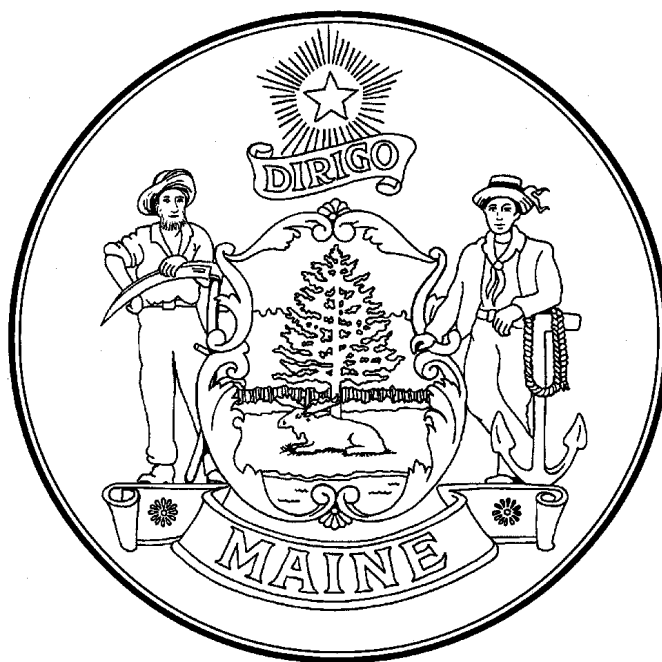


MAINE STATE LEGISLATURE

The following document is provided by the
LAW AND LEGISLATIVE DIGITAL LIBRARY
at the Maine State Law and Legislative Reference Library
<http://legislature.maine.gov/lawlib>



Reproduced from scanned originals with text recognition applied
(searchable text may contain some errors and/or omissions)

**132nd Maine State Legislature
Committee Activity**

Committee: Judiciary

LD: 1822

Title: An Act to Enact the Maine Online Data Privacy Act

Public Hearing(s): 05/05/25 10:00 AM

Work Session(s): 05/14/25 1:00 PM
05/23/25 9:30 AM
05/30/25 1:00 PM

Reported Out: 06/13/2025

Committee Report(s): OTP-AM
OTP-AM
ONTP

Committee History: 5/14/2025 1:37:00 PM Work Session Held
5/23/2025 8:14:14 AM Work Session Held
5/30/2025 8:22:00 AM Work Session Held
5/30/2025 8:22:13 AM Voted



132nd MAINE LEGISLATURE

FIRST SPECIAL SESSION-2025

Legislative Document

No. 1822

H.P. 1220

House of Representatives, April 29, 2025

An Act to Enact the Maine Online Data Privacy Act

Reference to the Committee on Judiciary suggested and ordered printed.

A handwritten signature in cursive script that reads "R B. Hunt".

ROBERT B. HUNT
Clerk

Presented by Representative KUHN of Falmouth.
Cosponsored by Senator CARNEY of Cumberland and
Representatives: Speaker FECTEAU of Biddeford, LEE of Auburn, MOONEN of Portland,
SATO of Gorham, SINCLAIR of Bath.

1 Be it enacted by the People of the State of Maine as follows:

2 Sec. 1. 10 MRSA c. 1057 is enacted to read:

3 **CHAPTER 1057**

4 **MAINE ONLINE DATA PRIVACY ACT**

5 **§9601. Short title**

6 This chapter may be known and cited as "the Maine Data Privacy and Protection Act."

7 **§9602. Definitions**

8 As used in this chapter, unless the context otherwise indicates, the following terms
9 have the following meanings.

10 **1. Affiliate.** "Affiliate" means a person that, directly or indirectly through one or more
11 intermediaries, controls, is controlled by or is under common control with another person,
12 such that the person:

13 A. Owns or has the power to vote more than 50% of the outstanding shares of any
14 voting class of the other person's securities;

15 B. Has the power to elect or influence the election of a majority of the directors,
16 members or managers of the other person;

17 C. Has the power to direct the management of the other person; or

18 D. Is subject to the other person's exercise of the powers described in paragraph A, B
19 or C.

20 **2. Authenticate.** "Authenticate" means to use reasonable means to determine that a
21 request to exercise a consumer right in accordance with section 9606 is being made by, or
22 on behalf of, a consumer who is entitled to exercise the consumer right with respect to the
23 personal data at issue.

24 **3. Biometric data.** "Biometric data":

25 A. Means data generated by automatic measurements of the biological characteristics
26 of a consumer that can be used to uniquely authenticate a consumer's identity, including
27 a fingerprint, a voiceprint, an image of a retina or iris and any other biological
28 characteristic that can be used to uniquely authenticate a consumer's identity; and

29 B. Does not include a digital or physical photograph, an audio or video recording or
30 any data generated from a digital or physical photograph or an audio or video recording,
31 unless the data is generated to identify a specific consumer.

32 **4. Business associate.** "Business associate" has the same meaning as in HIPAA.

33 **5. Child.** "Child" means an individual who has not attained 13 years of age.

34 **6. Collect.** "Collect" means to purchase, rent, gather, obtain, receive, access or
35 otherwise acquire personal data.

36 **7. Consent.** "Consent":

1 A. Means a clear affirmative act signifying a consumer's freely given, specific,
2 informed and unambiguous agreement to allow the processing of personal data relating
3 to the consumer for a particular purpose. "Consent" may include a written statement,
4 including by electronic means, or any other unambiguous affirmative action; and

5 B. Does not include:

6 (1) Acceptance of a general or broad terms of use document or similar document
7 that contains descriptions of personal data processing along with other unrelated
8 information;

9 (2) Hovering over, muting, pausing or closing a piece of content; or

10 (3) Agreement obtained through the use of a dark pattern.

11 **8. Consumer. "Consumer":**

12 A. Means an individual who is a resident of this State; and

13 B. Does not include an individual acting in a commercial or employment context or an
14 individual acting as an employee, owner, director, officer or contractor of a company,
15 partnership, sole proprietorship, nonprofit organization or government entity whose
16 communications or transactions with a controller occur solely within the context of the
17 individual's role with the company, partnership, sole proprietorship, nonprofit
18 organization or government entity.

19 **9. Consumer health data.** "Consumer health data" means personal data that a
20 controller uses to identify a consumer's physical or mental health status, and includes, but
21 is not limited to, data related to gender-affirming health care services and reproductive
22 health care services.

23 **10. Control. "Control" means:**

24 A. Ownership of, or the power to vote, more than 50% of the outstanding shares of
25 any class of voting security of a person;

26 B. Control in any manner over the election of a majority of the directors of a person
27 or of individuals exercising similar functions in a business; or

28 C. Power to exercise controlling influence over the management of a person.

29 **11. Controller.** "Controller" means a person that, alone or jointly with other persons,
30 determines the purpose and means of processing personal data.

31 **12. Covered entity.** "Covered entity" has the same meaning as in HIPAA.

32 **13. Dark pattern.** "Dark pattern" means a user interface designed or manipulated with
33 the substantial effect of subverting user autonomy, decision making or choice and includes,
34 but is not limited to, any practice the Federal Trade Commission refers to as a "dark
35 pattern."

36 **14. De-identified data.** "De-identified data" means data that cannot reasonably be used
37 to infer information about or otherwise be linked to an identified or identifiable consumer,
38 or a device that may be linked to an identified or identifiable consumer, if the controller
39 that possesses the data:

40 A. Takes reasonable measures to ensure that the de-identified data cannot be linked
41 with a consumer;

1 B. Commits in a publicly available terms and conditions document or in a publicly
2 available privacy policy to maintain and use the data in its de-identified format; and

3 C. Contractually obligates recipients of the data to satisfy the criteria and commitments
4 in paragraphs A and B.

5 **15. Decisions that produce legal or similarly significant effects concerning the**
6 **consumer.** "Decisions that produce legal or similarly significant effects concerning the
7 consumer" means decisions that result in the provision or denial to the consumer of
8 financial or lending services; housing; insurance; education enrollment or opportunity;
9 criminal justice; employment opportunities; health care services; or access to essential
10 goods or services.

11 **16. Familial status.** "Familial status" has the same meaning as in Title 5, section 4553,
12 subsection 5-A.

13 **17. Gender identity.** "Gender identity" has the same meaning as in Title 5, section
14 4553, subsection 5-C.

15 **18. Gender-affirming health care services.** "Gender-affirming health care services"
16 has the same meaning as in Title 14, section 9002, subsection 4.

17 **19. Genetic data.** "Genetic data" means any data, regardless of its format, that
18 concerns a consumer's genetic characteristics. "Genetic data" includes, but is not limited
19 to:

20 A. Raw sequence data that results from sequencing of a consumer's complete extracted
21 deoxyribonucleic acid, or DNA, or a portion of the consumer's DNA;

22 B. Information extrapolated, derived or inferred from analyzing the raw sequence data
23 under paragraph A, including, but not limited to, genotypic and phenotypic
24 information; and

25 C. Self-reported health information submitted to a direct-to-consumer genetic testing
26 company by a consumer regarding the consumer's health conditions that is used for
27 scientific research or product development and analyzed in connection with the
28 consumer's raw sequence data.

29 **20. Geofence.** "Geofence" means technology that establishes or monitors a virtual
30 geographic perimeter around a specific physical location through the use of global
31 positioning system coordinates, cellular tower connectivity, cellular data, radio frequency
32 identification, wireless access point data or any other form of location detection
33 technology.

34 **21. HIPAA.** "HIPAA" means the federal Health Insurance Portability and
35 Accountability Act of 1996, 42 United States Code, Chapter 7, Subchapter XI, Part C, and
36 the regulations, rules, guidance and exemptions adopted pursuant to that Act.

37 **22. Identified or identifiable consumer.** "Identified or identifiable consumer" means
38 a consumer who can readily be identified, either directly or indirectly.

39 **23. Institution of higher education.** "Institution of higher education" means a person
40 that is licensed or accredited to offer one or more programs of postsecondary education
41 leading to one or more degrees.

1 **24. Personal data.** "Personal data" means information that is linked or can be
2 reasonably linked to an identified or identifiable consumer or that is linked or reasonably
3 can be linked to a device that is linked or reasonably can be linked to an identified or
4 identifiable consumer. "Personal data" does not include de-identified data or publicly
5 available information.

6 **25. Physical or mental disability.** "Physical or mental disability" has the same
7 meaning as in Title 5, section 4553, subsection 7-A.

8 **26. Precise geolocation data.** "Precise geolocation data":

9 A. Means information derived from technology that can precisely and accurately
10 identify the specific location of a Consumer within a radius of 1,750 feet. "Precise
11 geolocation data" includes global positioning system level latitude and longitude
12 coordinates or data from other similar mechanisms; and

13 B. Does not include the content of communications, data generated by or connected to
14 advanced utility metering infrastructure systems or data generated by equipment used
15 by a utility.

16 **27. Process.** "Process" means any operation or set of operations performed on personal
17 data or on sets of personal data by manual or automated means, including the use, storage,
18 disclosure, analysis, deletion or modification of personal data.

19 **28. Processor.** "Processor" means a person that processes personal data on behalf of
20 a controller.

21 **29. Profiling.** "Profiling" means any form of automated process performed on personal
22 data to evaluate, analyze or predict personal aspects related to an identified or identifiable
23 consumer's economic situation, health, demographic characteristics, personal preferences,
24 interests, reliability, behavior, location or movements.

25 **30. Protected health information.** "Protected health information" has the same
26 meaning as in HIPAA.

27 **31. Publicly available information.** "Publicly available information":

28 A. Means information about a consumer that a person:

29 (1) Lawfully obtains from a record of a governmental entity;

30 (2) Reasonably believes has been lawfully made available to the general public by
31 the consumer or by widely distributed media; or

32 (3) Obtains from a person to whom the consumer disclosed the information unless
33 the consumer has restricted the information to a specific audience; and

34 B. Does not include:

35 (1) Any obscene visual depiction as described in 18 United States Code, Section
36 1460;

37 (2) Biometric data;

38 (3) Genetic data, unless the genetic data has been made available to the general
39 public by the consumer;

1 (4) Inferences derived from a combination of publicly available information and
2 other personal data; or

3 (5) Intimate images a controller or processor knows have been created or shared
4 without consent of the consumer depicted in the images. For purposes of this
5 subparagraph, "intimate image" means a photograph, videotape, film or digital
6 recording of a consumer in a state of nudity or engaged in a sexual act or engaged
7 in sexual contact for which there is no public or newsworthy purpose.

8 **32. Reproductive health care services.** "Reproductive health care services" has the
9 same meaning as in Title 14, section 9002, subsection 9.

10 **33. Sale of personal data.** "Sale of personal data":

11 A. Means the exchange of personal data for monetary or other valuable consideration
12 by a controller, processor or affiliate of a controller or processor to a 3rd party; and

13 B. Does not include:

14 (1) The disclosure of personal data to a processor that processes the personal data
15 on behalf of the controller if the processing of the personal data is limited to the
16 controller's processing purpose;

17 (2) The disclosure of personal data to a 3rd party for purposes of providing a
18 product or service affirmatively requested by the consumer;

19 (3) The disclosure of personal data to an affiliate of the controller;

20 (4) The disclosure of personal data when the consumer directs the controller to
21 disclose the personal data or intentionally uses the controller to interact with a 3rd
22 party;

23 (5) The disclosure of personal data that the consumer:

24 (a) Intentionally made available to the general public via mass media; and

25 (b) Did not restrict to a specific audience; or

26 (6) The disclosure of personal data to a 3rd party as an asset that is part of an actual
27 or proposed merger, acquisition, bankruptcy or other transaction in which the 3rd
28 party assumes control of all or part of the controller's assets.

29 **34. Sensitive data.** "Sensitive data" means personal data that includes:

30 A. Data revealing racial or ethnic origins, religious beliefs, consumer health data,
31 sexual activity, sexual orientation, gender identity, national origin or citizenship or
32 immigration status;

33 B. Genetic data or biometric data;

34 C. Personal data of a consumer that the controller knows or should know is a minor;

35 D. Precise geolocation data;

36 E. A social security number, driver's license number or nondriver identification card
37 number;

38 F. Billing, financial or payment method information, except that "sensitive data" does
39 not include the last 4 digits of a debit card or credit card number;

1 G. Account or device log-in credentials or security or access codes, including
2 passwords, for an account or device; or

3 H. Data concerning a consumer's status as a victim of a crime. For the purposes of this
4 paragraph, "victim" has the same meaning as in Title 17-A, section 2101, subsection 2.

5 **35. Sex.** "Sex" has the same meaning as in Title 5, section 4572-A, subsection 1.

6 **36. Sexual orientation.** "Sexual orientation" has the same meaning as in Title 5,
7 section 4553, subsection 9-C.

8 **37. Targeted advertising.** "Targeted advertising":

9 A. Means displaying advertisements to a consumer or on a device identified by a unique
10 identifier when the advertisement is selected based on personal data obtained or
11 inferred from the consumer's activities over time and across nonaffiliated websites or
12 online applications that are unaffiliated with each other in order to predict the
13 consumer's preferences or interests; and

14 B. Does not include:

15 (1) Advertisements based on the context of a consumer's current search query or
16 visit to a website or online application;

17 (2) Advertisements based on a consumer's activities within a controller's own
18 websites or online applications;

19 (3) Advertisements directed to a consumer in response to the consumer's request
20 for information or feedback; or

21 (4) Processing personal data solely to measure or report advertising frequency,
22 performance or reach.

23 **38. Third party.** "Third party" means a person other than the consumer, controller,
24 processor or affiliate of the controller or processor of particular personal data.

25 **39. Trade secret.** "Trade secret" has the same meaning as in section 1542, subsection
26 4.

27 **§9603. Applicability**

28 **1. Effective date.** The requirements of this chapter take effect on July 1, 2026.

29 **2. Persons affected.** The provisions of this chapter apply to persons that conduct
30 business in this State or persons that produce products or services that are targeted to
31 residents of this State and that during the preceding calendar year:

32 A. Controlled or processed the personal data of not less than 35,000 consumers,
33 excluding personal data controlled or processed solely for the purpose of completing a
34 payment transaction; or

35 B. Controlled or processed the personal data of not less than 10,000 consumers and
36 derived more than 20% of gross revenue from the sale of personal data.

37 **§9604. Exceptions**

38 **1. Exempt entities.** The provisions of this chapter do not apply to:

39 A. A body, authority, board, bureau, commission, district or agency of this State, a
40 political subdivision of this State or a federally recognized Indian tribe in this State;

1 B. An organization that is exempt from taxation under Section 501(c)(3), Section
2 501(c)(4), Section 501(c)(6) or Section 501(c)(12) of the United States Internal
3 Revenue Code of 1986, as amended;
4 C. An institution of higher education;
5 D. A national securities association that is registered under the federal Securities
6 Exchange Act of 1934, 15 United States Code, Section 78a et seq.;
7 E. A supervised financial organization or a service corporation. For purposes of this
8 paragraph, "supervised financial organization" has the same meaning as in Title 9-A,
9 section 1-301, subsection 38-A and "service corporation" has the same meaning as in
10 Title 9-B, section 131, subsection 37;
11 F. A health care facility, a health care practitioner or an affiliate of a health care facility
12 or health care practitioner that qualifies both as a business associate of that health care
13 facility or health care practitioner and provides services only to covered entities. For
14 purposes of this paragraph, "health care facility" and "health care practitioner" have the
15 same meaning as in Title 22, section 1711-C, subsection 1, paragraphs D and F,
16 respectively;
17 G. A person or entity that qualifies as a licensee under Title 24-A, section 2263,
18 subsection 8, to the extent the person or entity is in compliance with any applicable
19 data security and data privacy requirements of Title 24-A; or
20 H. A person or entity that is a provider of broadband Internet access service as defined
21 in Title 35-A, section 9301, but only to the extent that the person or entity is providing
22 broadband Internet access service.
23 **2. Exempt data.** The provisions of this chapter do not apply to:
24 A. Nonpublic personal information regulated under and collected, processed, sold or
25 disclosed in accordance with the requirements of the federal Gramm-Leach-Bliley Act,
26 15 United States Code, Section 6801 et seq. (1999);
27 B. Protected health information;
28 C. Patient-identifying information as described in 42 United States Code, Section
29 290dd-2;
30 D. Identifiable private information used for the purposes of the federal policy for the
31 protection of human subjects in research under 45 Code of Federal Regulations, Part
32 46;
33 E. Identifiable private information to the extent that it is collected as part of human
34 subjects in research pursuant to the good clinical practice guidelines issued by the
35 International Council for Harmonisation of Technical Requirements for
36 Pharmaceuticals for Human Use or successor organization or in accordance with the
37 standards for the protection of human subjects in research under 21 Code of Federal
38 Regulations, Parts 50 and 56;
39 F. Personal data used or shared in research, as defined in 45 Code of Federal
40 Regulations, Section 164.501, that is conducted in accordance with the standards set
41 forth in paragraphs D and E, or other research conducted in accordance with applicable
42 law;

1 G. Information and documents created for purposes of the federal Health Care Quality
2 Improvement Act of 1986, 42 United States Code, Section 11101 et seq.;

3 H. Information derived from health care-related information listed in this subsection
4 that is de-identified in accordance with the requirements for de-identification pursuant
5 to HIPAA;

6 I. Information that originates from information described in paragraphs B to H, or
7 information that is intermingled so as to be indistinguishable from information
8 described in paragraphs B to H, that a covered entity, business associate or program or
9 activity relating to substance use disorder as described in 42 United States Code,
10 Section 290dd-2, creates, processes or maintains in the same manner as is required
11 under the applicable laws and regulations cited in paragraphs B to H;

12 J. Information used for public health activities and purposes as authorized by HIPAA;

13 K. The collection, maintenance, disclosure, sale, communication or use of personal
14 information bearing on a consumer's creditworthiness, credit standing, credit capacity,
15 character, general reputation, personal characteristics or mode of living by a consumer
16 reporting agency, furnisher or user that provides information for use in a consumer
17 report, and by a user of a consumer report, but only to the extent that such activity is
18 regulated by and authorized under the federal Fair Credit Reporting Act, 15 United
19 States Code, Section 1681 et seq.;

20 L. Personal data collected, processed, sold or disclosed in compliance with the federal
21 Driver's Privacy Protection Act of 1994, 18 United States Code, Section 2721 et seq.;

22 M. Personal data regulated by the federal Family Educational Rights and Privacy Act
23 of 1974, 20 United States Code, Section 1232g et seq.;

24 N. Personal data collected, processed, sold or disclosed in compliance with the federal
25 Farm Credit Act of 1971, 12 United States Code, Section 2001 et seq.;

26 O. Data processed or maintained:

27 (1) In the course of an individual's applying to, being employed by or acting as an
28 agent or independent contractor of a controller, processor or 3rd party, to the extent
29 that the data is collected and used within the context of that role;

30 (2) As the emergency contact information of an individual under this chapter used
31 for emergency contact purposes; or

32 (3) That is necessary to retain to administer benefits for another individual relating
33 to the individual who is the subject of the information under subparagraph (1) and
34 used for the purposes of administering those benefits; or

35 P. Personal data collected, processed, sold or disclosed in relation to price, route or
36 service, as such terms are used in the federal Airline Deregulation Act of 1978, 49
37 United States Code, Section 40101 et seq., by an air carrier subject to that Act, to the
38 extent this chapter is preempted by the federal Airline Deregulation Act of 1978, 49
39 United States Code, Section 41713.

40 **3. Compliance with COPPA.** Controllers and processors that comply with the
41 verifiable parental consent requirements of the federal Children's Online Privacy Protection
42 Act of 1998, 15 United States Code, Section 6501 et seq., and the regulations, rules,

1 guidance and exemptions adopted pursuant to that Act are compliant with an obligation to
2 obtain parental consent pursuant to this chapter.

3 **§9605. Consumer health data**

4 **1. Confidentiality.** A person may not provide an employee or a contractor access to
5 consumer health data unless:

6 A. The employee or contractor is subject to a contractual or statutory duty of
7 confidentiality; or

8 B. Confidentiality is required as a condition of employment of the employee.

9 **2. Processor duties.** A person may not provide a processor access to consumer health
10 data unless the person providing access to the consumer health data and the processor
11 comply with section 9609.

12 **3. Geofence.** A person may not use a geofence to establish a virtual perimeter that is
13 within 1,750 feet of any facility that provides in-person health care services for the purpose
14 of identifying, tracking or collecting data from or for the purpose of sending any
15 notification to a consumer regarding the consumer's health data. This subsection does not
16 prohibit the operator of a facility that provides in-person health care services from using a
17 geofence around the facility.

18 **§9606. Consumer rights**

19 **1. Consumer rights.** A consumer has the right to:

20 A. Confirm whether a controller is processing the consumer's personal data;

21 B. If a controller processes a consumer's personal data, access the consumer's personal
22 data;

23 C. Correct inaccuracies in the consumer's personal data, taking into account the nature
24 of the personal data and the purposes of the processing of the consumer's personal data;

25 D. Require a controller to delete personal data provided by, or obtained about, the
26 consumer unless retention of the personal data is required by law;

27 E. When processing of personal data is done by automatic means, obtain a copy of the
28 consumer's personal data processed by the controller in a portable and, to the extent
29 technically feasible, readily usable format that allows the consumer to transmit the data
30 to another controller easily and without hindrance;

31 F. Obtain a list of the 3rd parties to which the controller has sold the consumer's
32 personal data or, if the controller does not maintain information about the 3rd parties
33 to which the controller has sold the personal data of the specific consumer, obtain a list
34 of the 3rd parties to which the controller has sold any consumer's personal data; and

35 G. Opt out of the processing of the consumer's personal data for purposes of:

36 (1) Targeted advertising;

37 (2) The sale of personal data; or

38 (3) Profiling in furtherance of solely automated decisions that produce legal or
39 similarly significant effects concerning the consumer.

1 **2. Exception; trade secrets.** This section may not be construed to require a controller
2 to reveal a trade secret.

3 **3. Exercise of consumer rights.** This subsection governs exercise of the consumer
4 rights established in subsection 1.

5 A. A controller shall establish a secure and reliable method for a consumer to exercise
6 a consumer right under this section.

7 B. A consumer may exercise a consumer right under this section using the method
8 established by the controller under paragraph A.

9 **4. Exercise of consumer rights by agent or guardian.** The following persons may
10 exercise the rights established in subsection 1 on behalf of a consumer.

11 A. A consumer may designate an agent in accordance with section 9607 to exercise the
12 consumer's right under subsection 1, paragraph G to opt out of the processing of
13 personal data.

14 B. If the consumer is a child, a parent or legal guardian may exercise the consumer's
15 rights under subsection 1.

16 C. If the consumer is subject to a guardianship, conservatorship or other protective
17 arrangement, the guardian or conservator of the consumer may exercise the consumer's
18 rights under subsection 1.

19 **5. Response to exercise of consumer rights.** Except as otherwise provided in this
20 chapter, a controller shall comply with a request by a consumer or other person authorized
21 to exercise the consumer's rights under subsection 1 as follows.

22 A. A controller shall respond to a request not later than 45 days after the controller
23 receives the request. The controller may extend the response period by a period of 45
24 days if:

25 (1) It is reasonably necessary to extend the period to complete the request based on
26 the complexity and number of the requests; and

27 (2) The controller informs the consumer of the extension and the reason for the
28 extension within the initial 45-day response period.

29 B. If a controller declines to take action regarding the request, the controller shall
30 inform the consumer without undue delay, but not later than the 45th day after receipt
31 of the request, of:

32 (1) The justification for declining to take action; and

33 (2) Instructions for how to appeal the decision.

34 C. A controller shall provide information to a consumer in response to a request, free
35 of charge, once during any 12-month period, except that, if requests from a consumer
36 or other person authorized to exercise the consumer's rights are manifestly unfounded,
37 excessive, technically infeasible or repetitive, the controller may:

38 (1) Charge the consumer a reasonable fee to cover the administrative costs of
39 complying with the request; or

40 (2) Decline to act on the request.

1 The controller bears the burden of demonstrating the manifestly unfounded, excessive,
2 technically infeasible or repetitive nature of the request.

3 D. If a controller is unable to authenticate a request to exercise a consumer right under
4 subsection 1 using commercially reasonable efforts, the controller:

5 (1) Is not required to comply with a request to initiate an action in accordance with
6 this section; and

7 (2) Shall provide notice to the consumer that the controller is unable to authenticate
8 the request to exercise the right until the consumer or other person authorized to
9 exercise the consumer's rights provides additional information reasonably
10 necessary to authenticate the consumer and the consumer's request to exercise the
11 right.

12 E. Notwithstanding paragraph D and except as provided in section 9607, a controller
13 is not required to authenticate an opt-out request.

14 F. A controller that has obtained personal data about a consumer from a source other
15 than the consumer is in compliance with a request to delete that data pursuant to
16 subsection 1, paragraph D by retaining a record of the deletion request and the
17 minimum data necessary for the purpose of ensuring that the consumer's personal data:

18 (1) Remains deleted from the controller's records; and

19 (2) Is not used for any other purpose.

20 **6. Appeals.** A controller shall establish a process in accordance with the requirements
21 of this subsection for a consumer or other person authorized to exercise the consumer's
22 rights to appeal the controller's inaction on a request within a reasonable period of time
23 after the consumer's receipt of the decision.

24 A. The appeal process must be conspicuously available and similar to the process for
25 submitting requests to initiate action pursuant to this section.

26 B. Not later than the 60th day after receipt of an appeal, a controller shall inform the
27 consumer or other person authorized to exercise the consumer's rights in writing of
28 action taken or not taken in response to the appeal, including a written explanation of
29 the reasons for the decisions.

30 C. If a controller denies an appeal, the controller shall provide the consumer with an
31 online mechanism, if available, through which the consumer or other person authorized
32 to exercise the consumer's rights may contact the Attorney General to submit a
33 complaint.

34 **§9607. Authorized agent**

35 **1. Authority to designate agent to opt out of processing.** A consumer may designate
36 another person to serve as the consumer's authorized agent, and act on the consumer's
37 behalf, to exercise the consumer's right under section 9606, subsection 1, paragraph G to
38 opt out of the processing of personal data.

39 **2. Method of designating agent.** The consumer may designate an authorized agent
40 by way of, among other methods, a technology, including, but not limited to, an Internet
41 link or a browser setting, browser extension or global device setting, indicating the
42 consumer's intent to opt out of certain processing of the consumer's data.

1 **3. Authentication of agent's opt-out request.** A controller shall comply with a
2 request received from an authorized agent to exercise the consumer's right under section
3 9606, subsection 1, paragraph G to opt out of the processing of personal data if, using
4 commercially reasonable efforts, the controller is able to authenticate:

5 A. The identity of the consumer; and

6 B. The authorized agent's authority to act on the consumer's behalf.

7 **§9608. Actions of controllers**

8 **1. Prohibitions.** A controller may not:

9 A. Collect, process or share sensitive data concerning a consumer, unless the collection
10 or processing is strictly necessary to provide or maintain a specific product or service
11 requested by the consumer;

12 B. Sell sensitive data;

13 C. Process personal data in violation of state or federal laws that prohibit unlawful
14 discrimination;

15 D. If the controller knows or reasonably should know that the consumer is a minor:

16 (1) Process personal data of the consumer for the purpose of targeted advertising;
17 or

18 (2) Sell the personal data of the consumer;

19 E. Retaliate against a consumer for exercising a consumer right granted in this chapter,
20 including by denying goods or services, charging different prices or rates for goods or
21 services or providing a different level of quality of goods or services to the consumer;

22 F. Collect, process or disclose personal data or publicly available information in a
23 manner that unlawfully discriminates in or otherwise unlawfully makes unavailable the
24 equal enjoyment of goods or services on the basis of an individual's actual or perceived
25 race, color, sex, sexual orientation or gender identity, physical or mental disability,
26 religion, ancestry, national origin, age or familial status. This paragraph does not apply
27 to the collection, processing or disclosure of personal data for:

28 (1) The purpose of self-testing to prevent or mitigate unlawful discrimination;

29 (2) The purpose of diversifying an applicant, participant or customer pool; or

30 (3) A private establishment described in 42 United States Code, Section 2000a(e);
31 or

32 G. Unless the controller obtains the consumer's consent, process personal data for a
33 purpose that is neither reasonably necessary to nor compatible with the disclosed
34 purposes for which the personal data is processed, as disclosed to the consumer.

35 **2. Duties.** A controller shall:

36 A. Limit the collection of personal data to what is reasonably necessary and
37 proportionate to provide or maintain a specific product or service requested by the
38 consumer to whom the data pertains;

39 B. Establish, implement and maintain reasonable administrative, technical and physical
40 data security practices to protect the confidentiality, integrity and accessibility of

1 personal data appropriate to the volume and nature of the personal data at issue. These
2 processes must include the disposal of personal data in accordance with a retention
3 schedule that requires the disposal of personal data by the controller when the data is
4 required to be deleted by law or when the data is no longer necessary for the purpose
5 for which the data was processed unless the consumer has consented to the retention
6 of the data for a longer period of time or retention of the data is required by law. For
7 purposes of this paragraph, "disposal of personal data" means the destruction or
8 permanent deletion of the data or other modification of the data to make the data
9 unreadable and unrecoverable; and

10 C. Provide an effective mechanism for a consumer to revoke the consumer's consent to
11 processing personal data under this section that is at least as easy to use as the
12 mechanism by which the consumer provided the consumer's consent and, upon
13 revocation of the consent, shall cease to process the data as soon as practicable, but not
14 later than 30 days after the receipt of the request.

15 **3. Exceptions; loyalty programs.** Subsection 1 and 2 may not be construed to:

16 A. Require a controller to provide a product or service that requires the processing of
17 personal data of a consumer that the controller does not collect or maintain; or

18 B. Prohibit a controller from offering a different price, rate, level, quality or selection
19 of goods or services to a consumer, including offering goods or services for no fee, if
20 the offering is in connection with a consumer's voluntary participation in a bona fide
21 loyalty, rewards, premium features, discounts or club card program, as long as the sale
22 of personal data is not a condition of participation in the program.

23 **4. Privacy notice.** A controller shall provide consumers with a reasonably accessible,
24 clear and meaningful privacy notice that includes the following information:

25 A. The categories of personal data, including sensitive data, processed by the
26 controller;

27 B. The controller's purpose for processing personal data;

28 C. How consumers may exercise their consumer rights under this chapter, including
29 how a consumer may appeal a controller's decision regarding the consumer's request
30 and how a consumer may revoke consent;

31 D. The categories of 3rd parties with which the controller shares personal data, with a
32 level of detail that enables a consumer to understand the type of, business model of or
33 processing conducted by each category of 3rd party;

34 E. The categories of personal data, including sensitive data, the controller shares with
35 any 3rd party;

36 F. The length of time the controller intends to retain each category of personal data or,
37 if it is not possible to identify the length of time, the criteria used to determine the
38 length of time the controller intends to retain each category of personal data; and

39 G. An active e-mail address or other online mechanism that a consumer may use to
40 contact the controller.

41 **5. Notice of sale of personal data, targeted advertising or profiling; opt-out**
42 **mechanism.** If a controller sells personal data to 3rd parties, processes personal data for

1 the purposes of targeted advertising or processes personal data for the purposes of profiling
2 the consumer in furtherance of decisions that produce legal or similarly significant effects
3 concerning the consumer, the controller shall clearly and conspicuously disclose the sale
4 or processing, as well as the manner in which a consumer may exercise the right to opt out
5 of the sale or processing. The disclosure required under this subsection must be
6 prominently displayed on the controller's publicly accessible website and the language used
7 must be clear, easy to understand and unambiguous.

8 **6. Method for exercising consumer rights.** A controller shall establish, and shall
9 describe in the privacy notice as required by subsection 4, paragraph C, one or more secure
10 and reliable mechanisms for a consumer to submit a request to exercise each consumer
11 right under this chapter.

12 A. The design of the secure and reliable mechanism for a consumer to submit a request
13 must take into account:

14 (1) The ways in which consumers normally interact with the controller;

15 (2) The need for secure and reliable communication of consumer requests; and

16 (3) The ability of the controller to verify the identity of a consumer making the
17 request.

18 B. A controller may not require a consumer to create a new account to exercise a
19 consumer right. A controller may require a consumer to use an existing account to
20 exercise a consumer right.

21 C. A controller may satisfy the controller's obligation under this subsection to establish
22 a secure and reliable mechanism for a consumer to exercise the right to opt out under
23 subsection 5 by:

24 (1) Providing a clear and conspicuous link on the controller's publicly accessible
25 website to a webpage that allows a consumer, an authorized agent of the consumer
26 or a person authorized by section 9606, subsection 4 to exercise the consumer's
27 rights, to opt out of any processing of the consumer's personal data for the purposes
28 of targeted advertising or profiling or any sale of personal data; or

29 (2) No later than July 1, 2026, allowing a consumer to opt out of any processing of
30 the consumer's personal data for the purposes of targeted advertising or profiling
31 or any sale of personal data through an opt-out preference signal sent, with the
32 consumer's consent, by a platform, technology or mechanism to the controller
33 indicating the consumer's intent to opt out of the processing or sale. The platform,
34 technology or mechanism:

35 (a) Must be consumer-friendly and easy to use by the average consumer;

36 (b) Must use clear, easy to understand and unambiguous language;

37 (c) Must be as consistent as possible with any other similar platform,
38 technology or mechanism required by federal or state law, rule or regulation;

39 (d) Must enable the controller to reasonably determine whether the consumer
40 is a resident of the State, which reasonable determination may be based on the
41 location associated with the consumer's Internet protocol address, and whether

1 the consumer has made a legitimate request to opt out of any such processing
2 or sale of the consumer's personal data;

3 (e) May not unfairly disadvantage another controller; and

4 (f) May not make use of a default setting but must require the consumer to
5 make an affirmative, freely given and unambiguous choice to opt out of any
6 such processing or sale of the consumer's personal data.

7 A controller that recognizes an opt-out preference signal that has been approved by the
8 laws of another state is considered to be in compliance with this paragraph.

9 D. If a consumer's decision to opt out of any processing of the consumer's personal data
10 for the purposes of targeted advertising or profiling or any sale of personal data through
11 an opt-out preference signal sent in accordance with paragraph C, subparagraph (2)
12 conflicts with the consumer's existing controller-specific privacy setting or the
13 consumer's voluntary participation in a controller's bona fide loyalty, rewards,
14 premium features, discounts or club card program, the controller may notify the
15 consumer of the conflict and provide the consumer a choice to confirm the controller-
16 specific privacy setting or participation that program.

17 **§9609. Responsibilities of processors and controllers**

18 **1. Contract required.** If a controller uses a processor to process personal data of a
19 consumer, the controller and the processor shall enter into a contract in accordance with
20 the requirements of this section that governs the processor's data processing procedures
21 with respect to processing performed on behalf of the controller.

22 A. The contract must be binding and must clearly set forth:

- 23 (1) Instructions for processing personal data;
24 (2) The nature and purpose of the processing;
25 (3) The type of personal data subject to processing;
26 (4) The duration of the processing; and
27 (5) The rights and obligations of the processor and the controller.

28 B. The contract must require that the processor:

- 29 (1) Ensure that each person processing personal data is subject to a duty of
30 confidentiality with respect to the data;
31 (2) Establish, implement and maintain reasonable administrative, technical and
32 physical data security practices to protect the confidentiality, integrity and
33 accessibility of personal data, considering the volume and nature of the personal
34 data;
35 (3) Stop processing personal data on request by the controller made in accordance
36 with a consumer's authenticated request;
37 (4) At the controller's direction, delete or return all personal data to the controller
38 as requested at the end of the provision of service, unless retention of the personal
39 data is required by law;

1 (5) On the reasonable request of the controller, make available to the controller all
2 information in the processor's possession necessary to demonstrate the processor's
3 compliance with the obligations in this chapter;

4 (6) After providing the controller an opportunity to object, engage a subcontractor
5 to assist with processing personal data on the controller's behalf only in accordance
6 with a written contract that requires the subcontractor to meet the processor's
7 obligations regarding the personal data under the processor's contract with the
8 controller;

9 (7) Allow and cooperate with reasonable assessments by the controller, the
10 controller's designated assessor or a qualified and independent assessor arranged
11 for by the processor to assess the processor's policies and technical and
12 organizational measures in support of the obligations under this chapter. An
13 assessment conducted under this subparagraph must be conducted using an
14 appropriate and accepted control standard framework and assessment procedure;
15 and

16 (8) On request of the controller, provide the controller with a report of an
17 assessment conducted under subparagraph (7).

18 **2. Processor responsibilities. A processor shall:**

19 A. Adhere to a contract with a controller and the instructions of the controller;

20 B. Assist the controller in meeting the controller's obligations under this chapter,
21 including:

22 (1) By employing appropriate technical and organizational measures as much as
23 reasonably practicable to fulfill the controller's obligation to respond to requests to
24 exercise consumer rights, considering the nature of processing and the information
25 available to the processor; and

26 (2) By assisting the controller in meeting the controller's obligations in relation to
27 the security of processing the personal data under this chapter and in relation to the
28 notification of a breach of the security of a system, as required by chapter 210-B;
29 and

30 C. Provide necessary information to enable the controller to conduct and document
31 data protection assessments as required by section 9611.

32 **3. Processing relationship liability.** This section may not be construed to relieve a
33 controller or a processor from the liabilities imposed on the controller or processor by virtue
34 of the controller's or processor's role in the processing relationship in accordance with this
35 section.

36 **4. Fact-based determination of role.** The determination of whether a person is acting
37 as a controller or a processor with respect to a specific processing of personal data is a fact-
38 based determination that depends on the context in which the personal data is being
39 processed as described in this subsection.

40 A. A person is considered to be a controller if:

41 (1) The person is not limited in the person's processing of specific personal data in
42 accordance with a controller's instructions; or

1 (2) The person fails to adhere to a controller's instructions with respect to a specific
2 processing of personal data.

3 B. A processor that continues to adhere to a controller's instructions with respect to a
4 specific processing of personal data remains a processor.

5 C. If a processor or 3rd party begins, alone or jointly with others, determining the
6 purposes and means of the processing of personal data, the processor is a controller
7 with respect to the processing and may be subject to an enforcement action under
8 section 9614.

9 **5. Controller's duties unaffected.** This section may not be construed to alter a
10 controller's obligation to limit a person's processing of personal data or to take steps to
11 ensure that a processor adheres to the controller's instructions.

12 **§9610. Third-party responsibilities**

13 **1. Notice required.** If a 3rd party intends to use or share a consumer's personal data
14 in a manner inconsistent with the disclosures made to the consumer at the time that the
15 personal data was collected, the 3rd party shall provide an affected consumer with notice
16 of the new or changed use or sharing of personal data before implementing the new or
17 changed use or sharing.

18 **2. Method of notification.** The 3rd party shall provide the notice required by
19 subsection 1 in a manner and at a time reasonably calculated to allow a consumer to
20 exercise the consumer's rights under this chapter.

21 **§9611. Data protection assessments**

22 **1. Definition.** For the purposes of this section, "processing activities that present a
23 heightened risk of harm to a consumer" means:

24 A. The processing of personal data for the purposes of targeted advertising;
25 B. The sale of personal data;
26 C. The processing of sensitive data; and
27 D. The processing of personal data for the purposes of profiling, in which the profiling
28 presents a reasonably foreseeable risk of:

29 (1) Unfair, abusive or deceptive treatment of a consumer;
30 (2) Having an unlawful disparate impact on a consumer;
31 (3) Financial, physical or reputational injury to a consumer;
32 (4) A physical or other intrusion on the solitude or seclusion, or the private affairs
33 or concerns, of a consumer, when the intrusion would be offensive to a reasonable
34 person; or
35 (5) Other substantial injury to a consumer.

36 **2. Data protection assessments required.** A controller shall conduct and document a
37 data protection assessment for each of the controller's processing activities that present a
38 heightened risk of harm to a consumer, including an assessment for each algorithm that is
39 used. A single data protection assessment may address a comparable set of processing
40 operations that include similar activities.

1 **3. Required elements.** A data protection assessment required by subsection 2 must be
2 conducted in accordance with the requirements of this subsection.

3 A. The data protection assessment must identify and weigh the benefits that may flow
4 directly and indirectly from the processing to the controller, the consumer, other
5 interested parties and the public against:

6 (1) The potential risks to the rights of the consumer associated with the processing
7 as mitigated by safeguards that may be employed by the controller to reduce these
8 risks; and

9 (2) The necessity and proportionality of processing in relation to the stated purpose
10 of the processing.

11 B. The controller shall factor into a data protection assessment:

12 (1) The use of de-identified data;

13 (2) The reasonable expectations of consumers;

14 (3) The context of the processing; and

15 (4) The relationship between the controller and the consumer whose personal data
16 will be processed.

17 **4. Disclosure to Attorney General.** The Attorney General may require that a
18 controller disclose to the Attorney General a data protection assessment that is relevant to
19 an investigation conducted by the Attorney General. The Attorney General may evaluate
20 the data protection assessment for compliance with the responsibilities set forth in this
21 chapter.

22 **5. Confidentiality.** A data protection assessment is confidential and exempt from
23 disclosure under Title 1, chapter 13 but may be used by the Attorney General in an action
24 to enforce this chapter. To the extent that any information contained in a data protection
25 assessment disclosed to the Attorney General pursuant to this section includes information
26 subject to attorney-client privilege or work product protection, the disclosure does not
27 constitute a waiver of that privilege or protection.

28 **6. Reciprocity.** If a controller conducts a data protection assessment for the purpose
29 of complying with another applicable law or regulation, the data protection assessment
30 satisfies the requirements established in this section if the data protection assessment is
31 reasonably similar in scope and effect to the data protection assessment that would
32 otherwise be conducted in accordance with this section.

33 **7. Deadlines for performing data protection assessments.** A controller shall conduct
34 and document a data protection assessment as required by this section:

35 A. Within 6 months of the date that the controller first engages in a processing activity
36 that presents a heightened risk of harm to a consumer; and

37 B. Within 6 months of making a material change to any processing activity that presents
38 a heightened risk of harm to a consumer.

39 **8. Application.** The requirement to conduct a data protection assessment under this
40 section applies only to processing activities that occur on or after July 1, 2026.

41 **§9612. De-identified data**

1 **1. Re-identification not required.** This chapter may not be construed to require a
2 controller or processor to:

3 A. Re-identify de-identified data;

4 B. Maintain data in an identifiable form; or

5 C. Collect, obtain, retain or access any data or technology in order to be capable of
6 associating an authenticated consumer request with personal data.

7 **2. Consumer requests.** This chapter may not be construed to require a controller or
8 processor to comply with an authenticated consumer rights request if the controller:

9 A. Is not reasonably capable of associating the request with the personal data, or it
10 would be unreasonably burdensome for the controller to associate the request with the
11 personal data;

12 B. Does not use the personal data to recognize or respond to the consumer who is the
13 subject of the personal data, or associate the personal data with other personal data
14 about the same consumer; and

15 C. Does not sell the personal data to a 3rd party or otherwise voluntarily disclose the
16 personal data to a 3rd party other than a processor, except as otherwise allowed in this
17 chapter.

18 **3. Contractual oversight.** A controller that discloses de-identified data shall exercise
19 reasonable oversight to monitor compliance with contractual commitments to which the
20 de-identified data is subject and shall take appropriate steps to address breaches of those
21 contractual commitments. Whether oversight is reasonable and whether steps taken to
22 address breaches of contractual commitments are appropriate depends in part on whether
23 the disclosed de-identified data would be considered sensitive data if the data were re-
24 identified.

25 **§9613. Exemptions**

26 **1. Exempt activities.** This chapter may not be construed to restrict a controller's or
27 processor's ability to:

28 A. Comply with federal laws or regulations, the laws and rules of the State or local
29 laws and ordinances;

30 B. Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or
31 summons by a federal or Maine governmental authority, including a governmental
32 authority of a federally recognized Indian tribe in the State;

33 C. Cooperate with federal, tribal or Maine law enforcement agencies concerning
34 conduct or activity that the controller or processor reasonably and in good faith believes
35 may violate federal laws or regulations, the laws and rules of the State or local laws
36 and ordinances;

37 D. Investigate, establish, exercise, prepare for or defend legal claims;

38 E. Provide a product or service specifically requested by a consumer;

39 F. Perform under a contract to which a consumer is a party, including fulfilling the
40 terms of a written warranty;

41 G. Take steps at the request of a consumer prior to entering into a contract;

1 H. Take immediate steps to protect an interest that is essential for the life or physical
2 safety of the consumer or another individual and when the processing cannot be
3 manifestly based on another legal basis;

4 I. Prevent, detect, protect against, investigate, prosecute those responsible for or
5 respond to security incidents, identity theft, fraud, harassment, malicious or deceptive
6 activities or any other type of illegal activity;

7 J. Preserve the integrity or security of systems; or

8 K. Assist another controller or processor or a 3rd party with an obligation under this
9 chapter.

10 **2. Internal use.** The obligations imposed on a controller or processor under this chapter
11 do not restrict a controller's or processor's ability to collect, use or retain personal data for
12 internal use to:

13 A. Effectuate a product recall;

14 B. Identify and repair technical errors that impair existing or intended functionality; or

15 C. Perform internal operations that:

16 (1) Are reasonably aligned with the expectations of the consumer or can be
17 reasonably anticipated based on the consumer's existing relationship with the
18 controller; or

19 (2) Are otherwise compatible with processing data to provide a product or service
20 specifically requested by a consumer or performing under a contract to which the
21 consumer is a party.

22 **3. Evidentiary privilege.** The obligations imposed on controllers or processors under
23 this chapter do not apply when compliance with this chapter by the controller or processor
24 would violate an evidentiary privilege under state law. This chapter may not be construed
25 to prevent a controller or processor from providing personal data concerning a consumer
26 to a person covered by an evidentiary privilege under state law as part of a privileged
27 communication.

28 **4. Exceptions to liability.** This subsection limits the liability of a controller, processor
29 or 3rd-party controller for violations of this chapter by other persons.

30 A. A controller or processor that discloses personal data to a processor or a 3rd-party
31 controller in compliance with this chapter has not violated this chapter if the processor
32 or 3rd-party controller that receives the personal data violates this chapter as long as:

33 (1) At the time the disclosing controller or processor disclosed the personal data,
34 the disclosing controller or processor did not have actual knowledge that the
35 receiving processor or 3rd-party controller would violate this chapter; and

36 (2) At the time the disclosing controller or processor disclosed the personal data,
37 the disclosing controller or processor was, and remained, in compliance with its
38 obligations as the discloser of the personal data.

39 B. A 3rd-party controller or processor that receives personal data from a controller or
40 processor in compliance with this chapter is not in violation of this chapter for the
41 independent misconduct of the controller or processor from which the 3rd-party
42 controller or processor received the personal data.

1 **5. Freedom of speech; freedom of the press; personal or household use.** This
2 chapter may not be construed to:

3 A. Impose an obligation on a controller or processor that adversely affects the rights
4 or freedoms of any person, including, but not limited to, the rights of any person to
5 freedom of speech or freedom to engage in political activity or the right of freedom of
6 the press guaranteed in the United States Constitution, Amendment I; or

7 B. Apply to an individual's processing of personal data in the course of the individual's
8 purely personal or household activities.

9 **6. Burden of proof.** If a controller processes personal data pursuant to an exemption
10 in this section, the controller bears the burden of demonstrating that the processing qualifies
11 for the exemption and complies with the limitations in subsection 7.

12 **7. Limitations.** Personal data processed by a controller or processor pursuant to an
13 exemption in this section may be processed only to the extent that the processing is:

14 A. Subject to reasonable administrative, technical and physical measures to protect the
15 confidentiality, integrity and accessibility of the personal data and reduce reasonably
16 foreseeable risks of harm to consumers relating to the collection, use or retention of
17 personal data;

18 B. Reasonably necessary and proportionate to the purposes listed in this section; and

19 C. Adequate, relevant and limited to what is necessary in relation to the specific
20 purposes listed in this section.

21 **8. Processing personal data pursuant to an exemption.** A person that processes
22 personal data pursuant to an exemption in this section may not be considered a controller
23 solely based on that processing of personal data.

24 **§9614. Enforcement**

25 **1. Violation as unfair trade practice; exclusive Attorney General enforcement.** A
26 violation of this chapter constitutes an unfair trade practice under the Maine Unfair Trade
27 Practices Act, except that the provisions of Title 5, section 213 do not apply to this chapter
28 and except as provided in subsection 2. The Attorney General has the exclusive authority
29 to enforce violations of this chapter under the Maine Unfair Trade Practices Act.

30 **2. Discretionary notice and right to cure.** Notwithstanding any provision of the
31 Maine Unfair Trade Practices Act to the contrary, before initiating any action under
32 subsection 1 for an alleged violation that occurs on or before April 1, 2027, if the Attorney
33 General believes that it is possible to cure the alleged violation, the Attorney General may
34 issue a notice of violation to the controller or processor that is allegedly violating this
35 chapter. If the Attorney General issues a notice of violation to a controller or processor
36 under this subsection, the Attorney General may not bring an action to enforce the violation
37 unless the controller or processor fails to cure the violation within 60 days of receiving the
38 notice of violation. The Attorney General shall consider the following factors in deciding
39 whether to issue a notice of violation under this subsection:

40 A. The number of alleged violations;

41 B. The size and complexity of the controller or processor;

42 C. The nature and extent of the controller's or processor's processing activities;

D. The likelihood of injury to the public:

E. The degree to which the alleged violations affect the safety of persons and property:

F. Whether the alleged violation was likely caused by a human or technical error; and

G. The extent to which the controller or processor has previously violated this chapter or similar laws.

Sec. 2. Report. By February 1, 2027, the Attorney General shall submit a report to the joint standing committee of the Legislature having jurisdiction over judiciary matters regarding the implementation and operation of the Maine Revised Statutes, Title 10, chapter 1057. The report must include, at a minimum, the following information:

1. The number of notices the Attorney General has issued under Title 10, section 9614, subsection 2 and the nature of the violations alleged in the notices;

2. The number of persons sent a notice described in subsection 1 that conferred with the Attorney General during the notice period described in Title 10, section 9614, subsection 2 in a manner that alleviated the need for a civil action under the Maine Unfair Trade Practices Act;

3. The number of civil actions brought by the Attorney General under the Maine Unfair Trade Practices Act to enforce violations of Title 10, chapter 1057; and

4. Any recommendations the Attorney General has for improving the operation of Title 10, chapter 1057.

The joint standing committee of the Legislature having jurisdiction over judiciary matters may report out legislation related to the report to the 133rd Legislature in 2027.

Sec. 3. Effective date. This Act takes effect July 1, 2026.

SUMMARY

This bill enacts the Maine Online Data Privacy Act, which takes effect July 1, 2026. The Act regulates the collection, use, processing, disclosure, sale and deletion of nonpublicly available personal data by a person that conducts business in this State or that produces products or services targeted to residents of this State, referred to in the Act as a "controller," if the personal data is linked or can be reasonably linked to an identified or identifiable individual who is a resident of this State, referred to in the Act as a "consumer," or is linked or reasonably can be linked to a device that is linked or reasonably can be linked to an identified or identifiable consumer. Under the Act, a controller must limit the collection and processing of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer, except that the controller must limit the collection and processing of certain sensitive data to what is strictly necessary to provide or maintain a specific product or service requested by the consumer. Under the Act, "sensitive data" includes data revealing a consumer's race or ethnic origins, religious beliefs, mental or physical health conditions or diagnoses, sexual orientation, gender identity, citizenship or immigration status; genetic or biometric data; precise geolocation data; social security, driver's license or nondriver identification card numbers; specific financial or account access information; data of a minor under 18 years of age; or data concerning the consumer's status as the victim of a crime.

1 The Act establishes that consumers have the right to confirm whether a controller is
2 processing their data; correct inaccuracies in their personal data; require the controller to
3 delete any portion of their personal data that the controller is not required to maintain by
4 law; obtain a copy of their personal data in a format that can be readily transferred to
5 another controller; obtain a list of the 3rd parties to which the controller has sold personal
6 data; and opt out of the processing of their personal data for purposes of targeted
7 advertising, sale or consumer profiling. The Act also prohibits a controller from selling
8 any sensitive data; processing the personal data of a minor for purposes of targeted
9 advertising or sale; processing personal data in a manner that discriminates against a person
10 in violation of state or federal law; and retaliating against a consumer for exercising a
11 consumer's rights under the Act, except that a controller may offer different prices or
12 selection of goods in connection with a consumer's voluntary participation in a bona fide
13 loyalty or discount program.

14 The Act also requires a controller to provide consumers with a privacy notice
15 specifying how a consumer may exercise the consumer's rights under the Act; the
16 categories of personal data processed by the controller; the purposes for processing the
17 personal data; the categories of personal data transferred to 3rd parties; and the categories
18 of 3rd parties to whom personal data is shared. The controller must establish, implement
19 and maintain reasonable data security practices and a retention schedule that requires the
20 disposal of personal data by the controller either when deletion is required by law or when
21 the data is no longer necessary for the purpose for which it was processed and retention of
22 the data is not required by law. The controller must also require, by contract, that any
23 person who processes a consumer's personal data on behalf of the controller treats the
24 personal data confidentially and deletes or returns all personal data to the controller at the
25 end of the processing, unless retention of the data is required by law. If a controller engages
26 in a data processing activity that presents a heightened risk of harm to a consumer,
27 including processing any data for targeted advertising, sale or profiling or any processing
28 of sensitive data, the controller must conduct and document a data protection assessment
29 identifying and weighing the benefits and potential risks of the processing activity. The
30 controller may be required to disclose the data protection assessment to the Attorney
31 General, who must keep it confidential, when the assessment is relevant to an investigation
32 conducted by the Attorney General.

33 The Act further prohibits any person from establishing a geofence within 1,750 feet of
34 any in-person health care facility in the State, other than the operator of the facility, for the
35 purpose of identifying, tracking, collecting data from or sending a notification regarding
36 consumer health data to consumers who enter that area.

37 The provisions of the Act do not apply to specifically enumerated persons, including
38 the State, political subdivisions of the State and federally recognized Indian tribes in the
39 State; nonprofit organizations; institutions of higher education; federally registered national
40 securities associations; supervised financial organizations and service corporations; health
41 care facilities and health care practitioners as well as their affiliates that both qualify as
42 business associates and provide services only to covered entities; state-licensed and
43 authorized insurers that are in compliance with applicable Maine laws governing insurer
44 data security and data privacy; and broadband Internet service providers to the extent those
45 providers are subject to the data privacy requirements of the Maine Revised Statutes, Title
46 35-A, section 9301. In addition, the provisions of the Act do not apply to specifically

1 enumerated types of data, including, for example: nonpublic personal information
2 regulated under the federal Gramm-Leach-Bliley Act; protected health information under
3 the federal Health Insurance Portability and Accountability Act of 1996; personal data
4 regulated by the Family Educational Rights and Privacy Act of 1974; data processed and
5 maintained by the controller regarding an applicant for employment or employee to the
6 extent the data is collected and used within the context of that role; and data necessary for
7 the controller to administer benefits.

8 The Act also does not prohibit controllers from engaging in specifically enumerated
9 activities, including, for example: complying with state or federal law; complying with
10 investigations or subpoenas from federal, state or tribal governmental authorities;
11 cooperating with federal, tribal or Maine law enforcement agencies; providing a product or
12 service specifically requested by the consumer; protecting life and physical safety of
13 consumers; and preventing or responding to security incidents. The Act also does not
14 prohibit a controller from using personal data collected in a lawful manner to effectuate a
15 product recall, identify and repair technical errors and perform internal operations that are
16 reasonably aligned with a consumer's expectations or otherwise compatible with providing
17 the product or service specifically requested by the consumer.

18 Violations of the Act may be enforced exclusively by the Attorney General under the
19 Maine Unfair Trade Practices Act. If the violation occurs on or before April 1, 2027, the
20 Attorney General may provide a potential defendant with a notice of violation at least 60
21 days prior to initiating an enforcement action, during which time the potential defendant
22 may cure the violation to avoid the enforcement action. The Act further requires the
23 Attorney General to submit a report by February 1, 2027 to the joint standing committee of
24 the Legislature having jurisdiction over judiciary matters regarding the implementation and
25 operation of the Act. The committee may report out legislation related to the report to the
26 133rd Legislature in 2027.

STATE OF MAINE
132ND LEGISLATURE

LEGISLATIVE NOTICES

JOINT STANDING COMMITTEE ON JUDICIARY

Sen. Anne Carney, Senate Chair
Rep. Amy Kuhn, House Chair

PUBLIC HEARING: Monday, May 5, 2025, 10:00 AM, State House, Room 438

- (L.D. 1284) Bill "An Act to Repeal Provisions of Law Governing the Privacy of Broadband Internet Customer Personal Information" (SP0512)
(Presented by Senator STEWART, T. of Aroostook)
- (L.D. 1088) Bill "An Act to Enact the Maine Consumer Data Privacy Act" (HP0710)
(Presented by Representative HENDERSON, R. of Rumford)
(Cosponsored by Representative ROBERTS, T. of South Berwick,
Representative POIRIER, J. of Skowhegan)
- (L.D. 1224) Bill "An Act to Comprehensively Protect Consumer Privacy" (HP0799)
(Presented by Representative ROBERTS, T. of South Berwick)
(Cosponsored by Senator BALDACCI, J. of Penobscot, Senator GUERIN,
S. of Penobscot, Senator MOORE, M. of Washington, Representative
CROCKETT, E. of Portland, Representative STOVER, H. of Boothbay,
Representative COLLAMORE, A. of Pittsfield, Representative BRIDGEO,
W. of Augusta, Representative HENDERSON, R. of Rumford,
Representative DILL, J. of Old Town)
- (L.D. 1822) Bill "An Act to Enact the Maine Online Data Privacy Act" (HP1220)
(Presented by Representative KUHN, A. of Falmouth) (Cosponsored by
Senator CARNEY, A. of Cumberland, Representative LEE, A. of Auburn,
Representative SINCLAIR, D. of Bath, Representative SATO, E. of
Gorham, Representative MOONEN, M. of Portland, Speaker FECTEAU,
R. of Biddeford)

CONTACT PERSON:

Susan Pinette
100 State House Station
Augusta, ME 04333-0100
287-1327

WORK SESSION AGENDA

JUDICIARY COMMITTEE

Wednesday, May 14, 2025

1:00 PM

State House, Room 438

- (L.D. 194) Bill "An Act to Improve the Maine Unfair Trade Practices Act" (HP0127) (Presented by Representative LEE, A. of Auburn) (Cosponsored by Senator HICKMAN, C. of Kennebec, Representative MOONEN, M. of Portland, Representative GRAMLICH, L. of Old Orchard Beach, Representative KUHN, A. of Falmouth)

- (L.D. 844) Bill "An Act to Regulate Social Media Use by Minors Under 16 Years of Age" (HP0530) (Presented by Representative FREDETTE, K. of Newport)

- (L.D. 1284) Bill "An Act to Repeal Provisions of Law Governing the Privacy of Broadband Internet Customer Personal Information" (SP0512) (Presented by Senator STEWART, T. of Aroostook)

- (L.D. 1088) Bill "An Act to Enact the Maine Consumer Data Privacy Act" (HP0710) (Presented by Representative HENDERSON, R. of Rumford) (Cosponsored by Representative ROBERTS, T. of South Berwick, Representative POIRIER, J. of Skowhegan)

- (L.D. 1224) Bill "An Act to Comprehensively Protect Consumer Privacy" (HP0799) (Presented by Representative ROBERTS, T. of South Berwick) (Cosponsored by Senator BALDACCI, J. of Penobscot, Senator GUERIN, S. of Penobscot, Senator MOORE, M. of Washington, Representative CROCKETT, E. of Portland, Representative STOVER, H. of Boothbay, Representative COLLAMORE, A. of Pittsfield, Representative BRIDGEO, W. of Augusta, Representative HENDERSON, R. of Rumford, Representative DILL, J. of Old Town)

- (L.D. 1822) Bill "An Act to Enact the Maine Online Data Privacy Act" (HP1220) (Presented by Representative KUHN, A. of Falmouth) (Cosponsored by Senator CARNEY, A. of Cumberland, Representative LEE, A. of Auburn, Representative SINCLAIR, D. of Bath, Representative SATO, E. of Gorham, Representative MOONEN, M. of Portland, Speaker FECTEAU, R. of Biddeford)

Other Bills TBD

Amendment Reviews TBD

JUDICIARY COMMITTEE

WORK SESSION AGENDA

Friday, May 23, 2025

9:30 AM

State House, Room 438

- (L.D. 1088) Bill "An Act to Enact the Maine Consumer Data Privacy Act" (HP0710)
(Presented by Representative HENDERSON, R. of Rumford)
(Cosponsored by Representative POIRIER, J. of Skowhegan,
Representative ROBERTS, T. of South Berwick)
- (L.D. 1224) Bill "An Act to Comprehensively Protect Consumer Privacy" (HP0799)
(Presented by Representative ROBERTS, T. of South Berwick)
(Cosponsored by Senator BALDACCI, J. of Penobscot, Senator MOORE,
M. of Washington, Senator GUERIN, S. of Penobscot, Representative
BRIDGEO, W. of Augusta, Representative DILL, J. of Old Town,
Representative COLLAMORE, A. of Pittsfield, Representative
CROCKETT, E. of Portland, Representative HENDERSON, R. of
Rumford, Representative STOVER, H. of Boothbay)
- (L.D. 1822) Bill "An Act to Enact the Maine Online Data Privacy Act" (HP1220)
(Presented by Representative KUHN, A. of Falmouth) (Cosponsored by
Senator CARNEY, A. of Cumberland, Representative LEE, A. of Auburn,
Representative SINCLAIR, D. of Bath, Representative SATO, E. of
Gorham, Representative MOONEN, M. of Portland, Speaker FECTEAU,
R. of Biddeford)

Other Bills TBD

Amendment Reviews TBD

FOAA Reviews TBD

CONTACT PERSON:

Susan Pinette
100 State House Station
Augusta, ME 04333-0100
287-1327

WORK SESSION AGENDA

JUDICIARY COMMITTEE

Friday, May 30, 2025

1:00 PM

State House, Room 438

- (L.D. 1088) Bill "An Act to Enact the Maine Consumer Data Privacy Act" (HP0710)
(Presented by Representative HENDERSON, R. of Rumford)
(Cosponsored by Representative POIRIER, J. of Skowhegan,
Representative ROBERTS, T. of South Berwick)
- (L.D. 1822) Bill "An Act to Enact the Maine Online Data Privacy Act" (HP1220)
(Presented by Representative KUHN, A. of Falmouth) (Cosponsored by
Senator CARNEY, A. of Cumberland, Representative LEE, A. of Auburn,
Representative SINCLAIR, D. of Bath, Representative SATO, E. of
Gorham, Representative MOONEN, M. of Portland, Speaker FECTEAU,
R. of Biddeford)

Other Bills TBD

Amendment Reviews TBD

FOAA Reviews TBD

CONTACT PERSON:

Susan Pinette
100 State House Station
Augusta, ME 04333-0100
287-1327

Heard all four bills at the same time ...

JOINT STANDING COMMITTEE ON JUDICIARY

TESTIMONY SHEET

LD or CONFIRMATION: ~~DATA Privacy~~ LDs 1284, 1088, 1224, 1822
DATE: Monday 5 May 2025

Name	Town/Affiliation	FOR	AGAINST	NEITHER
Rep. Rachel Henderson	Sponsor LD 1088	x		
Rep. Tiffany Roberts	South Berwick 1224	X		
Rep Amy Koffa	FALMOUTH LD 1822	X		
Michael Kebede	MAINE ACLU	1822	1224	
Sen. Trey Stewart	ARDOOSTOCK LD 1284	X		
Blondan O'Neil Esq	Attorney General's Office	1822	1224	
Ian Quin Marvin	SCARBOROUGH	1224		
Alex MINARD	NCTA	1284		
Alicia Rae Esq	MAINE ACLU	1822		
LAURA Harper	MAINE Family Planning	1822	1088 1224 1284	
Jan Collins	Prisoner Advocacy	1822		
Petrack Woodcock	MAINE State Chamber	1284		
Ruben Torres	Immigrants Rights Coalition	1822		
Stacy Stithem	BLANK: Isaacson	1224	1822	
Bruce Generosity	Automobile dealers			
Nate Cloutier	Hospitality Maine	1224	1822	

P. 10/2

JOINT STANDING COMMITTEE ON JUDICIARY

TESTIMONY SHEET

LD or CONFIRMATION: DATA PRIVACY LDS 1284, 1088, 1224, 1882
 DATE: Monday 5 May 2023

Name	Town/Affiliation	FOR	AGAINST	NEITHER
Curtis Picard	Retail Assn. of Maine	1224	1822	
Christy van Voonhees	LL Bean	1822		
Ellen Parent	Maine Credit Union	1224		
Josh Steikman	Maine Bankers Assn		1822	
Caitriona Fitzgerald	Epic.org	1822	1224 1088 1284	
Michael Santorelli	ALCP - NYU School			
Lisa Lavasseur	Internet Safety Lab			
Lisa Marquies	VP Planned Parenthood	1822		
Matt Schwartz	Consumer Reports			
Arielle Garcia	"Check My Ads" Institute			
Zachary Taylor	Consumer Data Industry			
Toby Landreau	Findhelp			
Kenley Joseph	Multicultural Media			
Eric Null	Center for Democracy	1822		
Andrew Kingman	State Privacy & Security			
Christopher Gilrein	Technet			
Brian Langley	Elsworth SMALL BUSINESS OWNER	1224		
Robbie McLuckie	Consumer Healthcare Products			



HOUSE OF REPRESENTATIVES

2 STATE HOUSE STATION

AUGUSTA, MAINE 04333-0002

(207) 287-1400

TTY: MAINE RELAY 711

Amy Kuhn

P.O. Box 66831

Falmouth, ME 04105

(207) 939-6903

Amy.Kuhn@legislature.maine.gov

May 5, 2025

Testimony of Representative Amy D. Kuhn introducing

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

Before the Joint Standing Committee on Judiciary

Senator Carney and distinguished members of the Judiciary Committee, my name is Amy Kuhn, and I proudly represent most of Falmouth in House District 111. It is a pleasure to be with you today to introduce **LD 1822, An Act to Enact the Maine Online Data Privacy Act**.

Life in America today is inextricably intertwined with the devices we use, the browsers we access and the apps we open. From shopping to dating, health care to banking, entertainment to travel, every swipe, scroll and click we make generates a trail of data that can be deeply revealing.

No doubt these linkings can produce convenient results. However, left unchecked, this vast trove of data makes us vulnerable to a myriad of risks, including civil rights violations, identity theft, financial exploitation and unlawful discrimination. The right to control our personal information is essential in the digital era.

Let's get specific. Why should we care about data privacy? Here are some examples:

1. Civil rights –

- Policing – Police departments can now circumvent warrant requirements by buying sensitive data directly in the marketplace. The Brennan Center reports: “The government’s ability to buy sensitive location information without judicial or legislative oversight upends the time-honored balance of power between the people and the government established by the Fourth Amendment.”¹
- Discrimination – The use of data about race and gender in Artificial Intelligence (AI) decision making algorithms has resulted in different housing and employment opportunities being presented to people based on their personal profiles. For example, a University of Chicago study found that: “Facebook’s ad algorithm used personal data to deploy targeted housing advertisements that discriminated against Black, Hispanic, and Asian users.” These practices included

¹ Federal Agencies Are Secretly Buying Consumer Data, <https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data>

assigning lower priority to certain applications or offering higher interest rates to others.² Similarly, data about gender has been used to filter job postings, often “based on historical gender stereotypes,” showing, for example, ads for mechanics more often to men and ads for preschool teachers more often to women.³

2. Risk of Breach – Cyber attacks and subsequent data breaches are ubiquitous and pose significant threats to consumers' personal and financial security.⁴ Limiting collection on the amount and sensitivity of personal data on the internet helps reduce the risk of sensitive information from falling into the wrong hands.

3. Loss of Unbiased Viewpoint – When we open our phones, we do not see an objective portrayal of the world for us to consider and evaluate. Instead, the data that is collected about us facilitates the creation of a customized reality based on how an algorithm assesses our interests. The long term implications and consequences of this are unknown.

Since 2018, many states have adopted comprehensive data privacy laws. The first wave of these laws have been consent based laws, or what has been referred to here as the Connecticut Model. This model does offer new consumer rights such as the right to request, correct and delete data that has been collected about them. However, in terms of these companies' foundational business models, these laws essentially enshrine the status quo. In short, a company can collect, process and sell any data at all, so long as their practices are disclosed in their terms and conditions page and the consumer consents. There's only one problem – who reads the terms and conditions page? Almost no one. Most people click “accept” or “allow” or whatever the prompt may be so that we can get on with whatever we want to be doing, resulting in practice in no informed consent at all.

The second wave of laws prioritize real data minimization. This sets actual limits on what data can be collected and what companies can do with it. In order to be collected, personal data must be “reasonably necessary and proportionate” to the product or service the consumer requests. Sensitive data can only be collected if it is “strictly necessary” to the product or service requested. And, sensitive data cannot be sold. This means that any sensitive data that a consumer chooses to share will stay where the consumer left it, not travel around the internet without their knowledge.

This focus on data minimization brings us real benefits – it deters the possibility of civil rights violations, it protects us in the event of breach and it creates stronger data sets for AI.

² AI is Making Housing Discrimination Easier Than Ever Before, <https://kreismaninitiative.uchicago.edu/2024/02/12/ai-is-making-housing-discrimination-easier-than-ever-before/recruitment-practices>

³ People are missing out on job opportunities on Facebook because of gender, research suggests: <https://www.cnn.com/2023/06/12/tech/facebook-job-ads-gender-discrimination-asequals-intl-cmd/index.html>

⁴ The Biggest Data Breaches in 2024: 1 Billion Stolen Records and Rising, <https://techcrunch.com/2024/10/14/2024-in-data-breaches-1-billion-stolen-records-and-rising/>

This data minimization approach was signed into law earlier this year in Maryland. Data minimization is also central to bills pending now in Massachusetts and Vermont, and in amendments pending in Connecticut.

I would like to walk you through the bill and describe some highlights so that you have landmarks in the bill for further review, including:

- P. 4 Definitions
- P. 6 Applicability
- P. 6 Exceptions
- P. 9 Consumer rights
- P. 12 Actions of controllers
- P. 13-14 Opt out of targeted advertising
- P. 17 Data protection Assessments
- P.21 Enforcement
- P.22 AG Reports

In summary, through this bill, I have sought to respect and carry over the tremendous progress that the Legislature and the business community made in the 131st while addressing the business concerns that remained at the end of session. In the 132nd, Maine has an opportunity to enact a truly robust privacy law, where we strike a balance between innovation and accountability, and foster a safer, more equitable digital ecosystem for generations to come.

I thank you for the opportunity to present this bill. I would be happy to answer any questions.



Maine Medical
Association



Spectrum
Healthcare Partners



MAINE
AMBULANCE
ASSOCIATION

Comment on Privacy Legislation

LD 595 - *An Act To Update Privacy Protections For Maine Consumers*

LD 1088 - *An Act To Enact The Maine Consumer Data Privacy Act*

LD 1244 - *An Act To Comprehensively Protect Consumer Privacy*

LD 1822 - *An Act To Enact The Maine Online Data Privacy Act*

May 5, 2025

Chair Carney, Chair Kuhn, Honorable Members of the Judiciary Committee, my name is Jeffrey Austin and on behalf of the Maine Hospital Association, my colleagues at MaineHealth and Northern Light Health and the above-named healthcare entities, I submit these comments.

I am in Washington, DC and regret that I cannot attend the hearing today.

We request that health care entities be given entity-level exemptions from this legislation for the reasons below. This testimony closely mirrors the comments we made in the Fall of 2023 as this Committee deliberated the issue at that time. I have not had the opportunity to review each of these bills as closely as I would have liked to prior to your hearing. My apologies.

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

Maine hospitals and other healthcare providers are not the identified problem by proponents of the legislation. The three examples given over and over again by proponents are internet searches, cell phone apps and wearables like smart watches which are alleged to be out of the reach of HIPAA and the other existing laws. These are commercial interactions that are not part of traditional care giving. The entities that offer these apps and watches are not recognized by law as healthcare providers. We take no position on whether they need regulation; but suffice it to say, we are not them and they are not us.

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

To be clear, exempting the data is not enough; we should receive the same kind of entity-level exemptions as government.

Please consider this request as part of your deliberations.

Any of the representatives of the above groups would be happy to speak with you about this issue.

Thank you.

**Testimony in Support of LD 1822, An Act to Enact the Maine Online Data Privacy Act
In Opposition to LDs 1088, 1224, and 1284**

Committee on Judiciary
May 5, 2025

Dear Senator Carney, Representative Kuhn, and Distinguished Members of the Committee on Judiciary,

GLBTQ Legal Advocates & Defenders (GLAD Law) is a nonprofit legal organization that works in New England and nationally to create a just society free of discrimination based on gender identity and expression, HIV status, and sexual orientation. We appreciate the opportunity to submit this testimony together with EqualityMaine and MaineTransNet in support of LD 1822 and in opposition to LDs 1088, 1224, and 1284.

LD 1822 would be a major step forward in protecting the digital privacy of all Mainers. This is an especially urgent issue for LGBTQ+ people, who face heightened risks from digital surveillance, widespread data sharing, privacy breaches, algorithm-based decision-making, and other forms of data misuse. These risks include forced outing (the disclosure of a person's sexual orientation or transgender identity without their consent), targeted healthcare surveillance, and unlawful discrimination in housing, employment, lending, and other important settings.¹

Inappropriate collection and sale of personal data related to sexual orientation, gender identity, and transgender healthcare could also aid hostile governments in enforcing anti-transgender laws against Mainers.² As explained by the Project on Government Oversight, this threat is especially apparent in the healthcare context:

A huge array of personal information is derived from our digital footprints. . . . Digital surveillance techniques have clear applications for police investigations around gender-affirming care, experts say. Law enforcement agencies can access personal data in a number of ways when conducting criminal investigations. They can get geofence warrants (which allow police to obtain location data from cellular devices within a specified geographic area), . . . and they can purchase personal data without a warrant. Experts warn that law enforcement using personal data provided by tech companies like Google, Meta, and others, could identify people who have obtained, provided, or “aided and abetted” in providing gender-affirming care.

Police could “basically do a fishing expedition for anybody who may have been, for example, near a certain clinic or near a certain community center or near a

¹ See generally Chris Wood et al., *The Role of Data Protection in Safeguarding Sexual Orientation and Gender Identity Information*, Future of Privacy Forum (2022), <https://fpf.org/wp-content/uploads/2022/06/FPF-SOGI-Report-R2-singles-1.pdf>.

² See generally René Kladzyk, *Policing Gender: How Surveillance Tech Aids Enforcement of Anti-Trans Laws*, Project on Government Oversight (June 28, 2023), <https://www.pogo.org/investigations/policing-gender-how-surveillance-tech-aids-enforcement-of-anti-trans-laws>.

certain medical facility at a certain time, and use that as evidence as they're building their case," according to [Hayley] Tsukayama of the Electronic Frontier Foundation.³

Similar risks apply in the reproductive healthcare setting.⁴ Without comprehensive privacy protections in place, the risk that health data can be collected and sold to law enforcement in other jurisdictions, without patient consent, means that Mainers cannot fully and freely exercise their rights to aid or engage in legally protected healthcare activity.

More broadly, the fear that sensitive health information could be tracked, disclosed, or misused may cause LGBTQ+ individuals to delay or avoid seeking necessary healthcare, including gender-affirming and reproductive healthcare services, which undermines public health as well as individual wellbeing.⁵

LD 1822 protects against these risks. In addition to providing robust privacy protections for all forms of personal data, LD 1822 includes specific restrictions on the collection, processing, and sale of data revealing consumers' sexual orientation, gender identity, and location history. LD 1822 also imposes limits on geofencing around healthcare facilities. And it prohibits corporations from processing personal data in an unlawfully discriminatory manner, ensuring that algorithms and artificial intelligence are not used to exclude or harm Mainers because of their sexual orientation, gender identity, sex, or any other protected characteristic.

In sum, LD 1822 is an important step to prevent Mainers' most personal data from being misused for surveillance and discrimination, and it is necessary to protect LGBTQ+ Mainers from the unique risks they face. GLAD Law respectfully urges this committee to support this important legislation.

By contrast, LDs 1088, 1224, and 1284 would enable the kind of data collection, processing, and disclosure practices that threaten the privacy, safety, and wellbeing of LGBTQ+ Mainers. GLAD Law asks that this committee vote "ought not to pass" on these three bills.

Sincerely,
Mary Bonauto, Sarah Austin, and Hannah Hussey
GLBTQ Legal Advocates & Defenders, Portland, Maine
Bre Danvers-Kidman, MaineTransNet
Heide Lester, EqualityMaine

³ *Id.*

⁴ See, e.g., Joseph Cox, *Location Data Firm Provides Heat Maps of Where Abortion Clinic Visitors Live*, Vice (May 5, 2022), <https://www.vice.com/en/article/location-data-firm-heat-maps-planned-parenthood-abortion-clinics-placerai/>.

⁵ Cf. HIPAA Privacy Rule to Support Reproductive Health Care Privacy, 89 Fed. Reg. 32976, 32978 (Apr. 26, 2024).

**LEGAL SERVICES
FOR MAINE ELDERS**

In Support of LD 1822 — An Act to Enact the Maine Online Data Privacy Act
Before the Joint Standing Committee on Judiciary

Testimony of John Brautigam, Esq. for Legal Services for Maine Elders
Joint Standing Committee on Judiciary

May 13, 2025

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

My name is John Brautigam, and I offer this belated testimony on behalf of Legal Services for Maine Elders. LSE provides free legal help for Mainers aged 60 and older when their basic human needs are at stake.

We are living through a moment of profound transformation in our digital ecosystem. The ways we interact, access services, and share personal information have shifted dramatically — and often invisibly — to online platforms, apps, and data-driven systems. In this new environment, vast quantities of personal data are routinely collected, shared, and monetized, frequently without the full understanding or consent of the individuals to whom that data belongs. This transition is occurring faster than many legal frameworks can respond, and in the absence of meaningful protections, consumers — particularly vulnerable individuals — are exposed to serious risks. LD 1822 represents a thoughtful and urgent response to this reality, ensuring that Maine residents, including older adults, are not left behind in the digital age.

Protecting Older Mainers from Digital Exploitation

Older Maine residents are disproportionately targeted by online scams, fraudulent marketing schemes, and predatory data practices. These threats have grown more sophisticated as personal information has become a valuable — and easily traded — commodity in the unregulated corners of the digital economy.

LD 1822 takes meaningful steps to push back against that trend:

- By **limiting the collection of sensitive data** to what is strictly necessary for a requested service, the bill closes off avenues by which malicious actors can gather and exploit highly personal information such as health status, biometric identifiers, or financial account access.

LEGAL SERVICES FOR MAINE ELDERS, INC.
5 Wabon Street, Augusta, Maine 04333
(207) 621-0087 Fax (207) 621-0742
Offices in Augusta, Bangor, Lewiston, Biddeford and Presque Isle
LSE Helpline 1-800-750-5353 (Voice/TTY)
www.mainelse.org

- By **prohibiting the sale of sensitive data altogether**, and by **barring the use of personal data for discriminatory purposes**, the bill addresses structural risks that have emerged from the widespread and largely opaque collection of consumer data.
- By **empowering consumers with rights to access, correct, delete, and control their personal information**, LD 1822 gives older Mainers new tools to protect their dignity, safety, and autonomy in an increasingly complex digital world.

Addressing Risks Unique to Aging Populations

LD 1822 is especially significant for older adults living with physical or cognitive impairments, or those who have been victims of crimes — including financial exploitation, which remains one of the fastest-growing forms of elder abuse.

In a digital environment where data can be captured and analyzed without a person ever clicking a button or filling out a form, the need for legal protections is no longer optional — it is essential.

The bill's **definition of sensitive data** includes precisely the types of information that older adults most need to keep private: mental or physical health conditions, crime victim status, and precise geolocation data.

The prohibition on **geofencing near medical facilities** is particularly commendable. It helps shield consumers — including older adults seeking care — from being tracked, profiled, or manipulated based on their presence at health care locations. As digital surveillance technologies advance, this kind of forward-looking legal boundary is vital.

Implementation and Accessibility Considerations

We appreciate that LD 1822 is carefully crafted to balance meaningful privacy protections with reasonable business obligations. But for these rights to be truly effective in practice — especially for older Mainers — attention must be given to accessibility, equity, and enforcement.

As the Attorney General implements and oversees enforcement of this law, we respectfully encourage the following:

- That **public education efforts** include accessible materials for older residents who may not be digitally fluent, including written guides, printed notices, or outreach through community-based organizations.
- That regulators consider **clarifying procedures** for legally authorized representatives — such as individuals with powers of attorney or guardianship — to exercise a consumer's rights under the Act, especially for those with diminished capacity.
- That enforcement prioritize cases where vulnerable consumers, including older adults, are at the greatest risk of harm from misuse or sale of their data.

Conclusion

May 13, 2025

Legal Services for Maine Elders – LD 1822

Page 3

LD 1822 is a forward-looking, thoughtful framework that puts privacy and dignity back in the hands of Maine residents. It recognizes that we are no longer living in a world where privacy can be assumed — and that responsible, rights-based legal frameworks are needed to restore balance and trust.

For older Mainers — who are too often targeted, overlooked, or left behind by fast-changing digital systems — this bill provides critical safeguards and long-overdue protections.

On behalf of LSE and the older people we serve across the state, I respectfully urge the Committee to vote **Ought to Pass** on LD 1822.

Thank you.



Janet T. Mills
Governor

Michael J. Sauschuck
Commissioner

STATE OF MAINE
Department of Public Safety
MAINE STATE POLICE

45 Commerce Drive - Suite 1
Augusta, Maine 04333



William Ross
Colonel

LTC. Brian P. Scott
Deputy Chief

Testimony of Lieutenant Mathew Casavant
Maine State Police
Neither For Nor Against (1822)

An Act to Enact the Maine Online Data Privacy Act

Sponsored by Representative Kuhn
Committee on Judiciary

Senator Carney, Representative Kuhn, and other distinguished members of the joint standing committee on Judiciary, my name is Lieutenant Mathew Casavant, and I am here to represent the Maine State Police and the Maine Department of Public Safety to testify neither for nor against LD 1822, "An Act to Enact the Maine Online Data Privacy Act."

The Maine Department of Public Safety and Maine State Police are still reviewing this 24-page bill to carefully determine any potential public safety issues related to this very detailed and complex bill. One concern surrounds the definition of HIPPA within the bill and how this might impact the National Precursor Log Exchange, and the sharing of state statute required information by pharmaceutical entities. A more thorough review of this bill's language is needed to determine if there will be an impact on tools used by law enforcement to identify suspects in crimes, locate next of kin in homicide and death investigations, and matters related to ensuring the safety of all those who live and visit Maine.

On behalf of the State Police and the Department of Public Safety, we appreciate your careful consideration of these issues.

Respectfully,

Lieutenant Mathew Casavant

HOSPITALITY
MAINE



45 Melville St. Augusta, ME 04330
207-623-2178
www.hospitalitymaine.com

327 Water St, Hallowell, ME 04347
207-623-0363
www.maine-tourism.com

Testimony of Nate Cloutier

Before the Joint Standing Committee on Judiciary
May 5, 2025

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

Senator Carney, Representative Kuhn, and distinguished members of the Joint Standing Committee on Judiciary, my name is Nate Cloutier, and I am here today on behalf of HospitalityMaine, representing Maine’s restaurant and lodging industries. I am also testifying on behalf of the Maine Tourism Association (MTA). MTA has been promoting Maine and supporting tourism-related businesses—from lodging and dining to camps, retail, guides, amusements, and historic attractions—for over 100 years. HospitalityMaine and the Maine Tourism Association support the bipartisan proposal in LD 1224 and respectfully oppose LD 1822.

Together, our industries employ more than 130,000 people and have an effect of nearly \$16 billion on the Maine economy. According to the Maine Office of Tourism, that impact helps lower the tax burden for every Maine household by nearly \$2,500. Maine’s hospitality and tourism businesses are fueled by small, independent, family-run establishments. In many ways, they’re what make Maine feel like Maine—for both people who live here and those who visit.

From small coastal inns to family-run restaurants, these businesses define the character of our communities. And right now, many of them are navigating real uncertainty. Between food and labor costs that have both increased 30% in the last five years, staffing challenges, and shifting travel patterns, small business owners are watching every dollar. Adding complex and inconsistent privacy regulations into the mix, especially those that don’t match what neighboring states are doing, only adds to that uncertainty.

We support LD 1224 because it strikes the right balance. It protects consumer privacy, gives people control over their data, and sets clear expectations for businesses. Just as importantly, it aligns with laws passed in 17 other states, including NH, RI, and CT. That consistency matters.

What we are trying to avoid is a situation like LD 1822 could create, where Maine becomes an outlier. As you know, this is modeled after a Maryland law that hasn’t even taken effect yet. It creates compliance burdens that even large companies would find difficult to manage, let alone the small businesses like I work with every day.

Take, for example, a small inn in Boothbay that depends on repeat customers and targeted outreach. Under LD 1822's standards on targeted advertising (particularly, the "reasonably should know" language), it's unclear whether that business could confidently run a Facebook ad aimed at families looking for summer getaways. Would someone in that audience be a minor? Possibly. Could that ad now be considered too risky to run? Quite possibly. That's a problem.

Or think about a local restaurant in Bar Harbor that sees thousands of digital interactions during peak season. Those are just folks checking the menu, making a reservation, or looking for directions. But under LD 1822, all of those website visits count toward a 35,000-consumer threshold—a number so low that many small and seasonal businesses could hit it without realizing it. Once they do, they'd have to conduct data protection assessments even if they don't collect much personal information at all. Maine's law should have a 100,000-consumer threshold like most other states with a data privacy law.

Even small businesses that don't meet that threshold could still have compliance obligations as "processors." They'd be required to modify contracts, conduct data mapping, and ensure any subcontractors meet the same standards. These are real costs both in dollars and time, and the more Maine's policy differs from those in other states, the higher those costs will be.

By contrast, we view LD 1224 as modeled on a bipartisan, regional framework that provides necessary clarity. It requires opt-in consent for the use of sensitive data, rather than ambiguous standards like "strictly necessary." It gives enforcement authority clear guidance, and it gives businesses a chance to comply with consistent regulations that are already being implemented across the country.

This is especially important in tourism. Hospitality businesses don't just compete with each other; they compete with neighboring states. If an inn in Conway, New Hampshire, can market itself more effectively than a lodge in Bethel, that's a real disadvantage. If a Portland restaurant loses out to a Portsmouth one because of different privacy requirements, that's revenue leaving our state.

Hospitality and tourism have helped carry Maine through challenging times. These businesses, many of whom are your constituents and neighbors, are eager to comply with thoughtful privacy protections. But they need a framework that's workable. LD 1224 provides that. LD 1822 does not.

Thank you for your time and attention. I would be happy to answer any questions now or for the work session.

Maine PRISONER ADVOCACY Coalition



May 5, 2025

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

My name is Jan Collins, I am Assistant Director of Maine Prisoner Advocacy Coalition (MPAC) an organization committed to ethical, positive, and humane changes in Maine's prison system. I am here in support of LD 1822 An Act to Enact the Maine Online Data Privacy Act and against LDs 1224, 1088, and 1284.

LD 1822 would create a new statute giving Maine consumers a range of rights in their digital data. Like Maryland Online Data Privacy Act, the bill would apply to for-profit companies that annually process the data of 35,000 or more Maine residents or derive 20% or more of their revenue from the sale of data and have the data of 10,000 or more Maine residents. The fact that a significant percentage of a companies profit results from the sale of data would come as a shock to most Maine residents.

This bill would limit the collection, processing, and sharing of consumer data, a welcome and necessary step in providing consumer privacy and to help slow the dissemination of data which is then used to spam our mail boxes. Of greater concern is the use of purchased data to scam consumers, a practice that costs Mainer's millions of dollars annually.

We are under a daily barrage of information streams and commercial gimmicks intended to make a profit for a commercial interest. But we are also being conned and coerced by more nefarious actors who can easily purchase our information for their purposes. Most of us are neither aware of, nor would we consent to, the use of our data.

Some of the people most affected by the current practices are people newly released from prison after a long stay. Some have never seen a smart phone or used a computer. They are highly susceptible to scammers. Even those who have taken college courses while they are incarcerated have not been exposed to the world wide web. All their computer access is highly controlled.

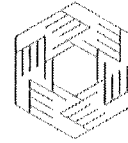
I know of people who received their master's degree while incarcerated. They were totally overwhelmed by their email inbox upon release. Even highly intelligent individuals have fallen prey to scams and viruses they were exposed to in their inbox.

This bill allows us the protections we would want for ourselves, our children, and our loved ones.

Please protect Maine consumers by passing LD 1822 and by opposing LDs 1224, 1088, and 1284.

Thank-you,
Jan

Jan M. Collins
Assistant Director
Maine Prisoner Advocacy Coalition
PO Box 360, E. Wilton, ME 04234
207.578.8419



HEALTHCARE
PURCHASER
ALLIANCE
OF MAINE

May 5, 2025

Senator Anne Carney, Chair
Representative Amy Kuhn, Chair
Committee on Judiciary
c/o Legislative Information Office
100 State House Station
Augusta, ME 04333

Dear Senator Carney, Representative Kuhn, and Members of the Committee on Judiciary

My name is Sara Fitzgerald, and I'm the Director of Analytics at the Healthcare Purchaser Alliance of Maine. We are a small nonprofit organization based in Falmouth, Maine that helps employers and public trusts obtain more affordable and higher quality health care for their employees and dependents.

One of the services we offer to Maine-based employers and sponsors of group health benefit plans is analysis of health care claims incurred by covered plan members. In this capacity, we process protected health information to provide benchmarking reports and cost driver analyses that help our members understand how their health care costs, utilization, disease prevalence, and quality measures compare to other Maine-based employers.

In reviewing the various privacy bills before the committee today, we were pleased to see that the processing and analysis we perform on behalf of our Maine employer members would meet the exemption provisions for protected health information included in each of the LDs.

Consistent with all of these bills, we hope that the legislation ultimately recommended by the Committee will preserve this exemption for protected health information.

Thank you for the opportunity to provide the HPA's feedback. If you have any questions or need any additional information, I can be reached at sfitzgerald@purchaseralliance.org.

May 5, 2025

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

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

EPIC writes in support of LD 1822, An Act to Enact the Maine Online Data Privacy Act, because it would provide critical protections Mainers need to stay safe online. We also write in opposition to LD 1224, LD 1088, and LD 1284 because they fail to accomplish that goal. The Electronic Privacy Information Center (EPIC) is a nonprofit research organization established in 1994 to secure the fundamental right to privacy in the digital age for all people. EPIC has long advocated for strong privacy laws at the state and federal levels and was heavily involved in last session's deliberations on a data privacy bill in Maine.¹

LD 1822 builds on existing state privacy laws already enacted in nineteen states and incorporates essential provisions to provide Mainers with the protections they need to stay safe online. Key provisions of LD 1822 include:

- **Data minimization:** LD 1822 limits the unfettered collection of personal data by setting a baseline requirement that entities only collect personal data that is reasonably necessary to provide or maintain a product or service requested by the consumer.
- **Strong protections for sensitive data:** LD 1822 sets heightened protections for sensitive data like biometrics, location, and health data such that its collection and use must be strictly necessary for the product or service the consumer requests, and it may not be sold.
- **Preventing discrimination:** LD 1822 extends civil rights to online spaces by prohibiting entities from processing data in a way that discriminates or otherwise makes unavailable the equal enjoyment of goods and services on the basis of race, color, religion, national origin, sex, sexual orientation, gender, or disability.
- **Protections for children and teens:** LD 1822 prohibits targeted advertising to minors and bans the sale of minors' data.

In my testimony, I will discuss why it is so critical that Maine enact a strong privacy law, the current state of state privacy laws, and go into detail on a few key protections that are crucial to keep Mainers safe online. I also include an attachment with a few suggested amendments to the bill.

¹ See e.g. EPIC, *The State Data Privacy Act: A Proposed Model State Privacy Bill*, <https://epic.org/the-state-data-privacy-act-a-proposed-model-state-privacy-bill/>.

Data Abuse Harms Mainers

Advertisers and data brokers track our every move online and our data is constantly used against us, harming our wallets, opportunities, and rights. Examples of these harms include:

1. **Increased insurance premiums.** Texas Attorney General Ken Paxton recently sued insurance giant Allstate for unlawfully collecting, using, and selling Texans' location data through secretly embedded software in mobile apps such as Life360 and GasBuddy. Paxton alleged that Allstate and other insurers then used the covertly obtained data to justify raising Texans' insurance rates.²
2. **Increased pricing on consumer goods.** The Federal Trade Commission recently found that retailers frequently use people's personal information to set targeted, tailored prices for goods and services—from a person's location and demographics, down to their mouse movements on a webpage.³

Small businesses are harmed by these systems as well. As Check My Ads, an advocacy group formed by former advertising industry employees recently wrote to Congress:

Privacy legislation that emphasizes data minimization and transparency leads to higher-quality, more relevant data. Right now, the advertising supply chain is bloated with third-party data—often inaccurate, outdated, or collected without meaningful consent. Acxiom, one of the world's largest data brokers, even admitted their consumer data is made up of “informed guesses,” with the hope it doesn't lead to credit denial or other harm. This kind of data is not only unreliable—it wastes ad spend. Privacy-focused frameworks should encourage a shift to first-party data—information voluntarily shared by users—delivering more accurate, context-rich insights. Advertising that uses high-quality data performs better. With privacy legislation in place to curb harmful data practices and enforce consent, advertisers gain access to permissioned, engaged audiences—the kind that convert and stay loyal.⁴

These economic harms are on top of the harms to our rights. Last year, Senator Ron Wyden found that Near, a location data broker, sold location data to an anti-abortion organization who used it to target misinformation and ads to people who visited reproductive health clinics, including in Maine.⁵

² Press Release, Att'y Gen. of Texas, *Att'y Gen. Ken Paxton Sues All-state and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Cos.* (Jan 13, 2025), <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45>.

³ FTC, *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices* (Jan. 2025), <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer>.

⁴ Letter from Check My Ads to House Energy & Commerce Comm. Privacy Working Group 8 (Apr. 2025), <https://checkmyads.org/wp-content/uploads/2025/04/Privacy-Working-Group-RFI-Check-My-Ads-Submission.pdf>.

⁵ Press Release, Sen. Ron Wyden, *Wyden Reveals Phone Data Used to Target Abortion Misinformation at Visitors to Hundreds of Reproductive Health Clinics* (Feb. 2024), <https://www.wyden.senate.gov/news/press-releases/wyden-reveals-phone-data-used-to-target-abortion-misinformation-at-visitors-to-hundreds-of-reproductive-health-clinics>.

The State of State Privacy Law: Existing Laws Don't Do Enough

Because there is no federal comprehensive privacy law, states have been enacting laws to fill this void. Since 2018, 19 states have passed comprehensive privacy laws. EPIC and U.S. PIRG recently released a report grading these laws.⁶ Nearly half failed, and none received an A. These laws do little to limit mass data collection and abuse.

Many of these state laws closely follow a model initially drafted by tech giants.⁷ This draft legislation was based on a privacy bill from Washington state that was modified at the behest of Amazon, Comcast, and Microsoft.⁸ An Amazon lobbyist encouraged a Virginia lawmaker to introduce a similar bill, which became law in 2021. Unfortunately, this Virginia law became the model that industry lobbyists pushed other states to adopt. In 2022, Connecticut passed a version of the Virginia law with some additional protections, which has now become the version often pushed by lobbying groups doing the bidding of Big Tech companies in select states. **Privacy laws should not be written by the very companies they are meant to regulate.**

Laws based on industry's model bill, which includes LD 1224 and LD 1088, do not meaningfully limit what data companies can collect or what they can do with that data — they merely require that companies disclose these details in their privacy policies, which consumers rarely read. Companies should not be allowed to determine for themselves what are the permissible purposes of collecting and using consumers' personal information. Unfortunately, the limitations on data collection in LD 1224 and LD 1088 allow companies to do just that. They read:

A controller shall limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer.

This reinforces the failed status quo of “notice and choice” — businesses can list any purpose they choose in their privacy policies, knowing that very few consumers will read them. In fact, it incentivizes companies to list as many purposes as possible, and as broadly as possible, to cover every conceivable reason they would ever want to collect your data. And the only “choice” the consumer has is to not use the service at all. The clearer limits on data collection in LD 1822 are critical because they require companies to better align their data practices with what consumers expect, allowing Mainers to use online services without being forced to sacrifice their privacy.

⁶ EPIC and U.S. PIRG Edu. Fund, *The State of Privacy: How State “Privacy” Laws Fail to Protect Privacy and What They Can Do Better*, EPIC and U.S. PIRG (Jan. 2025), <https://epic.org/state-of-privacy-2025/>.

⁷ Jeffrey Dastin, Chris Kirkham & Aditya Kalra, *Amazon Wages Secret War on Americans' Privacy, Documents Show*, Reuters (Nov. 19, 2021), <https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/>.

⁸ Emily Birnbaum, *From Washington to Florida, Here Are Big Tech's Biggest Threats from States*, Protocol (Feb. 19, 2021), <https://www.protocol.com/policy/virginia-maryland-washington-big-tech>; Mark Scott, *How Lobbyists Rewrote Washington State's Privacy Law* (Apr. 2019), <https://www.politico.eu/article/how-lobbyists-rewrote-washington-state-privacy-law-microsoft-amazon-regulation/>.

Data Minimization, Sensitive Data Protections, and Strong Enforcement: The Keys to a Strong Privacy Law

Data Minimization

LD 1822 relies on a concept that has long been a pillar of privacy protection: data minimization. When consumers interact with a business online, they reasonably expect that their data will be collected and used for the limited purpose necessary to provide the goods or services that they requested. For example, a consumer looking up symptoms on WebMD does not expect that what they're reading is sent in the background to Meta, Google, and over a dozen advertisers, but that's exactly what's happening right now.

To incentivize better data practices, LD 1822 set a baseline requirement that entities only collect data that is “*reasonably necessary and proportionate*” to provide or maintain a product or service requested by the consumer. This standard is referred to as “data minimization” and it better aligns business practices with what consumers expect.

The rule in LD 1822 is modeled on the rule in the Maryland Online Data Privacy Act, which was enacted last year. It is not as strict as the rule advanced by this Committee last session. It doesn't go far as privacy advocates would like – we prefer that data minimization rules cover both how much data a company can collect *and* how they can use that data. LD 1822 takes a compromise position and applies to collection only, which mirrors the rule in Maryland's law. Data minimization offers a practical solution to a broken internet ecosystem by providing clear limits on how companies can collect and use data.

A Ban on the Sale of Sensitive Data Prevents Some of the Worst Data Harms

LD 1822 sets heightened protections for sensitive data such that its collection and use must be *strictly necessary* to provide the product or service the consumer is asking for. This is a critical provision that protects the data we all consider to be the most sensitive, such as our location, health, and financial data. It also bans the sale of sensitive data entirely. Both of these rules are included in the recently enacted Maryland Online Data Privacy Act.

Many an app has likely prompted you to request access to your location. Sometimes, the app has a legitimate reason to access the information, like displaying your local weather. Sometimes, it doesn't. In either case, the app may be selling your location data to a third party. A top Catholic Church official was forced to resign a few years ago after a Catholic media site used cellphone data to show that the priest was a regular user of the queer dating app Grindr and visited gay bars.⁹

⁹ Michelle Boorstein et al., *Top U.S. Catholic Church Official Resigns After Cellphone Data Used to Track Him on Grindr and to Gay Bars*, Wash. Post (July 21, 2021), <https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/>.

The recent bankruptcy of genetic testing company 23andMe further highlights the need for heightened protections for sensitive data. 23andMe has genetic data on 15 million customers, so a massive amount of highly sensitive information—now 23andMe’s most valuable asset—will be sold off to the highest bidder. After a federal judge gave permission for the company to sell its sensitive customer data, millions of customers have no control over who their information is sold to. While research shows that most Americans believe—incorrectly— that the personal health information they give to health apps and websites is protected by the Health Information Portability and Accountability Act (HIPAA), the law does not apply to 23andMe’s handling of consumer genetic information. I suggest an amendment in the enclosure to ensure sensitive data is protected in the case of a merger or bankruptcy.

Enforcement is Critical

Robust enforcement is critical to effective privacy protection. Strong enforcement by state government via Attorney General authority is an essential component of a strong privacy law. Funds should be appropriated to ensure the Attorney General can meaningfully enforce the law, particularly in the absence of a private right of action to supplement state enforcement.

* * *

EPIC also asks you to oppose LD 1284, which would repeal Maine’s ISP privacy law. We feel that the law’s protections are still critical even if a comprehensive privacy law is enacted in Maine because of the unique relationship between a consumer and their broadband service provider.

* * *

LD 1822 is not a privacy advocate’s ideal bill. EPIC would prefer that the data minimization rule cover data use in addition to collection. We’d like to see a private right of action included so that individuals can enforce their rights under the law. We’d prefer that the bill cover non-profits. But LD 1822 reflects a compromise that would provide Mainers with important privacy protections that they lack today and is the most consumer-friendly privacy bill before this Committee. EPIC asks that you to support LD 1822 and oppose LDs 1224, 1088, and 1284. I am happy to be a resource to the Committee as it navigates this issue.

Sincerely,

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
Deputy Director, EPIC

Encl.

EPIC's Suggested Amendments

1. Delete §9808(1)(G), which conflicts with the data minimization rule

§9808(1)(G) refers to obtaining consent for purposes that are not disclosed in the privacy policy, which conflicts with the data minimization provision in §9808(1)(A) limiting data collection to what is reasonably necessary and proportionate to provide or maintain the specific product or service requested by the consumer. It is unclear how these two provisions would work together, but at worst it provides a loophole for companies to simply ask for consent for any data use they desire. Consent has been proven to be an ineffective way to protect privacy.

2. Confirm that controllers must offer universal opt-out mechanism

§9808(6)(C) appears to give controllers the option of providing an opt-out link or allowing consumers to opt-out via a universal opt-out preference signal. This conflicts with §9607(2), which gives consumers the right to exercise their opt-out rights via a global device setting. And nearly every other state that has a universal opt-out mechanism (including CT and NH) require both an opt-out link *and* the option of a universal opt-out preference signal.

EPIC asks that you change the “or” to an “and” in line 28 on page 14, which would mirror CT, NH, and most other state laws.

3. Ensure sensitive data such as genetic data is protected in mergers and bankruptcy sales

The recent bankruptcy of genetic testing company 23andMe revealed loopholes in many state privacy laws that fail to protect consumers from the sale of their sensitive data in the event of a merger, acquisition, or bankruptcy.¹⁰ An exemption in the definition of “sale” that excludes the transfer of data during a bankruptcy proceeding renders consumers’ right to opt out of data sales useless in terms of 23andMe’s sale resulting from bankruptcy. California amended its privacy law last year to remove this exemption and clarify that consumers can opt out of the sale of their data even in the context of a bankruptcy proceeding.¹¹

To provide protections for Mainers in these situations, we recommend (1) striking subsection (B)(6) from the definition of “sale” and (2) adding the following to the exemptions in §9613(1):

L. Transfer assets to a third party in the context of a merger, acquisition, bankruptcy or similar transaction when the third party assumes control, in whole or in part, of the controller’s assets, only if the controller, in a reasonable time prior to the transfer, provides an affected consumer with:

(A) A notice describing the transfer, including the name of the entity receiving the consumer’s personal data and the applicable privacy policies of such entity and

(B) a reasonable opportunity to:

(i) withdraw previously provided consent related to the consumer’s personal data, and

(ii) request the deletion of the consumer’s personal data;

¹⁰ Kara Williams, *Concern over Potential 23andMe Data Sale Highlights Weaknesses of State Privacy Laws* (May 2, 2025), <https://epic.org/concern-over-potential-23andme-data-sale-highlights-weaknesses-of-state-privacy-laws/>.

¹¹ Cal. Assembly Bill No. 1824 (2024), https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB1824.

4. Remove addition to “publicly available information” definition that opens loophole

“Publicly available information” is exempted from coverage of the bill, so it is critical that it is defined as narrowly as possible. LD 1822 proposes adding a provision that includes in the definition any information about a consumer that a person “obtains from a person to whom the consumer disclosed the information unless the consumer has restricted the information to a specific audience.”

This addition is a dangerous extension of the definition and a big loophole in our view -- it would make a wide swath of information publicly available in a way that many consumers wouldn't expect to be. And in many instances, consumers might not even have the ability to restrict the audience. For example, this would mean any time a consumer provides data to a company (e.g. signing up for an account or filling out an application) and doesn't limit the audience, it is public information and exempt from coverage under the law.

It seems more like this should instead be an exemption to the definition, i.e. “Publicly available information” does not include information that the consumer has restricted to a specific audience.” That would be our preference but at minimum, EPIC would ask that it be amended to match the language in last session’s Committee bill, which reads:

A website or online service made available to all members of the public, either for free or for a fee, including a website or online service in which all members of the public can log on to the website or online service either for free or for a fee, unless the individual who made the information available via the website or online service has restricted the information to a specific audience.

5. Add definition of “minor”

There is no definition of “minor” in the bill. The summary indicates that it is meant to be under 18 years of age, but there's no definition of it in the bill.

AARON M. FREY
ATTORNEY GENERAL



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

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

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

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

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

Testimony in Support of LDs 1822, in Opposition to LD 1088 and 1224

Senator Carney, Representative Kuhn, and honorable members of the Joint Standing Committee on Judiciary, my name is Brendan O'Neil, I am an Assistant Attorney General and appear on behalf of Attorney General Aaron Frey to testify in support of L.D. 1822 and in opposition to L.D.s 1088 and 1224, all proposing different approaches to comprehensive consumer privacy. We thank the Committee for investing its time into these proposals at this critical moment as advances in technology, the digital information economy, the rise of artificial intelligence, and digital surveillance raise many concerns. As we learn more about these issues, it is critical that Maine's consumers gain greater control and rights over their and their families' information.

The Attorney General's Office supports L.D. 1822 because, if enacted, Maine would be among the states leading the nation on privacy, with among the strongest and most protective provisions. Of the three bills, we believe L.D. 1822 will do more to restore an appropriate balance between consumers and industry regarding control over individuals' information and data. In supporting L.D. 1822, we want to highlight certain critical components of a strong comprehensive data privacy bill, along with suggestions for improvements:

Meaningful data minimization: A core protection for Mainers is limiting the information that companies may collect about us and our activities online to the minimum necessary to provide the product or service the consumer is requesting, coupled with keeping that information only for the minimum period necessary to do so. This keeps data collection focused on the consumer's needs. It also minimizes the work consumers must do to opt out of data collection on each website or application they engage with and, because of this, we think this form of data minimization is more efficient and more effective at protecting Mainers' data than the notice-and-opt-out model of privacy legislation found in L.D.s 1224 and 1088¹. L.D. 1822 includes, in §9608, this kind of meaningful data minimization and we strongly support passing a privacy bill including these provisions. Further, L.D. 1822 provides stronger protections for Maine's

¹ Because businesses and other entities collecting individual data will almost always know more about what they do with that data than consumers, "that may mean that placing the burden on [industry] to identify and mitigate risks to consumers would be a more efficient approach than obligating consumers to continually take action to guard the consumer's data." Consumer Financial Protection Bureau, *State Consumer Privacy Laws and the Monetization of Consumer Financial Data*, Section 2.3, n. 21, November 2024 (<https://www.consumerfinance.gov/data-research/research-reports/state-consumer-privacy-laws-and-the-monetization-of-consumer-financial-data/>).

children by limiting the collection and use of data about youths up through age 17, rather than only up through age 12 as in L.D.s 1224 and 1088.

This form of data minimization is in Maryland's privacy statute enacted last year, and is being considered by state legislatures including in Connecticut and Massachusetts. And limiting data retention is now in the federal rule implementing the Children's Online Privacy Protection Rule (COPPA) as updated in January by the Federal Trade Commission's recent rulemaking.²

This version of data minimization is much more robust and protective of consumers than versions that describe limiting data collection to the practices a company discloses in its privacy policy. That version is found in L.D.s 1224 and 1088. Under that model, companies may continue to collect any information about us they wish so long as they merely disclose it in a privacy policy, which they may change at any time. We believe that is no limit. The Attorney General's office does not support legislation with that version because we believe it does not sufficiently protect consumers and instead keeps data collection focused on the collectors' economic needs. As the Federal Trade Commission recently found, "Many companies' insistence that their data collection practices are justified simply because they are 'disclosed' to consumers only amplifies [concern about companies' data handling and oversight]." These so-called disclosures are very hard to read (often made across various policies, located in different places across websites, apps, etc.), nearly impossible to understand, too vague to effectively communicate a platform's actual practices, and subject to change (and it is up to the consumer to determine what has changed and when)."³

Limiting the data collected from and about us to the absolute minimum necessary, and the time it's kept to only as long as necessary, is strong privacy protection. In 2024, the Attorney General's office received over 1,000 data breach notices alerting nearly 1 million Mainers that their data was put at risk. Data breach investigations by state Attorneys General or the FTC often involve significant amounts of consumer information, including sensitive data, and data that has been kept far longer than it is needed, resulting in increased scam and fraud risk to consumers and significant liability for businesses. Consumers, and companies, are at less risk of a data breach when less information is collected and when it is deleted as soon as no longer needed according to a public schedule.

Robust data minimization is critical at this time - more and more of our data and information is being collected, bought, sold, and processed against consumers' expectations, without our knowledge, and sometimes to our detriment. Financial institutions and, increasingly, other companies and firms offering consumer financial products, are collecting large quantities of consumer data, building new business models around monetizing that data as a source of revenue, including by selling that data to 3rd parties.⁴ Consumers highly value their financial data, perhaps even more than their medical records, and are especially concerned about

² 16 C.F.R. 312.10, see also Statement of FTC Chair Lina Khan, January 16, 2025, page 2 (<https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-chair-lina-m-khan-regarding-final-rule-amending-childrens-online-privacy-protection-rule>)

³ Federal Trade Commission, *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services*, Section IV(D), September, 2024 (<https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services>)

⁴ *Supra* note 1, Section 3.

maintaining the privacy of that data.⁵ While consumers are increasingly using digital tools for banking and payment services, financial institutions are also increasingly sharing consumer information with advertisers, perhaps without the awareness of consumers, and some have launched their own advertising platform affiliates.⁶

Social media companies and video streaming services collect significant amounts of data about consumers, both directly and indirectly by purchasing data, and those companies share this data with affiliates and 3rd parties.⁷ These companies sometimes cannot identify what data they collect about consumers.⁸ L.D. 1822 attempts to address such vast overcollection and hidden uses through its strong data minimization and data deletion requirements, which we commend.

We believe that data minimization as found in L.D. 1822 is much more protective of Mainers than the notice and opt-out model found in L.D.s 1088 and 1224 by collecting less data and by better balancing the work of data protection and the risks that follow data collection and retention.

Exemptions for data, not entities: The Attorney General's office supports legislation that avoids exempting entire sectors of the economy on the basis that some of the work an entity does may be regulated by a federal statute which provides some privacy regulation. Instead, we support legislation that exempts data, not entities, and only to the extent the specific activity – the collection and use of the data – is regulated by a federal statute. Anything more than that we believe is overbroad and leaves consumers unprotected and without rights over significant data collection practices. Some federal statutes, such as the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA), while establishing a regulatory floor with some privacy-related provisions, expressly permit states to enact greater privacy protections.⁹ We strongly support limiting any exceptions to the use of data, not the entire entity beyond the use of the data, thereby increasing the privacy protections for Mainers. Further, at a time when significant questions exist about whether the federal regulators on the privacy beat, including the CFPB and the FTC, will continue to exist, will face significant cuts in staffing, and will divert any remaining enforcement efforts elsewhere, Mainers may not be able to rely on federal privacy enforcement and states have additional incentive to raise the floor and provide stronger privacy protections for their citizens.¹⁰

⁵ *Id.*

⁶ *Id.*

⁷ *Supra* note 3.

⁸ *Id.*

⁹ “Given financial institutions’ rapid investment in expanding their own data monetization and absent stronger federal protections, States should consider whether they wish to continue to exempt these activities from the consumer rights and protections their comprehensive state privacy laws provide.” *Supra*, note 1, Section 5, noting that “Under the GLBA, the term “financial institution” broadly encompasses a wide variety of businesses engaged in financial activities, including lending, transferring money or securities, financial advisory services, asset management, consumer reporting, debt collection, loan servicing, various transactional services, and in many circumstances acting as a service provider for companies engaged in these activities.”, citing 12 U.S.C. § 1843(k)(4); 12 C.F.R. §§ 225.28, 225.86.

¹⁰ Commissioner Slaughter Opening Statement, U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, Hearing on *The World Wild Web Examining Harms Online*, Wednesday, March 26, 2025 (https://democrats-energycommerce.house.gov/sites/evo-subsites/democrats-energycommerce.house.gov/files/evo-media-document/testimony_rebecca-kelly-slaughter.pdf).

States enforcing their existing privacy statutes report that overbroad entity-level exemptions are challenging for consumers and for privacy enforcement – Connecticut is considering legislation to scale back its exemptions. We strongly support the position taken in L.D. 1822 to include only data-level exemptions for activity regulated by the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA). However, exempting entire health care entities, nonprofits, and institutions of higher education removes major sectors of Maine’s digital economy from these privacy rights for Mainers and significantly limits this legislation. We recommend the Committee consider strengthening L.D. 1822 by eliminating the following entity-level exemptions in §9604(1):

- (F) - Health care affiliates, practitioners, or affiliates thereof – This exemption allows such entities to use hidden pixels, data brokers, or other means to collect, process, and sell any information – including non-HIPAA-related data - about consumers, for any purpose, including marketing or additional profit. HIPAA-related data is already exempt under §9604(2)(B), rendering an entity-level exemption unnecessary and redundant, and leaving Mainers at risk. Perhaps unique among other entities covered by this legislation, consumers will always need to interact with these entities and should be able to keep their information safe when they need healthcare.
- (C) – Institutions of higher education – This provision risks exempting any post-high school educational or training entity, including for-profit Internet-based colleges, private colleges, and possibly any entity offering courses or certificates or degrees of any kind, or any entity setting itself up as a “college”. As with health care entities, the data of students is already exempted under §9604(2)(M), rendering an entity-level exemption redundant and creating risks for Mainers. Institutions of higher education of any kind serving Mainers would be able to collect, buy, and sell significant amounts of non-FERPA-related data. It is reasonable to expect that such institutions will and should be as able to comply with this legislation as other covered entities.
- (B) – Nonprofit entities – Nonprofit entities collect a significant amount and breadth of consumer data, and other states have not exempted them. Nonprofits may be large entities, may have a regional or national presence, and are often sophisticated organizations. Smaller nonprofits may utilize sophisticated vendors to assist them with meeting ‘back-office’ regulatory and administration obligations. Nonprofits should be expected to protect Mainers’ information by complying with L.D. 1822.

Enforcement: The enforcement mechanism, in each of the bills should be improved. As with other consumer protection laws, the Attorney General’s Office believes it is necessary that Mainers be empowered to enforce their own rights under any comprehensive privacy legislation. There is nothing sufficiently different about consumer privacy that warrants treating it differently from other consumer protection statutes. We believe the Legislature, in granting rights to individual consumers, should not require them to rely on a state agency to enforce those rights. We note that privacy legislation in Massachusetts includes a private right of action. Other state Attorneys General are enforcing their states’ privacy statutes and we expect to do so as well. However, even with additional resources being provided to our office, we likely will not be able to pursue every violation. Maine consumers should be empowered to protect themselves. We are prepared to work with the Committee to address concerns and balance Mainers’ ability to pursue their claims with businesses’ ability to operate with certainty. In particular, we believe the

Legislature can address concerns about excessive litigation by clearly and particularly identifying the parts of the legislation for which individuals may bring claims. Following are a few proposals we suggest the Committee consider:

- Coupling a right to cure with a private right of action – this would help those entities which are attempting to comply in good faith by giving them an opportunity to address inadvertent noncompliance or minor/technical noncompliance. We recommend any such right to cure be subject to a sunset;
- Exempting small businesses from a private right of action for some period of time; and
- Delay implementation of a private right of action for some period of time to give businesses and consumers time to adjust to the new privacy protections.

Information for consumers: We appreciate L.D. 1822 enhancing the rights of Maine consumers by enabling them to request a list of the 3rd parties to which a controller has sold the consumer's data. This critical information enables consumers to follow their data downstream so that they may learn more about who is using their data and request its deletion. This is another area in which L.D. 1822 provides stronger protections for Mainers than L.D.s 1088 and 1224. We suggest improving upon this by enabling consumers to request the information a company has about a consumer which it claims is publicly available information (PAI). Because PAI is carved out of the definition of personal data, companies have no obligation to reveal information it has designated as PAI to consumers, nor do consumers have an opportunity to challenge this designation. And, because of the challenges presented by PAI as reported by states enforcing their statutes, we also recommend the Committee consider the change to its definition being considered by the Connecticut Legislature.¹¹

Opt-out preference signals: Particularly in the absence of a private right of action, consumers should have the ability to – as simply and easily as possible, with minimal friction – exercise their opt out rights through technology that can efficiently and conveniently signal their preference to opt out of the sale of personal data, use for targeted ads, or processing for certain purposes. We recommend the Committee consider eliminating §9608(6)(C)(2) (e) and (f) in L.D. 1822.

Affiliates: The Federal Trade Commission and the Consumer Financial Protection Bureau both raised concerns last year about consumer data being shared with affiliates, some of which are part of extensive corporate conglomerates, including affiliates in foreign countries.¹² Such affiliates may be providing services very different from the collector of the data, and consumer data may be used for unknown purposes beyond its original collection, such as AI training.¹³ However, the definition for Sale of Personal Data exempts sharing with Affiliates, which may be a significant loophole that undermines Mainers' expectations about who has access to their data and for what purposes. We suggest narrowing the Affiliate exemption to restrict such transfers to providing or maintaining a specific product or service requested by the consumer.

¹¹ See S.B. 1356, 2025, Section 1(34)

(https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&which_year=2025&bill_num=1356).

¹² *Supra* notes 1 and 3.

¹³ *Supra* note 3, at section IV(D); note 1, at sections 2 3, 3.

Internet Service Providers (ISPs): The Attorney General has consistently opposed any attempt to repeal Maine's landmark consumer protection law providing some of the strongest privacy protections for broadband internet customers nationwide.¹⁴ Consistent with our office's testimony opposing L.D. 1284 which would repeal the ISP privacy law, we oppose L.D. 1088 which also includes a repeal provision. Again, this first in the nation law restricts the extent to which ISPs may use, disclose, or sell their customers' personal information, such as Mainers' browsing history, their location, the content of their communications, and their financial and health information. As the Federal Trade Commission has noted, because ISPs are essentially the gateways or onramps to the internet, they can collect vast amounts of information regarding their customers' online activity. Recognizing that position, the Maine Legislature wisely enacted the ISP law with very strong protections for consumers online information, and it should not now retreat from its zealous protection of our residents' privacy.

Thank you for your consideration of these comments, and I am happy to answer any questions.

¹⁴ 35-A M.R.S.A. c. 94.



Check My Ads Institute Written Testimony to Maine Legislature in Support of the Maine Online Data Privacy Act

May 5, 2025

Senator Anne Carney, Senate Chair
Representative Amy Kuhn, House Chair
Committee on Judiciary
100 State House Station, Room 438
Augusta, Maine 04333-0100

Re: Testimony in Support of LD 1822, the Maine Online Data Privacy Act

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

We write in support of LD 1822, the Maine Online Data Privacy Act. Check My Ads is a 501(c)(3) nonprofit independent digital advertising watchdog advocating for a transparent and fair digital advertising market for advertisers and the public.¹

My name is Arielle Garcia, and I am Chief Operating Officer of Check My Ads Institute. Prior to joining Check My Ads in 2024, I spent ten years in digital advertising, serving most recently as Chief Privacy Officer at UM Worldwide, a major global advertising agency that manages advertising campaigns on behalf of advertisers. For years, I helped advertisers navigate the evolving regulatory environment, as they looked to strike the balance between privacy and targeted advertising. Indeed, I resigned² from my role due to my realization that the only winners in the current state of the digital advertising industry are big technology (“big tech”) companies like Google, and the data brokers and advertising technology (“adtech”) middlemen that dwell in their shadows.

¹ CHECKMYADS.ORG, <https://checkmyads.org/> (last visited Mar 12, 2025).

² Arielle Garcia, *An Industry In Conflict: It's Time For Tough Questions And Hard Decisions*, ADEXCHANGER, Sep. 2023, <https://www.adexchanger.com/marketers/an-industry-in-conflict-its-time-for-tough-questions-and-hard-decisions/> (last visited Mar 12, 2025).

The \$700 billion digital advertising industry is the primary business model of the internet. As it stands today, that business model is broken.

Big tech companies, like Google and Meta have built empires on a foundation of unbridled extraction. Not only have they amassed massive troves of data, but they have cemented themselves across all corners of industry and society, unilaterally establishing norms that benefit their own business to the detriment of their users, advertisers, and publishers alike. Yet, while these companies are household names, there are hundreds of other companies in the advertising technology (“adtech”) sector that have followed in their footsteps.

Before the advent of modern digital advertising, advertisers would typically work with an ad agency to identify which publications their target audiences are likely to consume. Today, most advertising online is transacted through automated, real-time auction. This is known as programmatic advertising.³ Over the past two decades, the central promise of programmatic was that it would help advertisers of all sizes more efficiently and effectively reach their audiences, and help publishers monetize - or sell - more of their ad space. The following is a simplified explanation of how a real-time programmatic ad auction works:

1. A user visits a website, triggering a bid request from the website to the Supply Side Platform (“SSP”) that publishers use to sell their ad space. That bid request includes data about the user, such as demographic information, browsing history, location, and the page being loaded.
2. The SSP then sends it over to the Demand Side Platform (“DSP”) that automatically submit bids on behalf of advertisers for the users that match the advertiser’s criteria.
3. The highest bid will win, and the ad will be shown to the user.

This real-time bidding occurs automatically and near-instantaneously.

As such, advertisers today are typically reliant on a supply chain comprised of various intermediaries, including these adtech companies, the ad agencies that plan and execute campaigns on their behalf, and data brokers. For every dollar a business spends on digital ads, each of these intermediaries gets a percentage revenue share, with most paid based on volume. This creates dysfunctional incentives, as every company in the middle stands to gain by having more money pass through their pipes. In addition, in each transaction, these middlemen get access to personal data. This is how programmatic advertising has resulted in constant tracking and widespread sale and leakage of consumer personal data.

³ See Mike Sweeney, *What Is Programmatic Advertising? Everything You Need to Know in 2023*, CLEARCODE (Apr. 21, 2020), <https://clearcode.cc/blog/programmatic-advertising/> (last visited Mar 12, 2025).

Yet, while this process sounds efficient and powerful in theory, the reality is much different. Out of every dollar spent on programmatic advertising, only 36 cents makes it to the publisher.⁴ 29 cents of the ad dollar goes to adtech intermediaries, and 35 cents is wasted on fraud, invalid (e.g. bot) traffic, low-quality made-for-advertising (“MFA”) websites.⁵ The average programmatic ad campaign serves on 44,000 websites.⁶ All the while, even the biggest advertisers, with the most leverage, have limited ability to confirm where exactly their ads appeared.⁷

These figures, produced by leading advertiser trade association, the Association of National Advertisers (“ANA”), represent a *conservative* estimate. This estimate does not, for example, account for ad agency fees. It does not include the money wasted on ineffective ad verification tools that advertisers use in an attempt to make sure their ads go where they want them to go, and are seen by real people.⁸ Nor does it include wasted spending on advertising that, while not technically meeting industry definitions of ad fraud, does not adhere to the criteria outlined by advertisers. Thus, while research suggests that ad fraud accounts for a whopping \$84 billion⁹ in global spend – placing it second only to the drug trade as a source of revenue for organized crime – that is just the tip of the iceberg as it comes to advertiser waste.¹⁰

Bad incentives hurt small businesses.

For small businesses, this is not only detrimental to their growth, but at times, to their survival. Recently, Check My Ads Institute launched an advertising campaign with the

⁴ Association of National Advertisers, ANA Programmatic Media Supply Chain Transparency Study: Complete Report, <https://www.ana.net/miccontent/show/id/rr-2023-12-ana-programmatic-media-supply-chain-transparency-study> (last visited Mar 7, 2025).

⁵ *Id.*

⁶ *Id.*

⁷ See, e.g. Kendra Barnett, *Buyers Blame Adtech Opacity for Funding Child Abuse Online*, (Feb. 7, 2025), <https://www.adweek.com/media/ad-buyers-blast-google-amazon-and-others-after-ads-appear-on-site-hosting-child-abuse-content/> (last visited Mar 12, 2025).

⁸ See, e.g. Seb Joseph, *Ad Verification Is under Fire: Ad Execs Are Questioning Its Role as Protector*, DIGIDAY (2024), <https://digiday.com/marketing/ad-verification-is-under-fire-ad-execs-are-questioning-its-role-as-protector/> (last visited Mar 12, 2025); Marty Swant, *Amazon, Google and Verification Vendors among Ad Tech Cohort under Fire from U.S. Senators over Child Safety Shortcomings*, DIGIDAY (2025), <https://digiday.com/media-buying/amazon-google-and-verification-vendors-among-ad-tech-cohort-under-fire-from-u-s-senators-over-child-safety-shortcomings/> (last visited Mar 12, 2025).

⁹ QUANTIFYING THE COST OF AD FRAUD: 2023-2028, (2023), <https://fraudblocker.com/ad-fraud-data-facts> (last visited Mar 5, 2025).

¹⁰ Press Release, *Sens. Warner & Schumer Call on FTC to Protect Consumers from Digital Ad Fraud* (July 11, 2016), <https://www.warner.senate.gov/public/index.cfm/2016/7/sens-warner-schumer-call-on-ftc-to-protect-consumers-from-digital-ad-fraud/>; Press Release, Sen. Mark R. Warner, *Warner Calls on FTC and Google to Address the Prevalence of Digital Ad Fraud* (Oct. 25, 2018), <https://www.warner.senate.gov/public/index.cfm/2018/10/warner-calls-on-ftc-and-google-to-address-the-prevalence-of-digital-ad-fraud/>; WFA issues first advice for combatting ad fraud - World Federation of Advertisers, <https://wfanet.org/knowledge/item/2016/06/06/WFA-issues-first-advice-for-combatting-ad-fraud/> (last visited Mar 12, 2025).

intention of emanating the experience of an average small business user. We set up a Google Ads account, as millions of other small businesses do.¹¹ We were nudged into Google's AI-driven, opaque product, Performance Max, which is notorious for restricting advertiser transparency and control, and has a history of placing ads on potentially illegal content, while ignoring advertiser targeting criteria.¹²

Unsurprisingly, our ads were served exclusively¹³ on AI-generated spam websites and other low-quality websites more likely to attract bot clicks than real humans.¹⁴ Our ads appeared on YouTube videos in other languages, when we explicitly chose to target English language content. Indeed, with some of our ads landing on kids' videos, we have no idea *who* Google's algorithm targeted.¹⁵ Due to the opacity of the product, a small business cannot determine which websites or YouTube channels increased sales or which audiences drove revenue.¹⁶ While Google gets more money and more data, small businesses are merely the unwitting conduit.

The same phenomenon occurs outside of Google's products. The consumer data peddled by data brokers for ad targeting, while being invasively collected, is also astoundingly

¹¹ See, *Plaintiff's Trial Exhibit 1231*, United States v. Google LLC, No. 1:23-cv-00108 (E.D. Va.), <https://www.justice.gov/atr/media/1369916/dl>.

¹² See, e.g., Kali Hays, *Google Served Ads on Sanctioned Websites, Adalytics Report Says*, BUS. INSIDER (Apr. 6, 2022), <https://www.businessinsider.com/google-served-ads-sanctioned-websites-adalytics-report-russia-2022-4>; *Google advertises on sanctioned sites, according to report*, FINANCIAL TIMES (Nov. 28, 2023), <https://www.ft.com/content/45101fb1-83d3-4b28-87ac-de562be9fb31>; Claire Atkin & Nandini Jammi, *Google Search Ads Lack Transparency*, CHECK MY ADS (Dec. 14, 2023), <https://checkmyads.org/google-search-ads-no-transparency/>.

¹³ Google's Performance Max ("PMax") product places ads across both Google's own properties (e.g. YouTube, Search), as well as across third party websites and apps – known as Google's "network." This comment refers specifically to network ad placements.

¹⁴ The details of the Check My Ads Institute advertising campaign placements can be accessed here: https://www.dropbox.com/scl/fi/b82iwmksktszeflkoyxb7/PMAX_Placements_Backup.pptx?rlkey=aszmumgmattlpwwc7ai5h8v4ak&dl=0/

¹⁵ This is not the first instance where Google has appeared to serve adult-targeted ads to children. Natasha Singer, *YouTube and Google Are Accused of Violating Children's Privacy*, N.Y. TIMES (Aug. 17, 2023), <https://www.nytimes.com/2023/08/17/technology/youtube-google-children-privacy.html>; Press Release, Sen. Edward J. Markey, *Senators Markey, Blackburn Demand FTC Investigate YouTube, Google for Suspected Violations of Children's Privacy* (Aug. 17, 2023), <https://www.markey.senate.gov/news/press-releases/senators-markey-blackburn-demand-ftc-investigate-youtube-google-for-suspected-violations-of-childrens-privacy/>.

¹⁶ See, e.g., *Sweetgreen Admedia: Google Search Advertising*, ADWEEK (Apr. 15, 2024), <https://www.adweek.com/media/sweetgreen-admedia-google-search-advertising/> ("... buyers have complained that Performance Max is a black box. Specifically, advertisers say there's no sufficient controls on where ads go or reporting data on where ads actually ended up"); *Are YouTube Ads COPPA Compliant?*, ADALYTICS, <https://adalytics.io/blog/are-youtube-ads-coppa-compliant> ("...advertisers report they cannot audit this issue because Pmax does not provide them with granular placement reports."); Department of Justice, *Proposed Remedies for Search Trial: Access to Data Reports*, <https://storage.courtlistener.com/recap/gov.uscourts.dcd.223205/gov.uscourts.dcd.223205.1062.1.1.pdf> (last visited Jan. 16, 2024) ("Google must not limit the ability of advertisers to export in real time...data or information relating to their entire portfolio of ads or advertising campaigns bid on, placed through, or purchased through Google, including data relating to placement or performance (i.e., conversion data)."); Lara O'Reilly, *IPG Mediabrands 'Privacy Alert' Says Clients Should 'Consider' a Pause on Google Ads Product*, BUS. INSIDER (Aug. 17, 2023), <https://www.businessinsider.com/ipg-mediabrands-privacy-alert-pause-google-performance-max-ads-2023-8/>.

ineffective for marketing.¹⁷ Research has shown that leading ad data brokers were only right about people's gender 42% of the time – worse than guessing at random. This is what advertisers are paying for.¹⁸

My own desktop research echoed these findings.¹⁹ One ad platform held over 500 audience segments to which I belonged, which it received from seven different data brokers. To their credit, supplying this much information is very uncommon in the absence of universal legal requirements. Yet, these audiences were highly inaccurate, often contradictory, and sometimes sensitive. According to this data, I'm both high income and below the poverty level. I'm listed as both a middle-aged suburban homeowner without kids, as well as a mother of two. I am neither. I am, according to my profile: a defense contractor, I work in food service, and agriculture. I was identified as likely suffering from heart disease, speaking Spanish, and celebrating Ramadan. None of these things are true. While the industry has finally started to acknowledge²⁰ these data quality realities out loud, this insight is far less accessible to small businesses.

The harms of online surveillance outweigh alleged benefits.

Nevertheless, right or wrong, this data can be used – within and beyond advertising – in ways that cause real harm. The Chief Privacy Officer of Acxiom - one of the world's largest data brokers - has admitted that their consumer data used by advertisers around the world is comprised of little more than “informed guesses.”²¹ He said he “hopes” that if they guess

¹⁷ Jack Neff, *Disturbing Findings from a Personal Data Journey / Ad Age*, <https://adage.com/article/data-driven-marketing/disturbing-findings-personal-data-journey/2577746/> (last visited Mar 12, 2025); Nico Neumann, Catherine E. Tucker & Timothy Whitfield, *How Effective Is Third-Party Consumer Profiling and Audience Delivery?: Evidence from Field Studies*, (2019), <https://papers.ssrn.com/abstract=3203131/> (last visited Mar 12, 2025); 'Marketers are buying this': Pitfalls and 'lies' to avoid on junk user data, clean room matching, MMM, incrementality tests and B2B tech – Melbourne Business School Associate Professor Nico Neumann | Mi3, <http://www.mi-3.com.au/04-02-2025/marketers-are-buying-pitfalls-and-lies-avoid-junk-user-data-clean-room-matching-mmm/> (last visited Mar 8, 2025).

¹⁸ Neumann, Tucker, and Whitfield, *supra* note 18.

¹⁹ The details from Arielle Garcia's access request, as excerpted from presentation at Programmatic/IO 2024: [https://www.dropbox.com/scl/fi/fd2fgu0xtm4jlrxfkn2/Programmatic-IO ArielleGarcia 2024 Excerpts.pptx?rlkey=uznf6cmmgblab2wce27vg3he2&dl=0/](https://www.dropbox.com/scl/fi/fd2fgu0xtm4jlrxfkn2/Programmatic-IO%20ArielleGarcia%202024%20Excerpts.pptx?rlkey=uznf6cmmgblab2wce27vg3he2&dl=0/) (Additional detail can be provided upon request).

²⁰ \$700bn delusion: Does using data to target specific audiences make advertising more effective? Latest studies suggest not | Mi3, <http://www.mi-3.com.au/26-06-2024/data-delusion-does-using-data-target-specific-audiences-advertising-actually-make/> (last visited Mar 12, 2025); Jack Neff, *supra* note 18; Neumann, Tucker, and Whitfield, *supra* note 18; Suzanne Smalley, "Junk Inferences" by Data Brokers Are a Problem for Consumers and the Industry Itself, <https://therecord.media/junk-inferences-data-brokers/> (last visited Mar 8, 2025); 'Marketers are buying this', *supra* note 18.

²¹ Suzanne Smalley, *supra* note 21.

wrong, it doesn't have any negative consequences for denial of benefits or credit.²² But, credit reference agencies have purchased and used Acxiom's data to determine credit worthiness.²³

Another data broker, named Epsilon, now also owned by an ad giant, has sold data to perpetrators of elder fraud.²⁴ Its parent company, Publicis, recently announced its acquisition of another data broker which it claims will give it deep insight into 91% of the world population.²⁵ This same company's Health unit entered a \$350M settlement for its role in the Opioid crisis.²⁶ As Attorney General Frey may recall, among the allegations, Publicis Health was accused of using doctor-patient recording data to glean insights on how to more effectively push opioids on pain sufferers in "higher and higher doses."²⁷ Meanwhile, its data broker unit, as recently as 2021, continued to sell data pertaining to pain sufferers, and may still do so to this day.

These harmful practices aren't the exception – they're the rule. These are a few examples of audience segments readily-available through LiveRamp's data marketplace, with limited restriction, to advertisers around the world:²⁸

- Individuals likely to have a condition that results in chronic pain
- Employee devices who work for the military
- Audience consists of mobile ad IDs collected at US military bases
- People who work at the US Department of Defense

Without strong privacy laws that codify transparency and choice, include principles of data minimization, and restrict use of sensitive data, these data-enabled harms will continue

²² *Id.*

²³ Data trading between credit agency and address trader illegal, <https://noyb.eu/en/data-trading-between-credit-agency-and-address-trader-illegal/> (last visited Mar 8, 2025).

²⁴ Office of Public Affairs | Marketing Company Agrees to Pay \$150 Million for Facilitating Elder Fraud Schemes | United States Department of Justice, (2021), <https://www.justice.gov/archives/opa/pr/marketing-company-agrees-pay-150-million-facilitating-elder-fraud-schemes/> (last visited Mar 8, 2025).

²⁵ CoreAI - YouTube, <https://www.youtube.com/watch?v=YCsEOYbH3vI/> (last visited Mar 12, 2025); Rebecca Stewart, *Inside Publicis Groupe's Surprise Acquisition of ID Business Lotame*, (Mar. 6, 2025), <https://www.adweek.com/agencies/inside-publicis-groupe-surprise-acquisition-of-id-business-lotame/> (last visited Mar 12, 2025).

²⁶ Attorney General Aaron M. Frey Announces \$350 million Settlement with Multinational Marketing Firm Publicis Over Role in Opioid Epidemic, OFFICE OF THE MAINE ATTORNEY GENERAL (Feb. 1, 2024), <https://www.maine.gov/ag/news/article.shtml?id=12348301> (last visited May 1, 2025).

²⁷ *Commonwealth v. Publicis Health, LLC*, No. 21-1055, at 27 (Mass. Super. Ct. Sept. 27, 2021) (complaint) ("[A]fter analyzing recordings of conversations between doctors and patients, Verilogue told Purdue...Purdue could use direct 'patient education' efforts too, Publicis said, to get patients comfortable with taking OxyContin, including in higher and higher doses."); Arielle Garcia, *What Do We Say To Emily? The Human Cost Of Advertising Data Abuse*, ADEXCHANGER (2024), <https://www.adexchanger.com/data-driven-thinking/what-do-we-say-to-emily-the-human-cost-of-advertising-data-abuse/> (last visited Mar 12, 2025).

²⁸ Ethan Ehrenhaft, *LiveRamp: Company Hosts Marketplace Selling Datasets That Target Millions of Americans Based on Sensitive Information, Military Status*, THE CAPITOL FORUM, Apr. 8, 2025, <https://thecapitolforum.com/liveramp-company-hosts-marketplace-selling-datasets-that-target-millions/> (last visited Apr 9, 2025).

unchecked. All of this so that data brokers and adtech companies can sell data that has less than a 50% chance of being accurate to unsuspecting small business advertisers?

This isn't efficiency. It's a dangerous market failure.

This bill would help make advertising *more* effective, not less.

This bill that would protect the privacy of Maine residents is not at odds with relevant, effective advertising. Nor would this bill end all targeted advertising.

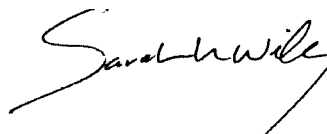
What it would do is reduce the supply of low-quality data at the core of the broken adtech market. It would allow for brands, publishers and other companies with legitimate customer relationships, built on a fair value exchange, to realize the value of those assets. Ultimately, it would create the conditions for more relevant advertising that benefits Maine businesses, while restricting the harmful practices that undermine the safety, liberty, and security of its citizens.

We appreciate the leadership that this Committee, and particularly Chairs Carney and Kuhn have shown towards enacting meaningful privacy protections for Maine residents. Thank you for the opportunity to testify in support of LD 1822 and contribute to the record. We are happy to answer any further questions, and to remain a resource for the Maine Legislature.

Sincerely,



Arielle Garcia
Chief Operating Officer
Check My Ads Institute
arielle@checkmyads.org



Sarah Kay Wiley
Director of Policy
Check My Ads Institute
sarah@checkmyads.org

Bruce C. Gerrity
bgerrity@preti.com
207.623.5300

May 7, 2025

Senator Anne Carney
Representative Kuhn
Judiciary Committee
3 State House Station
State House, Room 438,
Augusta, Maine 04333

RE: LD 1088 An Act to Enact the Maine Consumer Data Privacy Act
LD 1224 An Act to Comprehensively Protect Consumer Privacy
LD 1284 An Act to Repeal Provisions of Law Governing the Privacy of
Broadband Internet Customer Personal Information
LD 1822 An Act to Enact the Maine Online Data Privacy Act

Dear: Senator Carney and Representative Kuhn,

These comments augment the testimony presented at the public hearing on the above bills. The Maine Automobile Dealers Association (MADA) is the Association of all new car and truck dealers in Maine. Maine dealers are required to comply with a number of different statutes which impose varying privacy obligations. As such, Maine dealers should be fully exempt from the various provisions of the proposed legislation.

Several of the proposed bills before the Committee do exempt data provisions, such as the Gramm-Leach-Bliley Act (GLBA). Dealers are regulated by GLBA. Dealers are also broadly regulated by the Federal Trade Commission (FTC) (15 USC, section 41 et seq.), and more specifically, by the Fair Credit Reporting Act, (15 USC, section 1681 (FCRA)) and the Fair and Accurate Credit Transaction Act (FACT Act), (15 USC, section 1601). These two laws, along with the FTC Rules and regulations, protect consumer data in relation to credit transactions, and more broadly, information received from consumers by dealers. The Red Flags Rule is part of FTC regulation, also known as the FACT Act Identity Theft Rules. This rule requires dealers to implement a written identity theft prevention program designed to detect warning signs of identity theft. This involves protecting sensitive consumer information. The Red Flags Rule was issued in 2007 under section 114 of the FACT Act, which in turn amended the FCRA. The Rule is published at 16 CFR 681.1.

In addition, even though dealers have obligations to keep data and consumer information private, they are also required to report to the Internal Revenue Service (IRS) the receipt of cash or cash equivalents of more than \$10,000 in a single transaction or two or more related transactions. IRS form 8300: BSA E-FILING System. This requires reporting "identifying documents" in some detail.

May 7, 2025

Page 2

In addition, MADA runs a Multiple Employer Welfare Arrangement (MEWA). This is a self-insured health plan offering coverage to dealers and their employees and families. It is regulated by the Bureau of Insurance. 24-A MRS ch.81. This regulatory authority extends to the privacy chapter of Title 24-A (24-A MRSA ch.24). This means dealers' privacy requirements are also regulated by the Bureau.

Also, telematics is now a critical component of owning and operating a motor vehicle. As such, Maine dealers are privy to significant consumer information stored in a vehicle's electronic components. The Maine right to repair statute, 29-A MRS §1801 et seq., does regulate access to telematics for repairs. The Housing and Economic Development Committee (HED) has received a report authorized pursuant to resolve 2023, ch.171 to advise it about various aspects of Right to Repair.

<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwis77Wd1JGNAXW5G1kFHfIgH-0QFnoECBcQAQ&url=https%3A%2F%2Fwww.legislature.maine.gov%2Fdoc%2F11596&usg=AOvVaw29lSIId8edWeD7ochlOBV7a&opi=89978449>

Central among those issues are consumer privacy protections, safety protections, and cyber security. The HED Committee is reviewing several bills, which include LDs 292, An Act to Implement the Automotive Right to Repair Working Group Recommendations, 442, An Act to Amend the Automotive Repair Statute, 1227, An Act to Repeal the Requirements That Motor Vehicle Manufacturers Equip Vehicles with a Standardized Data Access Platform, 1228, An Act to Clarify Certain Terms in the Automotive Right to Repair Laws, 1394, An Act to Support Maine's Electric Vehicle Adoption Goals by Providing an Exclusion for Electric Vehicles from Certain Requirements of the Right to Repair Law, 1467, An Act to Ensure Accountability for Repairs Conducted by Independent Repair Facilities on Motor Vehicles Under Warranty, and 1468, An Act to Establish Standards for Independent Motor Vehicle Repair Facilities in Maine. In short, the HED Committee is working on its own set of privacy and cyber security rules and obligations, which will apply to dealers, to protect consumers in the context of the repair of motor vehicles and access to privacy protected information which are part of a telematic system.

Given the broad nature of auto dealer obligations arising out of disclosures, consumer privacy, protected consumer and cyber security data under several federal and Maine laws, it is appropriate to exempt the Maine automobile dealers from the provisions of the bills under consideration by the Committee. Adding additional obligations can only create confusion, notification requirements and obligations that may be inconsistent and will not further the goals of the various bills before the Committee.

Respectfully submitted,

Bruce C. Gerrity

PRETI FLAHERTY

May 7, 2025

Page 3

BCG:mlb



May 2, 2025

Chairs Anne Carney, Amy D. Kuhn, and Members of the Committee
Joint Committee on Judiciary
Maine Legislature

RE: Bill Nos. LD 1088 | LD 1224 | LD 1822

Dear Chairs Carney, Kuhn, and Members of the Committee:

Headquartered in Oak Brook, Illinois, and with a 113-year history, the National Insurance Crime Bureau (NICB) is the nation's premier not-for-profit organization exclusively dedicated to leading a united effort to prevent insurance crime and fraud through intelligence-driven operations. NICB's 400-plus employees sit at the intersection between the insurance industry and law enforcement. NICB maintains operations in every state around the country, including in Maine where NICB is a longstanding, trusted partner in the fight against insurance fraud. NICB analysts and agents work daily with federal, state and local Maine law enforcement and regulatory agencies to provide assistance in all manner of cases, including the Maine State Police and Maine Bureau of Motor Vehicles.

Maine's Insurance Crime Reporting Requirements

Recognizing the adverse impact of insurance crime on the citizens of Maine, the legislature enacted laws requiring Maine insurers to report suspected insurance fraud to the Bureau of Insurance.ⁱ In the vast majority of cases, insurers submit suspected fraud referrals to the BOI through NICB's Fraud Bureau Reporting Program (FBRP). The FBRP connects through the National Association of Insurance Commissioners' Online Fraud Reporting System to deliver fraud reporting information to regulators. In addition to mandating that information be provided to the State, the Maine State Legislature also recognized the importance of reporting insurance crime and fraud information to law enforcement by enacting a statute providing civil immunity to any person and insurance professionals delivering such information to law enforcement and regulatory agencies in Maine.ⁱⁱ

Maine's Insurance Information and Privacy Protection Act

The Insurance Information and Privacy Protection Act was enacted to provide rules and regulatory oversight for insurance companies, agents, and insurance-support organizations, such as NICB, with regard to handling the personal information of policyholders. That law also provided a specific carve-out for certain disclosures, including those made for purposes of detecting or preventing criminal activity or fraud, reporting to a regulatory agency, or reporting to law enforcement.ⁱⁱⁱ By enacting this statute, Maine has addressed and preserved privacy interests for consumers in the insurance realm; and recognized the need for the free flow of information relating to fraud.

Impact of the Various Consumer Data Privacy Bills on NICB

NICB's anti-fraud efforts currently benefit from exemptions from the 16 enacted comprehensive consumer data privacy laws across the country, ensuring that NICB's limited resources as a non-profit remain directed at our fraud-fighting mission—a public benefit we provide to Maine residents at no cost. Limited exceptions for preventing, detecting, and protecting against fraud and illegal activity would not provide a wholesale exemption for such activities. Such limited exceptions would subject NICB to complex compliance obligations that would interfere with our vital information-sharing role and fraud-fighting mission. The policy reasons for excluding NICB from these burdens are several-fold. First, NICB provides a significant public benefit to the government and the millions of consumers who are victims of insurance fraud. Second, as a non-profit organization that serves a public interest, NICB is not equally situated with private entities that typically establish more complex compliance infrastructure for private-sector-related obligations. Third, NICB would become subject to consumer requests to, for example, confirm the existence of (or to delete) data. Even for non-viable requests, NICB would nevertheless bear the burden of proving to each consumer directly, or in litigation, that NICB's activities fall within the limitation. The obligation to do so would strain our organization's resources to such a degree that our operations, and ability to protect Maine consumers, would be significantly encumbered. Lastly, NICB's required responses to individual consumer requests would likely expose otherwise covert criminal investigations. For example, a fraudster could demand that NICB confirm we are processing that individual's data. A mere response from NICB tying that information to a fraud-related purpose would provide a clear signal to that individual, thereby exposing an investigation.

NICB's Request and Policy Rationale

Imposing what is essentially a “compliance, response, reporting and litigation” obligation – without any benefit to consumers – is inconsistent with Maine's insurance fraud reporting requirements and civil immunity provisions. These were enacted to facilitate, not impede, the mandatory flow of insurance fraud information to state authorities. Consistent with longstanding public policy determinations providing for the protection and flow of insurance fraud reporting information already considered and enacted in Maine law, NICB respectfully requests an entity-level exemption from the various bills.

Thank you for considering our views. As always, please consider NICB a resource and partner in the fight against insurance crime. If you have any questions or need additional information, please contact me at hhandler@nicb.org or 312-771-3974.

Sincerely,



Howard Handler, Senior Director
Strategy, Policy and Government Affairs

ⁱ 24-A M.R.S. § 2186

ⁱⁱ 24-A M.R.S. § 2187

ⁱⁱⁱ 24-A M.R.S. § 2215



Post Office Box 587
Augusta, ME 04332-0587

t: 207.622.7524

f: 207.622.0836

Testimony in support:

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

Testimony in opposition:

LD 1088, "An Act to Enact the Maine Consumer Data Privacy Act"

LD 1224, "An Act to Comprehensively Protect Consumer Privacy" and

LD 1284, "An Act to Repeal Provisions of Law Governing the Privacy of Broadband Internet
Customer Personal Information"

Joint Standing Committee on Judiciary

May 5, 2025

Senator Carney, Representative Kuhn and members of the Joint Standing Committee on Judiciary, my name is Laura Harper. I'm a senior associate at Moose Ridge Associates and I live in Hallowell. I am here today on behalf of my client, Maine Family Planning (MFP) to speak in support of LD 1822, "An Act to Enact the Maine Online Data Privacy Act" and against LD 1088, "An Act to Enact the Maine Consumer Data Privacy Act," LD 1224, "An Act to Comprehensively Protect Consumer Privacy" and LD 1284, "An Act to Repeal Provisions of Law Governing the Privacy of Broadband Internet Customer Personal Information."

MFP provides comprehensive sexual and reproductive health care to teens and adults at 19 locations statewide. Our mission is to ensure that all people have access to high-quality, culturally relevant and affordable sexual and reproductive health care services, comprehensive sexual health education, and the right to control their sexual and reproductive lives. One of the cornerstones to maintaining this access is protecting our patients' privacy, including their electronic data.

One doesn't need to look far to discover the latest attack on people's reproductive privacy. Most recently, our health centers have been under the threat of a Federal investigation for supposed civil rights violations inextricably connected to our mission to provide unbiased, evidence-based care to every patient who seeks our services, regardless of their immigration status, gender identity, race, or sexual orientation. This unproven Federal allegation has served as a groundless pretext for the Federal authorities to freeze our Title X funding, a long-standing investment in public health and family planning services by the U.S. government. Now more than ever, we need Maine law to provide the most comprehensive protection for our providers and patients. LD 1822 provides important tools so that our doors remain open and patients can access the life saving healthcare we've provided for over 50 years, free of government intrusions and/or corporate surveillance.

For example, some of our patients find menstrual cycle apps helpful to monitor their menstruation. These apps collect deeply personal, sensitive data on when a person has their period, when they are ovulating, if and when they may experience pre-menstrual syndrome and other information. Most consumers assume that this data is kept private and covered under HIPPA protections; instead they are at the whim of the privacy policies set by the app vendors. Without the protections in LD 1822, our patients fear their menstrual data and information regarding pregnancy and abortion care could be sold. We hear from our patients that many are already afraid to use these apps for fear of legal action in states where abortion and other sexual and reproductive health care is banned. LD 1822 will help to strengthen Maine's Shield Law, ensuring that all people can safely access abortion care here in Maine without fear. This bill would also help to eliminate fears of being geolocated while accessing lifesaving healthcare. In short, more data privacy equals better access to healthcare.¹

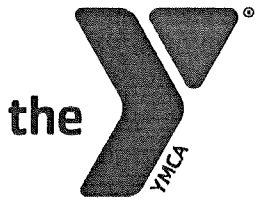
Of the four bills before you, LD 1822 is the only one that categorically prohibits collection of personal data. In contrast, LDs 1088 and 1224 would allow collection of sensitive data as long as the consumer clicks "I agree."² Most of us click "I agree" without a second thought, so these bills would not provide any meaningful protections for a majority of Maine people.

For these reasons and more, we oppose LDs 1088, 1224, and 1284; these bills lack the consumer protections our patients and providers need to safely access sexual and reproductive health services while keeping their personal data private.

In closing, we ask you to please vote LD 1822, "ought to pass" and to oppose LDs 1088, 1224 and 1284. Thank you for your attention and I'm happy to try to answer any questions you may have.

¹ LD 1088 also contains an anti-geofencing provision, but its data minimization provision would allow any collection or use of data as long as it is disclosed in a privacy policy. See LD 1088, p. 10, lines 7-20.

² See LD 1088, p. 10-11; LD 1224, p. 10.



FOR YOUTH DEVELOPMENT®
FOR HEALTHY LIVING
FOR SOCIAL RESPONSIBILITY

Testimony of Meg Helming
before the Committee on Judiciary
Neither For Nor Against

LD 1088: An Act To Enact The Maine Consumer Data Privacy Act

LD 1224: An Act To Comprehensively Protect Consumer Privacy

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

May 5, 2025

Senator Carney, Representative Kuhn, and honorable members of the Committee on Judiciary, my name is Meg Helming and I am the COO of the YMCA Alliance of Northern New England, which represents the 15 YMCAs in Maine. The YMCA would like to offer comments on LDs 1088, 1224, and 1822.

The first YMCA in Maine was founded in 1853. Today, the 15 Ys in this state serve 95,000 Mainers each year through our diverse array of programming. The Maine YMCAs provide essential services in our communities to support our state's economy and some of our most vulnerable residents. At the Y, these services include childcare, wellness, hunger relief, and community-based chronic disease prevention programs.

We greatly appreciate Representative Kuhn's recognition of the important role nonprofits play in serving our communities by exempting us from LD 1822. We strongly support efforts to strengthen data privacy protections for consumers and believe this can be achieved while also ensuring that nonprofits are exempt. Clear exemptions will help safeguard vital community services, all while maintaining responsible data stewardship across sectors.

We respectfully urge the Committee to include a nonprofit exemption in any of the privacy bills that advance out of Committee.

Sincerely,

Meg Helming
YMCA Alliance of Northern New England

Representing:

Bangor Region YMCA • Bath Area Family YMCA • Boothbay Region YMCA • Central Lincoln County YMCA
• Down East Family YMCA • Kennebec Valley YMCA • Mount Desert Island YMCA • Old Town Orono
YMCA • Penobscot Bay YMCA • Sanford-Springvale YMCA • State YMCA Camp of Maine • Waldo County
YMCA • YMCA of Auburn-Lewiston • YMCA of Greater Waterville • YMCA of Southern Maine

Contact: Meg Helming, COO, YMCA Alliance of Northern New England
P: 207.232.9896 **E:** meg.helming@nneymcas.org

TESTIMONY OF MICHAEL KEBEDE, ESQ.



LD 1822 – Ought to Pass
An Act to Enact the Maine Online Data Privacy Act

LDs 1224, 1088, 1284 – Ought Not to Pass
An Act to Comprehensively Protect Consumer Privacy
An Act to Enact the Maine Consumer Data Privacy Act
An Act to Repeal Provisions of Law Governing the Privacy of
Broadband Internet Customer Personal Information

PO Box 7860
Portland, ME 04112

Joint Standing Committee on Judiciary
May 5, 2025

(207) 774-5444
ACLUMaine.org
@ACLUMaine

Senator Carney, Representative Kuhn and distinguished members of the Joint Standing Committee on Judiciary, greetings. My name is Michael Kebede and I am policy director at the ACLU of Maine, a statewide organization committed to advancing and preserving civil liberties guaranteed by the Maine and U.S. Constitutions. On behalf of our members, I urge you to support LD 1822 and oppose LDs 1224, 1088, and 1284.

The ACLU has a long history of protecting the right to privacy, both as it pertains to governmental and to business intrusions into that right. The ACLU of Maine was instrumental in the drafting and passage of several of our state's seminal privacy laws, including our internet service provider privacy law, which is the strongest in the nation,¹ the law restricting the government's ability to use facial recognition technology, also the nation's strongest,² and the law requiring a warrant in order for law enforcement to access portable electronic information or cell phone location information.³ Two of the bills before you today – LDs 1088 and 1284 – would repeal our internet privacy law. LD 1088 goes further, as does LD 1224, to propose industry-written rules that would not provide Maine people with enough protections. Only LD 1822 would meaningfully expand privacy rights.

The Need for Meaningful Privacy Legislation

Large technology companies have built a surveillance economy that seeks to collect and monetize as much information about us as possible. These companies harvest data about what we do at home, what we do at work, what we buy, where we go, what doctors we see,

¹ See 35-A M.R.S. §9301.

² See 25 M.R.S. §6001.

³ See 16 M.R.S. §641 et seq., §647 et seq.

our contacts with the criminal and civil legal systems, and virtually any other measurable dimension of our behavior. In the United States, these companies face almost no real restrictions on the amount of personal information they can amass about us or the ways that they can exploit it. In the absence of meaningful protections, companies have compiled staggering amounts of information about each of us. This information can identify us across our interactions with the world both online and off, in public and in private, enabling an unprecedented power to predict and modify our behavior.

These unprecedented powers to predict and modify our behavior can be and are being sold to data brokers or used to manipulate public opinion, power surveillance-based advertising, and shape our decisions in any way intended by those able to pay. Many of these uses have discriminatory impacts, such as when companies exclude people from seeing advertisements for employment, housing, or credit on the basis of their gender, race, nationality, or membership in another protected class. Other uses undermine the very foundations of our constitutional democracy, fueling polarization or feeding skepticism about the integrity of our elections. Each of these harms can be traced back to the tech industry's unregulated amassment and analysis of intimate details of our lives.

To stop these harms, consumer privacy legislation must, at a minimum, contain these features:

- **Data minimization.** It is not enough that consumers receive notice of what personal data is collected and shared or that they are able to consent – especially when “notice” and “consent” are functionally legal fictions. “Notice” is commonly provided through privacy policies, and those policies are so dense and lengthy that they fail to provide any real “notice” at all. Similarly, “consent” is often inferred from use of the site or service or by clicking on a banner that provides no information on the service’s data practices. Notice and consent cannot be the only protections that consumers are afforded. Instead, laws must minimize data collection and the ways that data can be used – meaning that services and sites should only be allowed to collect, use, and disclose data as is necessary to provide what the consumer requested. Collecting and storing more data than what is needed to provide a good or service increases the harms of data breaches, since malicious actors can obtain more data than if companies collected only what was necessary.
- **Requiring opt-in consent before companies collect and use our personal information.** Maine’s internet service provider privacy law requires opt-in consent before internet service providers can sell our information, and that is a crucial protection for internet users. The so-called consumer privacy laws in Connecticut, Utah, Colorado, and eleven or so other states often apply “opt-in” only to a limited set of data, which is problematic because data mining and machine learning can use information that is not particularly sensitive to obtain a very specific picture of sensitive information.
- **Civil rights protections.** Our personal data is increasingly used in ways that affect our opportunities in traditionally protected areas of life such as housing, education, employment, and credit. There is ample evidence of the discriminatory harm that artificial

intelligence (AI) and algorithmic systems can cause to already marginalized groups.⁴ Bias is often baked into the outcomes the AI is asked to predict and the data used to train the AI, which can manifest throughout the AI's design, development, implementation, and use. The impact on the daily lives of Americans is unprecedented. Banks and other lenders use AI systems to determine who is eligible for a mortgage or student loan. Housing providers use AI to screen potential tenants. AI now often decides who's helped and who's harmed with influential predictions about who should be jailed pretrial, admitted to college, or hired. A comprehensive privacy law must ensure that the use of our data in AI adheres to our foundational values of equality and nondiscrimination.

- **Private right of action.** A private right of action, especially in a state as small as Maine, is crucial to ensuring that companies are held accountable for breaking the law. The experiences of other states is illustrative: Illinois has a private right of action to enforce violations of its Biometric Information Privacy Act, while Washington and Texas do not. Washington and Texas, though their offices of the Attorney General are much bigger than Maine's, have not meaningfully enforced their biometric privacy laws. The private right of action in Illinois has been enforced by individual litigants. You may hear much about the sky falling in Illinois, but we can learn lessons from that state to ensure that a private right of action serves its intended purpose, rather than jettisoning it altogether.

Of the bills before you today, LD 1822 includes most of these features. It does, however, lack two important features: a private right of action and a data minimization framework that restricts not just collection, but also sale and disclosure of non-sensitive information.⁵ In contrast, not only do LDs 1224 and 1088 also lack a private right of action, but they also lack an adequate data-minimization provision.

Why LDs 1224, 1088, and 1284 Ought Not to Pass

LDs 1088 and 1284 would both repeal our existing internet service provider privacy law, which prohibits internet companies from using or selling your data without your consent.⁶ These bills represent the latest attempt in a long series of the tech industry's attempts to have the legislature repeal or a judge invalidate Maine's internet privacy law. Each of these attempts has failed.⁷ But the tech industry is, apparently, undaunted. That is because repealing our internet privacy law will make it easier for tech companies to collect and monetize information about Mainers, with dire

⁴ Kaveh Waddell, *How Tenant Screening Reports Make It Hard for People to Bounce Back From Tough Times*, Consumer Reports, March 11, 2021, available at <https://www.consumerreports.org/electronics/algorithmic-bias/tenant-screening-reports-make-it-hard-to-bounce-back-from-tough-times-a2331058426/> (showing how tenant-screening algorithms are prone to errors and incorrectly include criminal or eviction records tied to people with similar names); Jeffrey Dastin, *Insight - Amazon scraps secret AI recruiting tool that showed bias against women*, Reuters, Oct. 10, 2018, available at <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/> (reporting about how algorithmic resume scanners preference male candidates, are inaccessible to applicants with disabilities, and may de-preference first-generation college graduates.)

⁵ See LD 1822, p. 12, lines 36-38.

⁶ See 35-A M.R.S. §9301.

⁷ See, e.g., *Internet service providers drop their challenge to Maine privacy law*, BDN, Sept. 6, 2022, available at <https://www.bangordailynews.com/2022/09/06/politics/maine-privacy-law-challenge/>.

consequences for Mainers' privacy, physical safety, and legal jeopardy. We strongly urge this committee to reject these bills and preserve Maine's pathbreaking internet privacy law.

We also urge you to oppose LDs 1088 and 1224. Although the ACLU shares the concerns that prompted the sponsors to propose these bills, we believe that the bills will not have the intended protective effect. LD 1224 would allow any sale or transfer of your data as long as the use is disclosed in a privacy policy.⁸ LD 1088 would similarly allow any sale or transfer of your data as long as it is disclosed in a Terms and Conditions page or you click "I agree".⁹ As you know, nobody really reads Terms and Conditions pages, and most of us click "I agree" without thinking twice. According to one peer-reviewed study, "98% of the participants did not read any agreement" for their cellphone applications.¹⁰ Neither bill would even require tech companies to seek your opt-in permission for the sale of your data, but would instead require you to ask them to stop.¹¹ Similarly, neither LDs 1088 nor 1224 provide meaningful protections against use of our data in invidious discrimination — a crucial supplement to existing civil rights laws as AI increasingly makes decisions about who has access to housing, employment, education, credit, and more.

Conclusion

Thank you for the opportunity to present our testimony on the privacy legislation pending before you. The surveillance economy poses grave threats to democracy and personal autonomy. After carefully analyzing all four bills before you, we have concluded that only LD 1822 would provide meaningful protections.

To be sure, LD 1822 is not perfect: It would not apply to companies that process the data of fewer than 35,000 Maine residents. It exempts nonprofits and other entities. It does not include a private right of action, meaning that Mainers must rely on the Attorney General to enforce their data privacy rights. Its data minimization rule applies to collection but not to disclosure of personal data. These compromises represent a middle-ground between no data privacy protections and the strongest possible protections, and Maryland enacted a very similar compromise last year. Despite its limitations, LD 1822 is a better starting point than any other bill before the legislature. We urge you to support it and oppose LDs 1224, 1088, and 1284.

⁸ See LD 1224 at p. 9, lines 24-32.

⁹ See LD 1088 at p. 10, lines 12-15.

¹⁰ Saadia Nemmaoui et al., *Privacy conditions changes' effects on users' choices and service providers' incomes*, International Journal of Information Management Data Insights, Vol. 3, Issue 1, Apr. 2023, available at <https://www.sciencedirect.com/science/article/pii/S2667096823000204>.

¹¹ LD 1224 at p. 7, line 39; LD 1088 at p. 8, line 30.

May 5, 2025



**Testimony of J.R. Kenny, Maine Alliance of Boys & Girls Clubs
In regard to LD 1088, An Act to Enact the Maine Consumer Data Privacy Act,
LD 1224, An Act to Comprehensively Protect Consumer Privacy and,
LD 1822, An Act to Enact the Maine Online Data Privacy Act**

On behalf of the **Maine Alliance of Boys & Girls Clubs** and the more than **8,000 youth we serve annually at 18 Club sites across Maine**, we appreciate the intent behind **LD 1088, LD 1224, and LD 1822** to enhance consumer data privacy protections in our state. However, we respectfully request that the committee carefully consider the impact these bills may have on nonprofit organizations, including Maine's Boys & Girls Clubs, and provide tailored provisions or exemptions to address our unique operational model and mission.

Boys & Girls Clubs operate within a federated model. Each Club is an independent 501(c)(3) organization, governed by its own board of directors, responsible for its own fundraising, and utilizing resources provided by **Boys & Girls Clubs of America (BGCA)** — including staff training, program curricula, strategic planning support, and data analysis tools. Like other nonprofit service providers, Boys & Girls Clubs collect limited personal information about youth members, families, staff, volunteers, and donors, and always with consent, solely for program delivery, safety, and reporting requirements to funders or for internal evaluation to improve services.

We have several concerns regarding the proposed legislation as currently drafted — specifically around compliance costs, data-sharing provisions, and applicability thresholds for nonprofit organizations. Every dollar that a youth-serving nonprofit like ours must devote to regulatory compliance is a dollar that cannot go toward feeding a child after school, providing academic support, or creating safe spaces for Maine kids during critical out-of-school hours. In other states where similar laws have passed, Boys & Girls Clubs have spent as much as **\$40,000 on legal and consultant fees** to navigate new requirements — a significant strain on already limited nonprofit resources.

Further, because of our **federated structure**, our local Clubs and BGCA would likely be classified as “third parties” under these bills, which could place burdensome restrictions on essential, mission-driven data sharing within our network. This limited, safeguarded sharing of de-identified or aggregated data between local Clubs and our national organization is critical for identifying statewide and national trends, securing grant funding, and continuously improving outcomes for the youth we serve.

Lastly, we note that **nonprofit organizations have historically been excluded from FTC consumer protection enforcement and exempt from most state consumer privacy laws**, given that nonprofits typically do not engage in commercial activity or data monetization. Nonprofits like ours collect only the data necessary to serve our mission and already adhere to strong ethical standards for safeguarding sensitive information.

Boys & Girls Clubs of Southern Maine • Boys & Girls Clubs of Kennebec Valley
Boys & Girls Clubs of Border Towns • Boys & Girls Clubs of Greater Waterville
Boys & Girls Clubs of Bangor

In closing, the Maine Alliance of Boys & Girls Clubs respectfully requests that the committee:

1. **Increase the applicability threshold for nonprofits** to align with other state laws and recognize operational scale — for example, raising the threshold to **100,000 consumers annually**.
2. **Push back enactment dates** for nonprofit organizations to allow time for compliance planning and cost management.
3. **Provide clear guidance and exemptions for nonprofit organizations**, especially those that operate under federated models like ours, to avoid unintended limitations on internal, mission-critical data sharing.

We strongly support efforts to protect the privacy of Maine families — including the thousands of youth and families we serve each year — and believe that thoughtful adjustments to these bills can achieve that goal while safeguarding the ability of nonprofit organizations to continue serving their communities effectively.

Thank you for your time and consideration.

J.R. Kenny
Lead Director, Government Relations
Maine Alliance of Boys & Girls Clubs
Boys & Girls Clubs of America
770-596-1183
jrkenny@bgca.org