product to be used primarily for personal, family, or household purpose
  - Does not include commercial clients

- Customer
  - subclass of "consumers" with a continuing relationship with the financial institution
  - Depends on the nature of the ongoing relationship
  - Former customers considered customers for purposes of Privacy Rule

8

Financial Institutions' obligations cont.

- Customers must also receive an annual privacy notice (full copy of privacy policy) each year for as long as relationship lasts
  - Some financial institutions may qualify for an exception to this rule:
    - Institution does not share NPI unless authorized by statute
    - Policies governing information sharing have not changed since the last annual privacy notice

9

Contents of Privacy Notice

Categories of information collected

- Nonpublic personal information (NPI) obtained from an application or a third party

Categories of information disclosed

- Information including
  - Name
  - Address
  - SSN
  - Phone number
  - Account information

10

Content of Privacy Notice Cont.

Affiliates and non-affiliated third parties to whom the financial institution discloses information

- Examples
  - Financial services providers
  - Mortgage brokers
  - Insurance companies
  - Non-financial companies
    - Retailers
    - Charitable organizations
    - Direct marketers

Information disclosed "as permitted by law"

- When administering financial products and services the customer authorizes, includes disclosures to creditors on credit applications
- Information shared to prevent fraud and comply with federal, state, or other rules (e.g. reporting elder financial exploitation); respond to subpoenas
- Disclosures required by the Fair Credit Reporting Act if the lender uses consumer reports when making credit decisions

11

Contents of Privacy Notice cont.

- If the financial institution discloses information to non-affiliated third parties, and the information does not fall within an exception authorizing financial institution to share with others, an explanation of the customer's and consumer's right to opt-out of these disclosures
- Only need to provide notice to consumers based on actual information collected and shared
  - "Simplified" privacy notice: a financial institution only needs to disclose (1) collection of NPI, (2) state only disclose information to non-affiliated third parties "as permitted by law," (3) explanation of how NPI is protected

12

Model Form – Regulation P

Version 2: Model Form with Opt-Out by Telephone and/or Online.

Rev. [insert date]

FACTS	WHAT DOES [NAME OF FINANCIAL INSTITUTION] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of financial institution] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing	■ Call [phone number]—our menu will prompt you through your choice(s) or ■ Visit us online: [website] Please note: If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [website]

13

Privacy Notice Form

"Clear and Conspicuous"

May be on paper or on a website (must obtain acknowledgment of receipt for electronic delivery)

Must be easily understood and read, use plain language, and provide explanation of information sharing

14

Opt-Out Notice – reasonable notice given?

- Accepted "reasonable" means to opt-out
  - Toll free phone number
  - Detachable form with check-off box and mailing information
- Reasonable time to opt out before information shared with non-affiliated third parties
  - Is 30 days reasonable? 90 days? Reasonableness will depend on the nature of the transaction.
  - Right to opt out can be exercised at any time, not just before the initial transaction or beginning of the relationship; once received, financial institution must comply as soon as reasonably possible
  - The opt-out continues until it is terminated in writing - even if the customer relationship ends

15

Joint-marketing exception to opt-out notice

- The service provider/joint marketing exception permits an institution to disclose consumers' nonpublic information to nonaffiliated third parties for marketing purposes without first providing customers the ability to opt-out
- To qualify for the exception: (1) The institution must "fully disclose" to the consumer that it will provide this information to the nonaffiliated third party before the information is shared; and (2) The institution must enter into a contract with the third party that requires the third party to maintain the confidentiality of the information provided
- Applies to opt-out requirement – other GLBA items, such as annual privacy notice and data security guidelines, still apply

16

FCRA Considerations

- FCRA considerations apply if a lender *chooses* to use consumer credit reports when making credit decisions (many do)
- Requires clear and conspicuous disclosures to consumer concerning information sharing, such as credit reports and credit application information
- Applies broadly to information contained in consumer reports, includes any written, oral, or other communication describing creditworthiness or information used to for obtaining credit. Information under FCRA may also be used for employment eligibility purposes
- Under the FCRA, if information is shared for marketing or solicitations, customer must be provided with an opportunity to opt-out

17

GLBA Enforcement

- Federal law
  - Enforcement: Bureau of Consumer Financial Protection, Federal functional regulators (FDIC, NCUA, Fed Reserve), State insurance authorities, and the Federal Trade Commission
- Penalties
  - 15 U.S.C. § 6823 – up to $100,000 fine, up to 5 years in prison
  - Enhancement for aggravated cases – illegal activity involving more than $100,000, pattern in a 12-month period, amounts raised and up to 10 years in prison
- Maine law
  - Title 9-B, Maine Banking Code
    - § 161 (M), (O)
    - § 241 (13)
  - Title 9-A, Maine Consumer Credit Code
    - § 9-310
    - § 3-314

18

Summary of Confidentiality Provisions in the Federal Health Insurance Portability and Accountability Act and the Maine Insurance Information and Privacy Protection Act

This is a summary of confidentiality provisions in the federal Health Insurance Portability and Accountability Act and the state Insurance Information and Privacy Protection Act, specifically, what entities are regulated by each law, what types of data are regulated by each law, and how that data is protected. More detailed information is provided in Appendix A, Permitted and Required Disclosures of Personal Health Information under HIPAA, Appendix B, List of Regulated Insurance Entity Types, Appendix C, Bulletin 308 Consumer Privacy Obligations of Regulated Insurance Entities, and Appendix D, Bulletin 379 "Safe Harbor" Privacy Notice Forms.

Regarding CMS Privacy Regulations promulgated under HIPAA, 45 CFR Part 164:

(a) The regulations apply to "covered entities" and their "business associates."

- Covered entities are providers, health plans (including but not limited to state regulated health insurance carriers) and health care clearinghouses. However, providers are not covered if they do not transmit any information in electronic form – this was part of the original 2000 definition.
- Business associates is a complex definition, but basically means any contractor that receives PHI from a covered entity in the course of its services. Before the HITECH Act of 2009, business associates were indirectly regulated, with the covered entity responsible for compliance, but business associates now have legal as well as contractual duties.
- As for clearinghouses, according to the Internet, "In plain language, a clearinghouse in healthcare is a middleman between a healthcare provider and a health plan that checks claims from healthcare providers to ensure they don't contain errors before forwarding them to a health plan for payment." Clearinghouses appear to be becoming obsolete.

(b) The HIPAA regulations cover protected health information (often referred to by the abbreviation PHI), meaning, with limited exceptions, all information relating to an individual's health and capable of being linked to that individual and created or received by a covered entity or employer (without the limitation to electronic information).

(c) The individual whose health information is being collected or created has the following rights:

- Right to limit sharing and use. Covered entities must make reasonable efforts to limit any disclosure of PHI "to the minimum necessary to accomplish the intended purpose." Affirmative ("opt-in") consent required with limited exceptions. Specific notice and consent required if the covered entity wants to sell the information, share or use it for marketing purposes, or if psychotherapy notes will be involved. With limited exceptions, consent to sharing or use of information can't be a condition of providing services.
- Right to notice of privacy rights.

- Right to access to medical records.
- Right to request amendment.
- Security regulations (a separate chapter) require covered entities and their business associates to protect PHI from accidents and intrusions and require notice of security breaches to affected individuals, regulators, and the media.

Regarding the Maine Insurance Information and Privacy Protection Act:

(a) The act applies to "regulated insurance entities," meaning anyone "required to be licensed" by the Bureau of Insurance under Title 24 (CHO and Delta Dental, for example) or Title 24-A (insurers, HMOs, producers, consultants, etc.). These are a subset of GLBA "financial institutions," so the Maine law operates concurrently with GLBA – see Bulletins 308 & 379. Maine's law is based on an NAIC Model Act which is currently in the midst of a major update project; we are active in the NAIC Privacy Protection Working Group.

(b) The act protects all "personal information" relating to insurance consumers, meaning "any information that identifies an individual gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health or any other personal characteristics," and defined broadly to specifically include an individual's name and address. Consumers are residents of Maine (or nonresidents who buy insurance in Maine) who obtain or apply for policies or file insurance claims. The scope of the act is primarily (but not exclusively) consumer insurance transactions, meaning transactions "primarily for personal, family or household needs rather than business or professional needs."

(c) Insurance consumers have the following rights:

- Right to limit sharing and use. Disclosures of personal information to any third party must be "made with due consideration for the safety and reputation of all persons who may be affected by the disclosure, is limited to the minimum amount of personal information necessary to accomplish a lawful purpose. General requirement for affirmative ("opt-in") consent, but information can be shared for marketing purposes on an "opt-out" basis as long as the information does not include "health care information, confidential investigative information or information relating to a consumer's character, personal habits, mode of living or general reputation." Unlike GLBA, this opt-out right does apply to "joint marketing" arrangements. However, state law does not require an opt-out for sharing with affiliates if the information shared does not include health information Federal law now does require an opt-out for sharing with affiliates.
- Right to notice of privacy rights – coordination with the GLBA notice is encouraged.
- Right to access to personal information and to reasons for adverse underwriting decisions.

- Right to have underwriting decisions based on first-hand information (not on secondary sources or the mere fact that another carrier has turned you down in the past).
- Right to request correction.
- Separate data security laws (Insurance Data Security Act and NRPDA) require regulated insurance entities and their third party service providers to protect nonpublic personal information from accidents and intrusions.

Appendix A

Permitted and Required Disclosures of Protected Health Information under HIPAA

Required Disclosures

- To an individual or that individual's personal representative, when the individual requests access to, or an accounting of disclosures of, the individual's protected health information
- To the federal Department of Health and Human Services when that department is undertaking a compliance investigation or review or enforcement action.

Permitted Disclosures

A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations. Covered entities may rely on professional ethics and best judgments in deciding to make these permissive uses and disclosures.

- To the individual (unless required for access or accounting of disclosures)
    - A covered entity may disclose protected health information to the individual who is the subject of the information.
- Treatment, payment, and health care operations[1]
    - A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities. A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship.
- Opportunity to agree or object;

[1] Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another. Payment encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual. Health care operations are any of the following activities: quality assessment and improvement activities, including case management and care coordination; competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; specified insurance functions, such as underwriting, risk rating, and reinsuring risk; business planning, development, management, and administration; and business management and general administrative activities of the entity.

- Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual. Example of this kind of disclosure are facility directories, dispensing filled prescriptions to a person acting on behalf of the patient, relying on an individual's informal permission to use or disclose protected health information for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care of the individual's location, general condition, or death.

- Incident to an otherwise permitted use and disclosure
  - A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by the Privacy Rule.
- Public interest and benefit activities
  - ***Public Health Activities.*** Covered entities may disclose protected health information to:
    - public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability
    - entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance
    - individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law
    - employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law
  - ***Victims of Abuse, Neglect or Domestic Violence.*** In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.
  - ***Health Oversight Activities.*** Covered entities may disclose protected health information to health oversight agencies for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.

- ***Judicial and Administrative Proceedings.*** Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.
- ***Law Enforcement Purposes.*** Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions:
    - as required by law, including court orders, court-ordered warrants, subpoenas and administrative requests
    - to identify or locate a suspect, material witness, or missing person or individual who appears to have escaped from lawful custody
    - in response to a law enforcement official's request for information about a victim or suspected victim of a crime
    - to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death
    - when a covered entity believes that protected health information is evidence of a crime that occurred on its premises
    - by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime
    - to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public

- ***Decedents.*** Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.
- ***Cadaveric Organ, Eye, or Tissue Donation.*** Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.
- ***Research.*** "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge. The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual's authorization, provided the covered entity obtains either:
    - documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board;

- representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or
- representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.

- ***Essential Government Functions.*** An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include:
  - assuring proper execution of a military mission,
  - conducting intelligence and national security activities that are authorized by law National Security Act (45 CFR 164.512(k)(2)),
  - providing protective services to the President(45 CFR 164.512(k)(3));,
  - making medical suitability determinations for U.S. State Department employees,
  - protecting the health and safety of inmates or employees in a correctional institution(45 CFR 164.512(k)(5)), and
  - determining eligibility for or conducting enrollment in certain government benefit programs.[41]
- ***Workers' Compensation.*** Covered entities may disclose protected health information as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.

Appendix B
List of Regulated Insurance Entity Types

Class	Entity	Regulatory Authority, Title 24-A if not otherwise specified	License Type
Individuals	Adjusters	Chapter 16	License
	Producers	Chapter 16	License
	Consultants	Chapter 16	License
	Navigators	§2188, Rule 950	License
Business Entities	Adjusting firms	Chapter 16 § 1402 3 A (business entity) § 1413	License
	Agencies	Chapter 16 § 1402 3 A (business entity) § 1413	License
	Consulting firms	Chapter 16 § 1402 3 A (business entity) § 1413	License
	Equipment rental companies	Chapter 16, § 1413(9) and § 3043	License
	Limited lines self storage providers	Chapter 99	License
	Motor vehicle rental companies	Chapter 16 § 1402, 3, A and § 1413	License
	Portable electronic device vendors	Chapter 89	License
	Structured settlement transferees	Chapter 24-A §2241-2246	License
	Supervising travel insurance producer	Chapter 90	License
Insurance Companies	Insurers	• Rule Chapter 231 (DOC) - (Certificates of Authority for Insurance Companies) - Replaced Reg. Chapter 230 effective August 9, 2005.	License

		• Title 24-A Section 410 - (Minimum Paid-In Capital and Surplus Requirements) • Title 24-A M.R.S.A., Chapter 75 §630-6311 - Rural Medical Access Program (RMAP) • Rule Chapter 630 (DOC) - Rural Medical Access Program (RMAP)	
	Captive insurers	Chapter 83 and Title 36 Chapter 817	License
	HMOs	• Title 24-A Chapter 56 - (Health Maintenance Organizations) • Rule Chapter 191 (DOC) - (Application Submission Requirements)	Cert of Auth
	Reinsurer	• Rule 740 (DOCX) (Credit for Reinsurance) • 24-A MRSA §731-B(B-1)(B-2)(B-3) (Credit for Reinsurance) • Rule 730 (DOC) (Standards for Acceptance of Reinsurance of Workers' Compensation Self-Insurance)	Accredited, have to be otherwise licensed
	Risk Retention Groups	• Title 24-A M.R.S.A. Chapter 72-A (Maine Liability Risk Retention Act) • Title 36 M.R.S.A. 2513-A (Tax on Premiums of Risk Retention Groups)	Registration
	Surplus Lines	• Title 24-A M.R.S.A. §2007 - Eligible Surplus Lines Insurers • Bulletin 378 (PDF) - Changes to the Nonadmitted Insurance Laws • Bulletin 439 (PDF) - Placement of Insurance in Surplus Lines Market • Title 24-A M.R.S.A., Chapter 75 §6301-6311 - Rural Medical Access Program (RMAP)	Eligible

		• Rule Chapter 630 (DOC) - Rural Medical Access Program (RMAP)	
Others	Continuing care retirement companies	Chapter 73	Cert of Auth
	Managing general agents	Chapter 16	Registration
	Medical utilization review entity	• Title 24-A M.R.S.A. Chapter 34 (Licensure of Medical Utilization Review Entities) • Title 24-A M.R.S.A. Chapter 56-A (Health Plan Improvement Act) • Title 24 M.R.S.A. §2302-A (Nonprofit Hospital or Medical Service Organizations) • Title 24-A M.R.S.A. §§2749(A) (Penalty for Failure to Notify of Hospitalization) • Title 24-A M.R.S.A §2847-A (Penalty for Failure to Notify of Hospitalization) • Maine Bureau of Insurance Rule 850 (DOC) (Health Plan Accountability) • Maine Bureau of Insurance Bulletin 265 (PDF) (Utilization Review Determinations)	License
	Multiple Employer Welfare Arrangement	• Title 24-A M.R.S.A. Chapter 81 (Multiple-Employer Welfare Arrangements) • Title 32 M.R.S.A. Chapter 125 (Employee Leasing Companies)	Approval
	Pharmacy benefits managers	§§ 4347-4350	Registration
	Reinsurance intermediaries	• Title 24-A M.R.S.A. Chapter 9 - Subchapter IV §741 - §754 (Reinsurance Intermediaries)	Registration

		• Title 24-A M.R.S.A. Chapter 9 - Subchapter IV §747 (Manager Required Contract Provisions) • Title 24-A M.R.S.A. Chapter 9 - Subchapter IV §748 (Managers Books, Records and Powers) • Title 24-A M.R.S.A. Chapter 9 - Subchapter IV §744 (Broker Required Contract Provisions) • Title 24-A M.R.S.A. Chapter 9 - Subchapter IV §745 (Brokers Books and Records)	
	Risk purchasing groups	Chapter 72-A	Registration
	Service contract provider or administrator	Chapter 91	Registration
	Special Purpose Reinsurance Vehicle	Chapter 9, Subchapter 6	License
	Third Party Administrator	Chapter 18	License
	Viatical and Life Settlement Provider	• Title 24-A MRSA Chapter 85 (Viatical and Life Settlements Act) • Bulletin 374 Life Insurance Policy Holder Notice (PDF) • Life Settlement Consumer Guide (PDF) - (for insurers and producers as required by § 6808-A(4)) • Alternative Life Settlement Consumer Guide (PDF) - ((for insurers and producers as required by § 6808-A(4))	License

Appendix C

Bulletin 308
Consumer Privacy Obligations of Regulated Insurance Entities

This Bulletin is being issued to clarify the privacy obligations of regulated insurance entities under state and federal law with respect to insurance consumers. In addition to the existing Maine Insurance Information and Privacy Protection Act, 24-A M.R.S.A. §§ 2201–2220 (the "Maine Insurance Privacy Act"), two recent privacy initiatives provide new consumer protections in all sectors of the financial services market, including insurance. At the federal level, Title V of the federal Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809, was enacted in 1999, and compliance became mandatory as of July 1, 2001. At the state level, "An Act to Conform the State's Financial Services Privacy Laws with Federal Law," P.L. 2001, c. 262 (L.D. 1640), was signed into law by Governor Angus S. King, Jr. on May 24, and takes effect on September 21, 2001 (the "Maine Financial Services Privacy Act").

(1) How does the new Maine Financial Services Privacy Act affect insurance? The effect of Chapter 262 on insurance is less extensive than on other financial services sectors, because the Maine Insurance Privacy Act has been in place for the life and health insurance industry. The principal insurance-related provision of the Maine Financial Services Privacy Act extends the scope of the Maine Insurance Privacy Act to include property and casualty insurance. Since the Maine Insurance Privacy Act is based on an NAIC Model Act used in a number of states, many property-casualty companies have already structured their operations so as to be in substantial compliance. Little or no change may be necessary for those companies after Chapter 262 takes effect. In addition, the Maine Financial Services Privacy Act clarifies the Superintendent's rulemaking authority to implement the provisions of the Gramm-Leach-Bliley Act. The Superintendent is currently evaluating the need for rulemaking, and expects to announce a proposal later this summer.

(2) Who is a covered insurance consumer? The Maine Insurance Privacy Act and the Gramm-Leach-Bliley Act apply only to insurance consumers: individuals who have been involved in insurance transactions for personal, family, or household purposes. This includes, but is not limited to, individuals who have shopped for or purchased personal lines coverage (even if the policy also provides incidental coverage for certain business activities), who are certificateholders under group life and health policies, or who have filed personal injury or workers' compensation claims against insurance policies or state-regulated self-insurance plans. However, individuals covered by self-funded private employer health plans are not considered insurance consumers, because federal law (ERISA) exempts those plans from state regulation. Finally, although the consumer privacy laws do not cover commercial policyholders or liability claims filed by business entities, **carriers and insurance professionals should be aware that if**

they have collected health information on individuals who are not consumers, such information remains protected under Maine law, 22 M.R.S.A. § 1711-C.

(3) When and how may personal information be shared? The Gramm-Leach-Bliley Act provides that "It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." The privacy laws establish four basic categories of disclosures of personal information. In all cases, the disclosure must be made in a manner that protects the confidentiality of the information and, in the words of the Maine Insurance Privacy Act, must be "made with due consideration for the safety and reputation of all persons who may be affected by the disclosure [and] limited to the minimum amount of personal information necessary to accomplish a lawful purpose." 24-A M.R.S.A. § 2215(1).

- Disclosures "permitted by law" – a variety of disclosures made for limited purposes in the ordinary course of business, such as underwriting, claims handling, information processing, and fraud prevention. These may be described in generic terms in the regulated insurance entity's notice of information practices.

- Disclosures to affiliates for marketing purposes – **such disclosures may not include health information.** Consent is not required under state law or the Gramm-Leach-Bliley Act as long as the privacy notice provides an adequate explanation. Similar standards apply if you disclose personal information to nonaffiliated "service providers" for purposes of marketing your own products and services.

- "Opt-out" – information may be disclosed for marketing purposes to non-affiliated third parties on an "opt-out" basis, as discussed more fully below, but only if it does not include health information or information about character, personal habits, mode of living, or general reputation. Under the Maine Insurance Privacy Act, the consumer has the right to opt out even if the third party has entered into a joint marketing agreement.

- "Opt-in" – anything that does not fall into the other three categories requires the affirmative written consent of the consumer; the law provides minimum standards for release forms. In situations where there may be a conflict of interest, consent must be given personally and not by a family member. When there is a legitimate business purpose – for example, access to health history when underwriting a life insurance application – the law does not prohibit a company from requiring the consumer to "opt in" to certain information disclosures as a condition of doing business.

(4) What should have happened by July 1, 2001? The Gramm-Leach-Bliley Act gives consumers two basic rights: the right to receive notices of information practices, and the right to withhold consent to certain disclosures of nonpublic personal information. Regulated insurance entities that are currently subject to the Maine Insurance Privacy Act, or which voluntarily adhere to nationwide standards consistent with the NAIC Model Privacy Act, should already be in substantial compliance with most Gramm-Leach-Bliley requirements. The most significant new federal requirement is that the reminder notices to existing customers, which under state law may be provided every other renewal cycle, must now be given at least annually. Although compliance with the Maine Insurance Privacy Act is voluntary for the property-casualty industry

until September 21, compliance with Gramm-Leach-Bliley is now mandatory for all lines of insurance. **Therefore, if regulated insurance entities were sharing any personal information that has become subject to a consent requirement, they must have ceased doing so by July 1, 2001 unless the individual has already been given notice and a reasonable opportunity to opt out (in cases where an opt-out standard applies) or the individual has given affirmative written or recorded electronic consent.**

(5) How does the opt-out process work? If a regulated insurance entity, as defined by 24-A M.R.S.A. § 2204(23) ("licensee"), wishes to share nonpublic personal information about insurance consumers with nonaffiliated third parties for marketing purposes (including the sale of customer lists), each consumer who is affected, including former customers, must first be given the right to "opt out" of such disclosures. Certain information sharing with affiliates may also be subject to an opt-out requirement under the federal Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq.* In addition, some companies for business reasons may voluntarily provide an opportunity to opt out of some information sharing with affiliates. In order for the consumer's implied consent to be valid, there must be a clear and conspicuous notice describing what information the licensee wishes to share for what purposes, and how the consumer may exercise his or her right to opt out. The licensee must provide a reasonable means to opt out, such as a clearly labeled toll-free number or a simple response form, and wait a reasonable period of time (30 days is considered sufficient) before sharing information if the consumer does not respond. Consumers may not be discriminated against if they choose to opt out. Under the Maine Insurance Privacy Act, **even if the consumer has declined to opt out, information shared by implied consent may not include health information or information about character, personal habits, mode of living, or general reputation.**

(6) Must carriers and producers both provide notice to the same consumers? It depends on the producer's information practices. Insurance producers or agencies do not have to provide a separate set of notices as long as the carriers they represent give adequate notice and the producers do not use or disclose a consumer's personal information in a manner inconsistent with the notice(s) the consumer receives from the carrier(s). However, if the producer is also going to disclose personal information for its own purposes – for example, if the producer sells customer lists to third parties – then the producer will have to provide notice, and when information is being shared for marketing purposes with nonaffiliated third parties, the producer must also provide an opportunity for consumers to opt out.

(7) Who is entitled to receive privacy notices? Any consumer who is a "customer" (a policyholder or someone else with an ongoing business relationship) is entitled to receive a copy of the regulated insurance entity's notice of information practices and privacy rights at the time the customer relationship is formed and annually thereafter. In addition, other consumers (including but not limited to applicants who do not purchase coverage, certificateholders under employee group policies, and third-party or workers' compensation claimants) are entitled to receive a copy of the notice if the regulated insurance entity either: (1) wishes to share personal information beyond the "disclosures permitted by law" in the necessary course of business; (2) collects additional information from sources other than the consumer; or (3) has selected the consumer for solicitation using criteria based on nonpublic personal information. Notice should also be provided to group policyholders and employee benefit plan sponsors. For individuals who are not customers or whose customer relationship has ended, a brief summary may be

provided in situations where providing the complete privacy notice is unduly burdensome, if the consumer is notified that the complete notice is available upon request.

(8) What needs to be in the notice? In order to comply with both the Gramm-Leach-Bliley Act and the Maine Insurance Privacy Act, a notice of information practices and privacy rights should contain, at a minimum, the following information:

- A statement of the licensee's policies and practices with respect to disclosing nonpublic personal information to affiliates and nonaffiliated third parties, encompassing the specific information set forth below;
- The categories of information that may be disclosed;
- The categories of persons to whom the information may be disclosed, other than "disclosures permitted by law" in the necessary course of business;
- A summary of any disclosures "permitted by law" which are made with such frequency as to constitute a general business practice;
- A description of any disclosures of personal information made for marketing purposes, and any applicable opportunity to opt out;
- The licensee's policies and practices with regard to information on former customers;
- The categories of nonpublic personal information that are collected;
- Whether such information may be collected from sources other than the consumer, and if so, how;
- A statement explaining the consumer's right to access and request correction of recorded personal information;
- If applicable, a statement that information obtained from a report prepared by an insurance support organization may be retained by the insurance support organization and disclosed to other persons;
- The policies the licensee maintains to protect the confidentiality and security of nonpublic personal information; and
- The disclosures required, if any, under the federal Fair Credit Reporting Act

While not required, a contact number and/or website link for additional information is highly encouraged.

(9) Can multistate privacy notice forms be used in Maine? Because the Maine Insurance Privacy Act exceeds the minimum requirements of Gramm-Leach-Bliley, standard multistate Gramm-Leach-Bliley notice forms will generally not be fully compliant with state law. Rather than prepare an entirely different form, licensees may use the multistate form along with a state-specific supplement, as long as the notice taken as a whole is clear and understandable to the consumer. If there is any conflict between the multistate form and the Maine supplement, the

consumer must be given clear and conspicuous notice that the Maine supplement controls, and inconsistent provisions in the multistate form do not apply in Maine.

(10) What additional rights are provided under the Maine Insurance Privacy Act? In addition to providing notice rights and confidentiality rights related to those provided by the Gramm-Leach-Bliley Act, regulated insurance entities should be aware that in Maine, as in other states that have enacted insurance privacy laws based on the NAIC Model Privacy Act, consumers have the following additional rights:

- The right to obtain access to recorded personal information in the possession or control of a regulated insurance entity, to request correction if the consumer believes the information to be inaccurate, and to add a rebuttal statement to the file if there is a dispute;

- The right to know the reasons for an adverse underwriting decision. Previous adverse underwriting decisions may not be used as the basis for subsequent underwriting decisions unless the carrier makes an independent evaluation of the underlying facts; and

- The right, with very narrow exceptions, not to be subjected to pretext interviews.

(11) Please remember the consumer perspective! Both in Maine and in other states, consumers have found some of the notices they have received to be quite confusing. Concerns raised include print that is too small, inadequate explanations of opt-out rights, and notices that are easily overlooked because they are surrounded by other promotional material. **It is essential for insurers and insurance professionals to review their practices and procedures to make sure that consumers receive privacy notices that are clear and easily understood, and to remember that even the best written material is not always sufficient; there must be well-trained staff who are ready and able to respond to consumer inquiries.**

August 20, 2001

ALESSANDRO A. IUPPA
Superintendent of Insurance

NOTE: This bulletin is intended solely for informational purposes. It is not intended to set forth legal rights, duties, or privileges, nor is it intended to provide legal advice. Readers are encouraged to consult applicable statutes and rules and to contact the Bureau of Insurance at (207) 624-8475 if they need additional information.

Appendix D

BULLETIN 379

"Safe Harbor" Privacy Notice Forms

The purpose of this bulletin is to clarify how regulated insurance entities in Maine may use the simplified Federal Model Privacy Form (sometimes referred to as the "safe harbor" form) to comply with the federal privacy notice requirements under Title V of the Gramm-Leach-Bliley Act (GLBA),[1] and to remind regulated insurance entities of their additional obligations under the Maine Insurance Information and Privacy Protection Act ("Maine Insurance Privacy Act").[2] For additional discussion of regulated insurance entities' obligations under GLBA and the Maine Insurance Privacy Act, see Bulletin 308.

As required by the federal Financial Services Regulatory Relief Act of 2006,[3] eight federal agencies[4] adopted a simplified Federal Model Privacy Form for use by federally regulated financial institutions. The purpose of the new form is to give consumers a clearer description of their privacy rights and information-sharing options. Federally regulated financial institutions that elect to use the new Federal Model Privacy Form may rely on it as a safe harbor to provide the notices required under the federal GLBA privacy rules. Generally, regulated insurance entities licensed by the Superintendent are considered "financial institutions" for purposes of GLBA.

Use of Model Privacy Form

The use of the Model Privacy Form set forth in Attachment A to this Bulletin, consistent with the Instructions set forth in Attachments B and C, constitutes compliance with the notice content requirements of GLBA. In order to comply with the requirements of the Maine Insurance Privacy Act, regulated insurance entities must also provide clear and sufficient notice of consumers' additional rights under Maine law as described in Bulletin 308. These additional rights include:

- The right to obtain access to the consumer's recorded personal information in the possession or control of a regulated insurance entity, to request correction if the consumer believes the information to be inaccurate, and to add a rebuttal statement to the file if there is a dispute;
- The right to know the reasons for an adverse underwriting decision. Previous adverse underwriting decisions may not be used as the basis for subsequent underwriting decisions unless the carrier makes an independent evaluation of the underlying facts; and
- The right, with very narrow exceptions, not to be subjected to pretext interviews.

The state-specific notice may be provided in the "Other Important Information" section of the Model Privacy Form, or it may be provided in a separate notice. If a separate notice is provided, it must either be provided together with the Model Privacy Form or specifically referenced in the "Other Important Information" section of the Model Privacy Form.

Use of Other Types of Privacy Notices

Use of the attached Model Privacy Form is not required. Insurers may continue to use other types of privacy notices to meet the requirements of GLBA and the Maine Privacy Act as long as the notices accurately describe the insurer's privacy practices and otherwise meet the requirements of state and federal law, consistent with the guidance provided in Bulletin 308.

Attachments

Attachment A to this Bulletin consists of the three approved versions of the Model Privacy Form together with an optional separate Mail-In Form:

- Version 1: Model Form with No Opt-Out (pages 3-4)
- Version 2: Model Form with Opt-Out by Telephone and/or Online (pages 5-6)
- Version 3: Model with Mail-In Opt-Out Form (pages 7-8)
- Optional Separate Mail-In Form (page 9)

Attachment B provides general instructions for customizing the form, and Attachment C describes the information that must be included.

[1] GLBA §§ 501-510 (substantive provisions codified at 15 U.S.C. §§ 6801-6809). The privacy notice requirement is set forth at GLBA § 503 (15 U.S.C. § 6803).

[2] 24-A M.R.S.A. chapter 24 (§§ 2201-2220). The privacy notice requirement is set forth at 24-A M.R.S.A. § 2206.

[3] Public Law 109-351.

[4] Office of the Comptroller of the Currency, Department of the Treasury; Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; Office of Thrift Supervision, Department of the Treasury; National Credit Union Administration; Federal Trade Commission; Commodity Futures Trading Commission; and Securities and Exchange Commission.

August 3, 2011

Eric A. Cioppa
Acting Superintendent of Insurance

NOTE: This bulletin is intended solely for informational purposes. It is not intended to set forth legal rights, duties, or privileges, nor is it intended to provide legal advice. Readers should consult applicable statutes and rules and contact the Bureau of Insurance if additional information is needed.

Attachment A - Federal Model Privacy Form

Attachment B - General Instructions

1. How the Model Privacy Form is used by regulated insurance entities in Maine

(a) The Model Form may be used, at the option of a regulated insurance entity (referred to in these Instructions as a "licensee"), including a group of licensees or other financial institutions that use a common privacy notice, to meet the content requirements of the privacy notice and opt-out notice required by the federal Gramm-Leach-Bliley Act. Notice of additional rights under Maine law must be provided to consumers in a manner consistent with the requirements of 24-A M.R.S.A. § 2206, as explained in Bureau of Insurance Bulletins 308 and 379.

(b) The Model Form is a standardized form, including page layout, content, format, style, pagination, and shading. Licensees seeking to obtain the safe harbor through use of the Model Form may modify it only as described in these Instructions.

(c) Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act (FCRA),[5] such as a requirement to permit consumers to opt out of disclosures to affiliates, or the licensee's designation as a consumer reporting agency if disclosures of such information are made to nonaffiliated third parties.

(d) The word "customer" may be replaced by another word such as "consumer," "member," or "enrollee" whenever it appears in the Model Form, if appropriate.

2. Contents of the Model Privacy Form

The Model Form consists of two pages, which may be printed on both sides of a single sheet of paper or may appear on two separate pages. Where a licensee provides a long list of licensees or financial institutions at the end of the Model Form in accordance with Instruction 3(a)(1) of Attachment C, or provides additional information in accordance with Instruction 3(c) of Attachment C, and the list or additional information exceeds the space available on Page Two of the Model Form, it may extend to a third page.

(a) Page One. The first page consists of the following components:[6]

(1) Date last revised (upper right-hand corner)
(2) Title
(3) Key frame (Why? What? How?)
(4) Disclosure table ("Reasons we can share your personal information")
(5) "To limit our sharing" box, as needed, for the licensee's opt-out information
(6) "Questions" box, for customer service contact information
(7) Mail-in opt-out form, as needed

(b) Page Two. The second page consists of the following components:

(1) Heading (Page 2)
(2) Frequently Asked Questions ("Who we are" and "What we do")
(3) Definitions
(4) "Other important information" box, as needed

3. Format of the Model Privacy Form.

The format of the Model Form may be modified only as described below.

(a) *Easily readable type font.* Licensees that use the Model Form must use an easily readable typeface and styling. While a number of factors together produce easily readable font, licensees are required to use a minimum of 10-point type (unless otherwise expressly permitted in these Instructions) and sufficient spacing between lines.

(b) Logo. A licensee may include a corporate logo on any page of the notice, so long as it does not interfere with the readability of the Model Form or the space constraints of each page.

(c) Page size and orientation. Each page of the Model Form must be printed in portrait orientation. The size of the paper must be sufficient to meet the layout and minimum font size requirements, with sufficient white space on the top, bottom, and sides of the content.

(d) Color. The Model Form must be printed on white or light color paper (such as cream) with black or other contrasting ink color. Spot color may be used to achieve visual interest, so long as the color contrast is distinctive and the color does not detract from the readability of the Model Form. Logos may also be printed in color.

(e) Languages. The Model Form may be translated into languages other than English and made available in those languages at the consumer's request.

Attachment C - Information Required in the Model Privacy Form

The information in the Model Form may be modified only as described below:

1. Name of licensee or group of affiliated licensees or institutions providing the notice

Insert the name of the licensee providing the notice, or the common identity of the affiliated licensees or other financial institutions jointly providing the notice, wherever **[name of financial institution]** appears on the form.

2. Page One

(a) Last revised date. The licensee must insert the date on which the notice was last revised in the upper right-hand corner. The information shall appear in minimum 8-point type as "rev.

[month/year]" using either the name or number of the month, such as "rev. July 2011" or "rev. 7/11."

(b) General instructions for the "What?" box

(1) The bulleted list identifies the types of personal information that the licensee collects and shares. All licensees must use the term "Social Security number" where shown in the first bullet, unless the licensee does not collect Social Security numbers.

(2) A licensee must use exactly five of the following terms, as appropriate to the licensee's business, to complete the bulleted list: income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions.

(c) General instructions for the disclosure table. The left column lists reasons for sharing or using personal information. Each reason correlates to a specific legal provision described in Paragraph 2(d) of this Instruction. In the middle column, each licensee must provide a "Yes" or "No" response that accurately reflects its information-sharing policies and practices with respect to the reason listed on the left. In the right column, each licensee must provide in each box one of the following three responses, as applicable, that reflects whether a consumer can limit such sharing:

"Yes," if it is required to provide an opt-out or voluntarily provides an opt-out;
"No," if it does not provide an opt-out; or
"We don't share," if it answers "No" in the middle column.

Only the sixth row ("For our affiliates to market to you") may be omitted at the option of the licensee when permitted by Paragraph (d)(6) below.

(d) Specific disclosures and corresponding legal provisions

(1) For our everyday business purposes. This reason incorporates all disclosures permitted by 24-A M.R.S.A. § 2215(1), other than the disclosures described in Paragraphs (2) through (7) below.

(2) For our marketing purposes. This reason incorporates sharing information with service providers by a licensee for its own marketing. To the extent permitted by 24-A M.R.S.A. § 2215(1)(B), a licensee that shares information for this reason may do so without being required to provide an opt-out may choose to provide an opt-out.

(3) For joint marketing with other financial companies. This reason incorporates sharing information under joint marketing agreements in accordance with GLBA § 502(b)(2). Because Maine law does not distinguish between joint marketing partners and other nonaffiliated third

parties, consumers have the right to opt out of information sharing under 24-A M.R.S.A. § 2215(1)(J)(2). If the licensee shares information under joint marketing agreements and does not voluntarily provide such an opt-out right in other states, the licensee must customize its Model Form for use in Maine, either by changing the "Can you limit this sharing?" column of the joint marketing line of the disclosure table to "Yes" or "We do not share," as applicable, or by using the "Other important information" box to apprise the consumer of his or her opt-out right in a manner that clearly explains that the "No" answer in the table is not accurate in every state.

(4) For our affiliates' everyday business purposes - information about transactions and experiences. This reason incorporates sharing information specified in FCRA §§ 603(d)(2)(A)(i) & (ii) (15 U.S.C. § 1681a(d)(2)(A)(i) & (ii)), other than information shared for marketing purposes. No opt-out is required under state or federal law, but a licensee that shares information for this reason may choose to provide an opt-out.

(5) For our affiliates' everyday business purposes - information about creditworthiness. This reason incorporates sharing information pursuant to section FCRA § 603(d)(2)(A)(iii) (15 U.S.C. § 1681a(d)(2)(A)(iii)), which requires the licensee to provide an opt-out.

(6) For our affiliates to market to you. This reason incorporates sharing information specified in FCRA § 624 (15 U.S.C. § 1681s-3), which requires the licensee to provide an opt-out. The licensee may elect to omit this reason from the disclosure table when: the licensee does not have affiliates (or does not disclose personal information to its affiliates); the licensee's affiliates do not use personal information in a manner that requires an opt-out; or the licensee provides the affiliate marketing notice separately. Licensees that include this reason must provide an opt-out of indefinite duration. A licensee that is required to provide an affiliate marketing opt-out, but does not include a mechanism for exercising that right in the Model Form, must separately provide a clear and conspicuous notice and opportunity to opt out in compliance with the requirements of FCRA and GLBA, including annual renewal notices.

(7) For nonaffiliates to market to you. This reason incorporates sharing permitted by 24-A M.R.S.A. § 2215(1)(J). Pursuant to 24-A M.R.S.A. § 2215(1)(J)(2) and GLBA § 502(b) (15 U.S.C. § 6802(b)), a licensee that shares personal information for this reason must provide an opt-out.

(e) To limit our sharing. A licensee must include this section of the Model Form if and only if it shares some classes of information subject to an opt-out. The word "choice" may be written in either the singular or plural, as appropriate. Licensees must select one or more of the applicable opt-out methods described: telephone, such as by a toll-free number; a Web site; or use of a mail-in opt-out form. Licensees may include the word "toll-free" before the telephone number, as appropriate. A licensee that allows consumers to opt out online must provide either a specific Web address that takes consumers directly to the opt-out page or a general Web address that provides a clear and conspicuous direct link to the opt-out page. The opt-out choices made available to the consumer who contacts the licensee through these methods must correspond accurately to the choices disclosed in the "Yes" responses in the third column of the disclosure table and any additional choices disclosed in the "Other important information" box. In the part

entitled "Please note," licensees that voluntarily provide a waiting period longer than 30 days may substitute the applicable time period in the space marked "[30]."

(f) Questions box. Customer service contact information must be inserted as appropriate where [phone number] or [website] appear. Licensees may elect to provide either a phone number, such as a toll-free number, or a Web address, or both. Licensees may include the words "toll-free" before the telephone number, as appropriate.

(g) Mail-in opt-out form. Licensees must include this mail-in form if and only if they state in the "To limit our sharing" box that consumers can opt out by mail. The mail-in form must provide opt-out options that correspond accurately to the choices disclosed in the "Yes" responses in the third column of the disclosure table and any additional choices disclosed in the "Other important information" box. Licensees that require consumers to provide only name and address may omit the section identified as "[account #]." Licensees that require additional or different information to implement an opt-out election, such as a random identifying number or a truncated account number, should modify the "[account #]" reference accordingly. This includes licensees that require customers with multiple accounts to identify each account to which the opt-out should apply. A licensee must enter its opt-out mailing address in the far right of this form (if Version 3 is used); or below the form (if the optional separate form is used). None of the content of the Model Form may be placed on the reverse side of the mail-in portion of the form.

(1) Joint accountholder. Licensees that give their joint accountholders the choice to opt out for only one accountholder, in accordance with Paragraph 3(a)(5) of these Instructions, must include the following statement in the far left column of the mail-in form:

If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.

❑Apply my choice(s) only to me.

The word "choice" may be written in either the singular or plural, as appropriate. Licensees may substitute the word "policy" for "account" in this statement where applicable. Licensees that do not provide this option must either leave this left column blank or eliminate it from the mail-in form.

(2) FCRA creditworthiness opt-out. If the licensee shares personal information pursuant to FCRA § 603(d)(2)(A)(iii) (15 U.S.C. § 1681a(d)(2)(A)(iii)), it must include the following statement in the mail-in opt-out form:

❑Do not share information about my creditworthiness with your affiliates for their everyday business purposes.

(3) FCRA marketing opt-out. If the licensee uses the Model Form to comply with FCRA § 624 (15 U.S.C. § 1681s-3) in accordance with paragraph 2(d)(6) of these Instructions, it must include the following statement in the mail-in opt-out form:

❑Do not allow your affiliates to use my personal information to market to me.

(4) Nonaffiliate opt-out. If the licensee shares personal information with nonaffiliates for marketing purposes, other than sharing pursuant to joint marketing agreements, it must include the following statement in the mail-in opt-out form:

❑Do not share my personal information with nonaffiliates to market their products and services to me.

If a Maine consumer checks this option, the licensee may not share the consumer's personal information pursuant to joint marketing agreements unless the licensee has provided a separate opt-out process for joint marketing and the consumer has chosen to permit sharing.

(5) Additional opt-outs. Licensees that use the disclosure table to provide opt-out options beyond those required by Federal law must provide those opt-outs in this section of the Model Form. A licensee that chooses to offer an opt-out for its own marketing in the mail-in opt-out form must include one of the two following statements:

❑Do not share my personal information to market to me.

or ❑Do not use my personal information to market to me.

A licensee that uses the Model Form to offer an opt-out for joint marketing must include the following statement:

❑Do not share my personal information with other financial institutions to jointly market to me.

(h) Barcodes. A licensee may elect to include a barcode and/or "tagline" (an internal identifier) in 6-point type at the bottom of page one, as needed for information internal to the licensee, so long as these do not interfere with the clarity or text of the form.

3. Page Two

(a) General Instructions for the Questions. Certain Questions on the Model Form may be customized as follows:

(1) "Who is providing this notice?" This question may be omitted when the Model Form is provided solely on the licensee's behalf and the licensee is clearly identified in the title on Page One. Two or more licensees or financial institutions that jointly provide the Model Form must use this question to identify themselves accurately in compliance with 24-A M.R.S.A. § 2206. If the list of licensees or financial institutions exceeds four (4) lines, the licensee must describe in the response to this question the general types of licensees or financial institutions jointly providing the notice and must separately identify those licensees or financial institutions, in minimum 8-point type, directly following the "Other important information" box, or, if that box is not included in the licensee's form, directly following the "Definitions." The list may appear in a multi-column format.

(2) "How does [name of financial institution] protect my personal information?"
The answer to this question must begin with the language specified in the form. The licensee may follow this with a supplemental response, no more than 30 words in length, providing additional information about its safeguards, such as the licensee's use of cookies.

(3) "How does [name of financial institution] collect my personal information?"
Licensees must use five (5) of the following terms to complete the bulleted list for this question: open an account; deposit money; pay your bills; apply for a loan; use your credit or debit card; seek financial or tax advice; apply for insurance; pay insurance premiums; file an insurance claim; seek advice about your investments; buy securities from us; sell securities to us; direct us to buy securities; direct us to sell your securities; make deposits or withdrawals from your account; enter into an investment advisory contract; give us your income information; provide employment information; give us your employment history; tell us about your investment or retirement portfolio; tell us about your investment or retirement earnings; apply for financing; apply for a lease; provide account information; give us your contact information; pay us by check; give us your wage statements; provide your mortgage information; make a wire transfer; tell us who receives the money; tell us where to send the money; show your government-issued ID; show your driver's license; order a commodity futures or option trade.

Licensees that collect personal information from their affiliates and/or credit bureaus must include the following statement after the bulleted list: "We also collect your personal information from others, such as credit bureaus, affiliates, or other companies." Licensees that do not collect personal information from their affiliates or credit bureaus but do collect information from other companies must include the following statement instead: "We also collect your personal information from other companies." Only licensees that do not collect any personal information from affiliates, credit bureaus, or other companies may omit both statements.

(4) "Why can't I limit all sharing?" Licensees that describe state privacy law provisions in the "Other important information" box must use the bracketed sentence: "See below for more on your rights under state law." Other licensees must omit this sentence.

(5) "What happens when I limit sharing for an account I hold jointly with someone else?"
Licensees that provide opt-out options must use this question. Other licensees must omit this question. Licensees must choose one of the following two statements to respond to this question: "Your choices will apply to everyone on your account." or "Your choices will apply to everyone on your account - unless you tell us otherwise." Licensees may substitute the word "policy" for "account" in this question and answer where applicable.

(b) General Instructions for the Definitions. The licensee must customize the space below the responses to the three definitions in this section. This specific information must be in italicized lettering to set off the information from the standardized definitions.

(1) Affiliates. Where ***[affiliate information]*** appears, the licensee must:

(i) If it has no affiliates, state: "***[name of licensee]*** has no affiliates";

(ii) If it has affiliates but does not share personal information with them, state: "*[name of licensee] does not share with our affiliates*"; or

(iii) If it shares with its affiliates, state, as applicable: "*Our affiliates include companies with a [common corporate identity] name; financial companies such as [insert illustrative list of companies]; nonfinancial companies, such as [insert illustrative list of companies]; and others, such as [insert illustrative list].*"

(2) Nonaffiliates. Where ***[nonaffiliate information]*** appears, the licensee must:

(i) If it does not share with nonaffiliated third parties, state: "***[name of licensee]*** *does not share with nonaffiliates so they can market to you*"; or

(ii) If it shares with nonaffiliated third parties, state, as applicable: "*Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations].*"

(3) Joint Marketing. Where ***[joint marketing]*** appears, the licensee must:

(i) If it does not engage in joint marketing, state: "**[name of licensee]** doesn't jointly market"; or

(ii) If it shares personal information for joint marketing, state, as applicable: "*Our joint marketing partners include [list categories of companies such as credit card companies].*"

(c) General instructions for the "Other important information" box. This box is optional. The space provided for information in this box is not limited, and an additional page may be used if necessary. Only the following types of information can appear in this box:

(1) State and/or international privacy law information; and/or

(2) A form by which the consumer may acknowledge receipt of the notice.

[5] Codified at 15 U.S.C. §§ 1681-1681x.

[6] The identifying headings in this Bulletin with the legends "Attachment A" and the four version numbers are not part of the Model Form and should not be included in the forms sent to consumers.

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

November 8, 2023

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

Sponsored by Rep. Maggie O'Neil

I. Maine should not imitate Big Tech-authored laws enacted in Virginia and Connecticut because those laws fail to adequately protect consumers.

Laws in Virginia and Connecticut were written by Big Tech and other large corporations to protect their current business practices. These laws fail to protect consumers. They do not stop harmful business practices that violate consumer expectations. Further, the proposal currently supported by industry lobbyists (LD 1973) now significantly differs from laws they have advanced in a few other states, calling into question the assertion that we should align with those states.

Here's how Connecticut's law compares to Sen. Keim's proposal (LD 1973):

- Connecticut's Data Privacy Act (1) allows companies to process our personal data without consent; and (2) gives individuals the right to opt-out from companies using our personal data in limited circumstances: (a) targeted advertising; (b) the sale of personal data; and (c) profiling. Opt-out privacy laws allow companies to maintain existing practices that violate consumer expectations. Such laws place the responsibility of preventing data abuses on consumers. They require us to seek out each website and entity we interact with, and even entities we don't interact with, to opt-out -- that could be a full-time job! Data shows that we are less likely to say "no" to unwanted ways that companies use our data when we are forced to jump through hoops to do so.

- Sen. Keim's LD 1973 amends the Big Tech model used in Connecticut and Virginia by prohibiting businesses from processing personal data for the above purposes *unless the individual first consents* ("opts-in") to such uses. The bill was changed from its original form (drafted by Tech and other industry leaders as opt-out – i.e., not requiring consent), acknowledging concerns that an opt-out model does not protect consumers. No other state has passed a law requiring opt-in consent in this way.

Sen. Keim's updates to the "Connecticut model" in LD 1973 acknowledge that Connecticut's law (which mirrors Virginia and other states' laws) does not adequately protect consumers. LD

1973 differs from Connecticut and Virginia's laws by requiring opt-in consent. No other state has passed a comprehensive privacy law requiring opt-in consent in this way.

Maine can achieve effective protections via LD 1977, a bipartisan compromise that was extensively negotiated with years of input from industry, consumer advocates, and civil rights groups. We can take advantage of the outcome of those negotiations in Maine. I will continue to work with Sen. Keim to move forward protections we both seek to advance and add a few pieces that LD 1977 advances.

II. For a "comprehensive" privacy law, consent is not the preferred model because it will place a significant burden on Mainers as they use the Internet.

There are two kinds of consumer privacy laws: (1) laws that protect data only in specific circumstances; and (2) laws that establish protections for all kinds of personal data that companies collect about us.

In specific circumstances, a consent-first model can be protective, such as when (a) a company collects an individual's unique biometric identifiers; or when (b) an internet service provider (ISP) monetizes a customer's entire browsing activity. In those cases, consumers merit notice before their data is collected and the opportunity to refuse consent. Here, consent requirements establish boundaries for the relationship and do not cause "consent fatigue." Often, we have a relationship with the entity as a consumer. At the outset of that relationship, we would receive notice that a company wants to collect our data, we answer yes or no, and then we continue with our activity. That is why Maine's current ISP privacy law requires ISPs to get our consent before monetizing customer data and why LD 1705 would require notice and consent before companies use facial recognition software on us or collect other biometric identifiers.

In contrast, for a "comprehensive" privacy law that applies to all kinds of personal data companies collect about us, a consent-first model would place a significant burden on Mainers as they use the Internet. A consent-first law incentivizes companies to (1) maintain harmful practices that violate consumer expectations and (2) merely obtain "consent" for those practices through sheer annoyance, consumer fatigue, or deception. "Consent" is often presented in such a way that consumers do not understand, preventing meaningful consent and choice. Consent is also frequently obtained by inundating consumers with requests. Imagine being presented with a choice to consent to multiple types of processing each time you visit a website – companies will simply tire us into hitting "accept." Consumers who would not typically consent might give up consent because it is too frustrating to click "no" ten times on each website we visit.

A "comprehensive" privacy law that relies on consent as its major consumer protection will not incentivize companies to shift harmful practices that violate consumer expectations. Consent is not used in other areas of consumer protection – e.g., you can't consent to a car without seat belts or to unsafe ingredients in your food. Consumers reasonably expect products to be safe, and the same should be the case online.

III. LD 1977 addresses the root of the problem by aligning company practices with consumer expectations.

LD 1977 will prevent "consent fatigue" and protect consumers by (1) aligning data collection and use with consumer expectations and (2) deterring harmful practices by ensuring violations of the law are enforced.

When we interact with a company online, we reasonably expect that our personal information will be collected and used for the specific purpose and amount of time necessary to provide services that we request. For example, a person using a map application for directions would not reasonably expect that their location data (and all that it reveals about a person, such as health status, sexuality, and religious and political affiliations), would be disclosed to third parties and combined with other data to profile them or sell their information for an unrelated purpose.

LD 1977 institutes the practice of "data minimization" to align data collection and use with consumer expectations. It has long been a pillar of privacy protection, from early privacy laws[1] to model business practices.[2] It requires companies we interact with to use our personal information for relevant purposes. Data minimization takes the onus off consumers and requires that companies limit data collection to better align with what consumers expect. That's why advocates and industry representatives settled on this this compromise solution after years of negotiations.

LD 1977 also does the following:

1. Recognizes that some sensitive categories and uses of data deserve stricter controls. The bill sets strong restrictions on the collection and use of sensitive data, including precise geolocation, biometric, and health information, as well as data identifying an individual's online activities over time and across third party websites and online services. Companies may only collect and use these types of data if doing so is strictly necessary and may not transfer such data to third parties without first obtaining a person's consent. The bill also prohibits the use of sensitive data for targeted advertising purposes. *These protections directly limit the most harmful business practices that privacy laws are intended to address.*
2. Gives users the right to access, correct, and delete data collected about them. These provisions align with Sen. Keim's proposal, aside from a few differences.
3. Extends civil rights protections online.
4. Creates a data broker registry so that Mainers will know who is selling data of Maine residents.

---

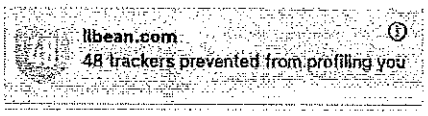
[1] Privacy laws dating back to the 1970s have recognized and applied this concept. The Privacy Act of 1974, a landmark privacy law regulating the personal data practices of federal agencies, requires data minimization. Each agency that collects personal data shall "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." 5 U.S.C. § 552a (e)(1).

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

5. Requires algorithmic impact assessments, addressing harmful AI applications and other automated decision-making.
6. Allows for multiple modes of enforcement, addressing the concern that our state OAG lacks adequate resources to ensure compliance. The private right of action only applies to the very largest businesses, ensuring enforcement while addressing small business concerns.

IV. Ads are still possible for businesses.

Nothing in LD 1977 would stop a retailer like LLBean from tracking customers within their website and sending them ads via email or mail about products they might be interested in. This is first party advertising. It will prevent unexpected activities like trackers that follow our activity across different apps, messaging, and websites. For example, on a recent visit to LLBean's website, my browser blocked 48 trackers. Even if a company like LLBean is trying to do the right thing with their own customer practices, the broader ecosystem and Big Tech companies that companies rely on for advertising need reform to honor consumer expectations.



Targeted advertising will still be possible. LD 1977 will simply put guardrails in place about how much of our data can be used in ways that we would not expect as consumers. EPIC is here today and can be a resource both on how advertising will still be possible under the provisions of the bill. As a reminder, this bill was a bipartisan compromise negotiated with years of industry input.

Financial Institutions

Today, you will receive a briefing on what financial institutions can do with personal data. I am sharing the following info from the U.S. Government Accountability Office to help understand this issue. Any exemption for financial institutions should be tailored to *information* regulated by the Gramm-Leach-Bliley Act of 1999 (GLBA). A complete exemption for GLBA-regulated entities and all activity that is not regulated by that law is overly broad and fails to protect consumers.

1. What types of information do banks collect and why?

Banks and credit unions collect and use many types of personal information to conduct everyday business activities and to market products and services. The information banks collect may be used to create bank statements, monitor for fraud, and determine credit eligibility. Banks and credit unions also gather information about consumers' online activities. This information may not identify an individual, but can be used for marketing. For example, when consumers access a financial institution's website and use mobile or online services, banks and credit unions collect information about their social media and browsing activities, type of computer or mobile device, and network address. Banks mainly use this information to ensure their websites function properly, detect and prevent fraud, and for marketing.

2. Why do banks share your information and who do they share it with?

Banks collect and share personal information for a range of reasons. It helps them approve customers for services like loans and set up accounts. But it is also helps them and their marketing partners determine whether they should offer other products and services. Banks share information with various types of third-party vendors including: financial companies like mortgage bankers, securities brokers-dealers, and insurance agents; retailers (e.g., home improvement stores), magazine publishers, airline companies, and direct marketers; companies that deliver services on behalf of the lender (e.g, mortgage servicers), and government agencies and nonprofits.

3. Financial institutions are allowed to share your information.

The primary law that governs how financial institutions can use or share personal information about consumers is the Gramm-Leach-Bliley Act of 1999 (GLBA). GLBA is not a privacy law. However, GLBA makes two privacy rules for financial institutions handling customer data: it requires (1) a privacy notice and (2) partial opt-out rights for how a customer's data is shared. States may enforce stricter rules than the GLBA.

Under the GLBA, banks, credit unions, and other financial institutions are allowed to share personal information. Without consent, financial institutions may collect, use, and share customer information with affiliates and third parties, including for marketing purposes, so long as they have certain processes in place to protect the information. Consumers have the right to opt out of some, but not all, sharing of their personal information.

Consumer protection laws that allow a company to share customer information until a customer opts out are critiqued for (a) permitting companies to violate consumer expectations; and (b) requiring consumers to undertake a laborious process to stop unwanted uses of their data. LD 1977 protects consumers from both of these harms by aligning the use of personal information with consumer expectations (via data minimization requirements) and by restricting unexpected data sharing with third parties. Those protections are important for Mainers.

Table 4: Types of Third Parties with Which Banks and Credit Unions May Share Consumer Information

Affiliate	Companies related by common ownership or control.
Nonaffiliate	Companies not related by common ownership or control.
Financial companies	Mortgage bankers, securities brokers-dealers, and insurance agents, among others.
Nonfinancial companies	Retailers, magazine publishers, airlines, and direct marketers, among others.
Service providers	Companies that deliver services to or perform functions on behalf of the institution.
Other organizations	Government agencies and nonprofit organizations, among others.

Source: GAO analysis of Regulation P (12 C.F.R. pt. 1016). | GAO- 21-36

	Institutions with over $10 billion in assets		Institutions with $10 billion or less in assets	
Reason for sharing personal information	Number of institutions that share	Number of institutions that offer opt-outs	Number of institutions that share	Number of institutions that offer opt-outs
For affiliates to market to customers	21	21	11	11
For nonaffiliates to market to customers	7	7	1	1

Source: GAO analysis of bank and credit union privacy notices. | GAO- 21-36

Note: We selected 29 institutions with total assets of more than $10 billion and 31 institutions with total assets of $10 billion or less. These institutions adopted the model privacy form to comply with notice and opt-out requirements under the Gramm-Leach-Bliley Act.

4. Any financial institution exemption should be limited to information regulated by GLBA.

A complete exemption for GLBA-regulated entities is overly broad. Any GLBA exemption should be limited to information regulated by GLBA, and it should never exempt activity left unregulated by the law. An information-level exemption would exempt what financial institutions do with customer information.[3] An entity-level exemption would exempt everything a company does from Maine's consumer protections, even though those activities are not regulated by the GLBA.

For example, if Maine enacted a law with an *information-level* GLBA exemption that required notice and consent before collecting biometric identifiers (LD 1705), customer financial transactions that use voice recognition for phone banking would be exempt. This makes sense

[3] GLBA regulates nonpublic personal information (NPI). NPI is "personally identifiable financial information: (i) provided by a consumer to a financial institution, (ii) resulting from a transaction or service performed for the consumer, or (iii) otherwise obtained by the financial institution." Financial institutions can share NPI with affiliated and non-affiliated third parties, provided such sharing takes place securely and in accordance with the institutions' privacy notice and any opt-outs of customers and consumers.

when consumers choose to use a voice recognition option and banks in Maine get consent. However, an information-level GLBA exemption would not exempt the bank from using face recognition on nonconsenting members of the public who pass by a public street corner (something we have already banned government from doing in Maine due to civil liberties concerns and risk of discriminatory impact).

In contrast, an entity-level exemption would exempt everything a GLBA-regulated company does with personal data, even when GLBA offers no protection in a particular area. This exemption is overly broad, especially because many unexpected types of entities are regulated by the GLBA. GLBA regulates U.S. "financial institutions" and their "affiliates" that are "significantly engaged" in providing financial products or services to consumers. Financial institutions can include, but are not necessarily limited to: banks, brokerage firms, insurers, payday lenders, ATM operators, car dealerships, car rental companies, courier services, debt collectors, financial advisory firms, non-bank mortgage lenders, property appraisers, and retailers. All of those entities would be completely exempt from the law, even if they are regulated for only a small aspect of their activity. For example, Kohl's or Walmart would be completely exempt from complying with the law's protections simply because they offer a credit card to consumers. An entity-level exemption would render the bill hollow.

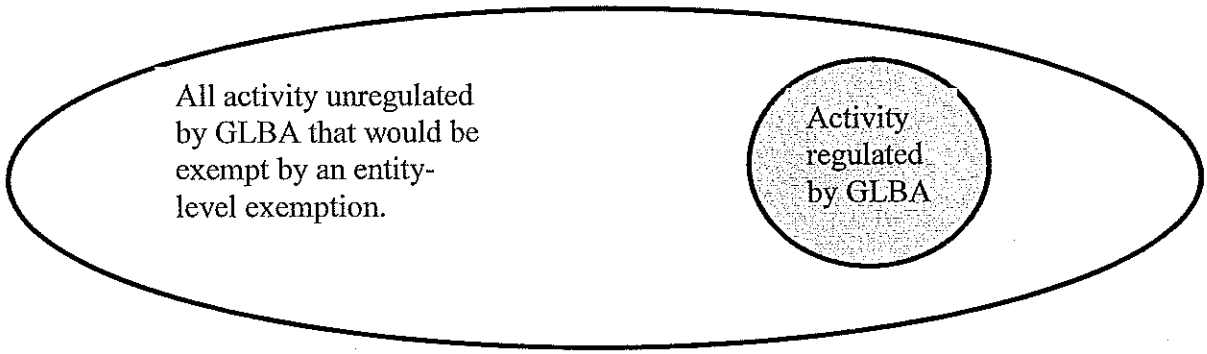
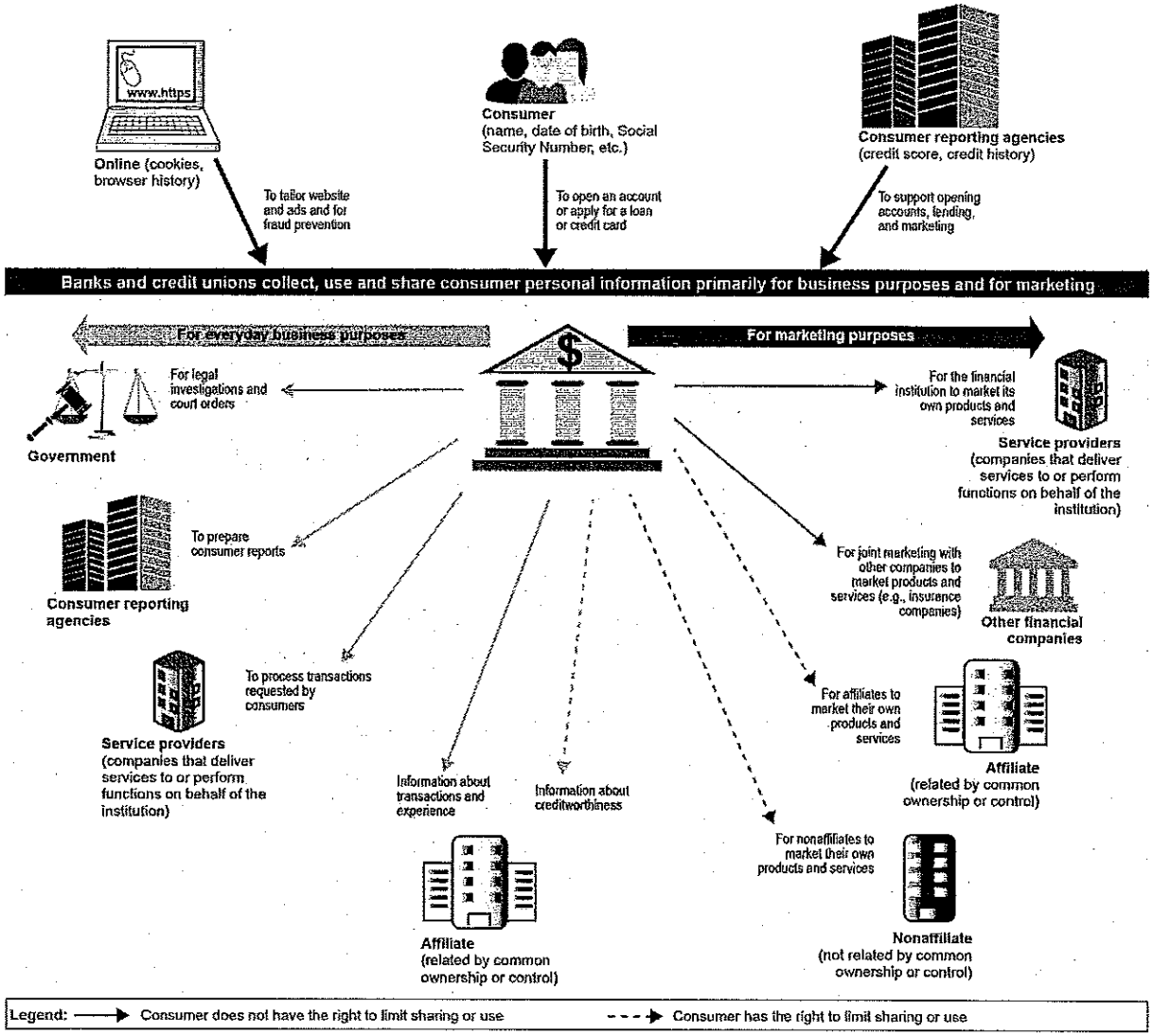


Figure 1: Summary of Bank and Credit Union Data Sharing



Source: GAO analysis of banks' and credit unions' privacy notices and related regulations. | GAO-21-36

Why Do Banks Share Your Financial Information and Are They Allowed To?

Posted on December 09, 2020

In a word: yes.

If you've ever applied for a loan, you know that banks and credit unions collect a lot of personal financial information from you, such as your income and credit history. And it's not uncommon for lenders to then share your information with other vendors, such as insurance companies after the loan is finalized. But why do banks and credit unions share your information and what protections are available to consumers to ensure their privacy?

Today's WatchBlog explores our new report on this issue. You can also tune in to our new podcast with GAO consumer protection and privacy experts Alicia Puente Cackley and Nick Marinos to learn more.

Podcast Session Image

Transcript

0:00 / 6:16

What types of information do banks collect and why?

Banks and credit unions collect and use many types of personal information to conduct everyday business activities and to market products and services. The information banks collect may be used to create bank statements, monitor for fraud, and determine credit eligibility.

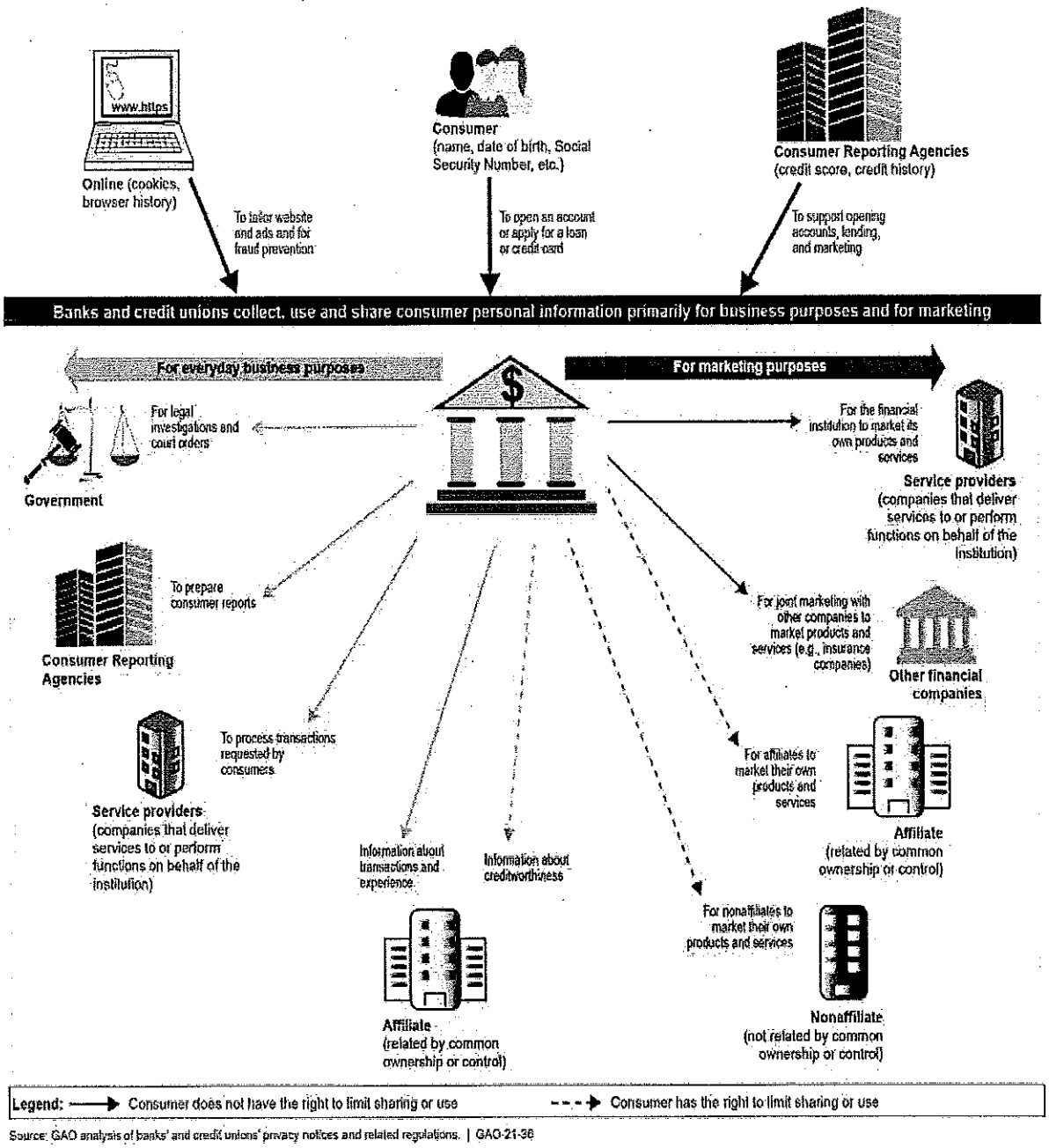
Banks and credit unions also gather information about consumers' online activities. This information may not identify an individual, but can be used for marketing. For example, when consumers access a financial institution's website and use mobile or online services, banks and credit unions collect information about their social media and browsing activities, type of computer or mobile device, and network address. Banks mainly use this information to ensure their websites function properly, detect and prevent fraud, and per our report, to tailor advertisements.

Why do banks share your information?

The personal information banks collect and share helps them approve customers for services like loans and set up accounts. But it is also helps them and their marketing partners determine whether they should offer other products and services. Banks share information with various types of third-party vendors including:

- financial companies like mortgage bankers, securities brokers-dealers, and insurance agents;

retailers (for example, home improvement stores), magazine publishers, airline companies, and direct marketers;
companies that deliver services on behalf of the lender (for example, mortgage servicers), and government agencies and nonprofits.



Source: GAO analysis of banks' and credit unions' privacy notices and related regulations. | GAO-21-36

Are they allowed to share your information?

Again, the answer is yes. But, banks and credit unions are also required to have processes in place to protect the personal information they collect, use, and share with third parties. Also, customers can opt out of having their information shared under certain conditions. The primary law that governs how financial institutions can use or share personal

information about consumers is the Gramm-Leach-Bliley Act of 1999. This law prohibits a financial institution from disclosing a consumer's nonpublic personal information like your Social Security number, income, and outstanding debt to companies that are not related to the financial institution. Consumers have the right to opt out of some, but not all, sharing of their personal information. There are exceptions. For example, banks don't have to let you opt out when transferring your information to their loan servicer.

To learn more about this topic and consumer protections, check out our report. And to learn more about our portfolio of work on this topic check out our key issues page on Consumer Financial Protections.

Comments on GAO's WatchBlog? Contact blog@gao.gov.

Topics

Business Regulation and Consumer Protection **Information Security**

Consumer Financial Protection Bureau | Consumer protection | Consumer protection laws | Cybersecurity | Banking | Banking law | Financial Markets and Community Investment | Information Technology and Cybersecurity

GAO Contacts

Alicia Puente Cackley
Director
cackleya@gao.gov
(202) 512-8678