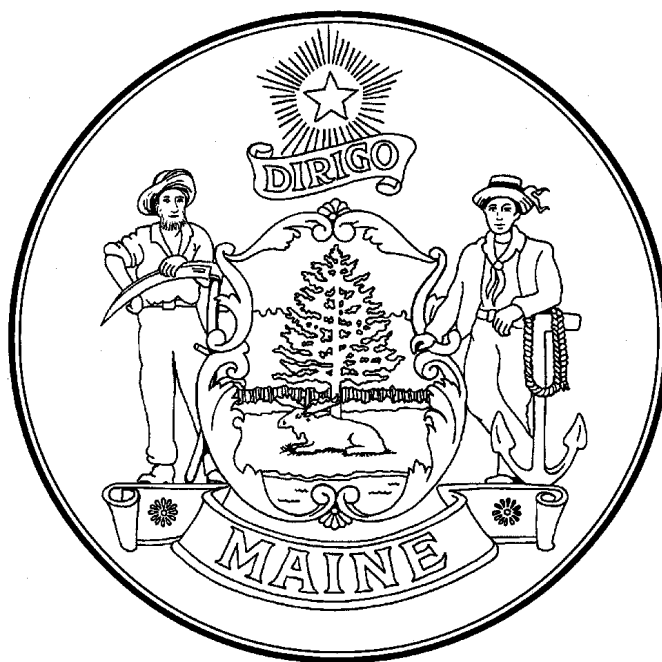


MAINE STATE LEGISLATURE

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: 1088

Title: An Act to Enact the Maine Consumer 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): ONTP
OTP-AM
OTP-AM

Committee History: 5/14/2025 1:36:06 PM Work Session Held
5/23/2025 8:13:23 AM Work Session Held
5/30/2025 8:07:13 AM Work Session Held
5/30/2025 8:08:58 AM Voted
6/4/2025 4:14:24 PM Work Session Reconsidered
6/4/2025 6:55:36 PM Voted



132nd MAINE LEGISLATURE

FIRST REGULAR SESSION-2025

Legislative Document

No. 1088

H.P. 710

House of Representatives, March 18, 2025

An Act to Enact the Maine Consumer Data Privacy Act

Received by the Clerk of the House on March 14, 2025. Referred to the Committee on Judiciary pursuant to Joint Rule 308.2 and ordered printed pursuant to Joint Rule 401.

A handwritten signature in cursive script, reading "R B. Hunt".

ROBERT B. HUNT
Clerk

Presented by Representative HENDERSON of Rumford.

Cosponsored by Representatives: POIRIER of Skowhegan, ROBERTS of South Berwick.

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 CONSUMER DATA PRIVACY ACT**

5 **§9601. Short title**

6 This chapter may be known and cited as "the Maine Consumer Data Privacy 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 business or nonprofit organization that shares
11 common branding with another business or nonprofit organization or controls, is controlled
12 by or is under common control with another business or nonprofit organization.

13 **2. Biometric data.** "Biometric data" means data generated by automatic measurements
14 of an individual's biological characteristics, such as a fingerprint, voiceprint, retina, iris or
15 other unique biological pattern or characteristic that is capable of being used to identify a
16 specific individual. "Biometric data" does not include:

17 A. A digital or physical photograph;

18 B. An audio or video recording;

19 C. Any data generated from a digital or physical photograph or an audio or video
20 recording, unless the data is generated to identify a specific individual; or

21 D. Data collected, used or stored for health care treatment, payment or operations under
22 the federal Health Insurance Portability and Accountability Act of 1996, 42 United
23 States Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and
24 exemptions adopted pursuant to that Act.

25 **3. Business associate.** "Business associate" has the same meaning as in 45 Code of
26 Federal Regulations, Section 160.103.

27 **4. Child.** "Child" means an individual who has not attained 13 years of age.

28 **5. Consent.** "Consent" means a clear affirmative act signifying a consumer's freely
29 given, specific, informed and unambiguous agreement to allow the processing of personal
30 data relating to the consumer. "Consent" may include a written statement, including by
31 electronic means, that is made in the language that the consumer uses to obtain a product
32 or service from the controller and in a format that is reasonably accessible to and usable by
33 consumers with disabilities. "Consent" does not include:

34 A. Acceptance of a terms of use document or similar document that contains
35 descriptions of personal data processing along with other unrelated information;

36 B. Hovering over, muting, pausing or closing a given piece of content; or

37 C. Agreement obtained through the use of a dark pattern.

1 **6. Consumer.** "Consumer" means an individual who is a resident of this State.
2 "Consumer" does not include an individual acting in a commercial or employment context
3 or as an employee, owner, director, officer or contractor of a company, partnership, sole
4 proprietorship, nonprofit organization or government agency whose communications or
5 transactions with the controller occur solely within the context of that individual's role with
6 the company, partnership, sole proprietorship, nonprofit organization or government
7 agency.

8 **7. Consumer health data.** "Consumer health data" means any personal data that a
9 controller uses to identify a consumer's physical or mental health condition or diagnosis.

10 **8. Control.** "Control" means:

11 A. Ownership of, or the power to vote, more than 50% of the outstanding shares of
12 any class of voting security of a company;

13 B. Control in any manner over the election of a majority of the directors of a company
14 or of individuals exercising similar functions in a company; or

15 C. Power to exercise controlling influence over the management of a company.

16 **9. Controller.** "Controller" means a person that, alone or jointly with other persons,
17 determines the purpose and means of processing personal data.

18 **10. Covered entity.** "Covered entity" has the same meaning as in 45 Code of Federal
19 Regulations, Section 160.103.

20 **11. Dark pattern.** "Dark pattern" means a user interface designed or manipulated with
21 the substantial effect of subverting or impairing user autonomy, decision-making or choice
22 and includes, but is not limited to, any practice the Federal Trade Commission refers to as
23 a dark pattern.

24 **12. Decisions that produce legal or similarly significant effects concerning the**
25 consumer. "Decisions that produce legal or similarly significant effects concerning the
26 consumer" means decisions that result in the provision or denial to the consumer of
27 financial or lending services, housing, insurance, education enrollment or opportunity,
28 criminal justice, employment opportunities, health care services or access to essential
29 goods or services.

30 **13. De-identified data.** "De-identified data" means data that cannot reasonably be
31 used to infer information about or otherwise be linked to an identified or identifiable
32 individual, or a device linked to an individual, if the controller that possesses the data:

33 A. Takes reasonable measures to ensure that the de-identified data cannot be associated
34 with an individual;

35 B. Publicly commits to process the de-identified data only in a de-identified fashion
36 and not attempt to re-identify the data; and

37 C. Contractually obligates recipients of the de-identified data to satisfy the criteria set
38 forth in paragraphs A and B.

39 **14. Federally recognized Indian tribe in this State.** "Federally recognized Indian
40 tribe in this State" means the Houlton Band of Maliseet Indians, the Mi'kmaq Nation, the
41 Passamaquoddy Tribe or the Penobscot Nation when the band, nation or tribe is acting in
42 a governmental capacity and not in a business capacity. "Federal recognized Indian tribe

1 in this State" does not include a business entity, including any federally chartered tribal
2 corporation or other business entity owned or partly owned by the Houlton Band of
3 Maliseet Indians, the Mi'kmaq Nation, the Passamaquoddy Tribe or the Penobscot Nation.

4 **15. Geofence.** "Geofence" means technology that uses global positioning system
5 coordinates, cellular tower connectivity, cellular data, radio frequency identification,
6 wireless access point data or any other form of location detection to establish a virtual
7 perimeter around a specific physical location.

8 **16. Nonprofit organization.** "Nonprofit organization" means an organization that is
9 exempt from taxation under Section 501(c)(3), Section 501(c)(4), Section 501(c)(6) or
10 Section 501(c)(12) of the United States Internal Revenue Code of 1986, as amended.

11 **17. Personal data.** "Personal data" means information that is linked or reasonably
12 linkable to an identified or identifiable individual. "Personal data" does not include de-
13 identified data or publicly available information.

14 **18. Precise geolocation data.** "Precise geolocation data" means information derived
15 from technology, including, but not limited to, global positioning system level latitude and
16 longitude coordinates, that directly identifies the specific location of an individual with
17 precision and accuracy within a radius of 1,750 feet. "Precise geolocation data" does not
18 include:

19 A. The content of communications; or

20 B. Data generated by or connected to advanced utility metering infrastructure systems
21 or equipment for use by a utility.

22 **19. Process.** "Process" means an operation or set of operations performed on personal
23 data, including the collection, use, storage, disclosure, analysis, deletion or modification of
24 personal data.

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

27 **21. Profiling.** "Profiling" means any form of automated process performed on personal
28 data to evaluate, analyze or predict personal aspects related to an identified or identifiable
29 individual's economic situation, health, personal preferences, interests, reliability,
30 behavior, location or movements.

31 **22. Protected health information.** "Protected health information" has the same
32 meaning as in the regulations, rules, guidance and exemptions adopted pursuant to the
33 federal Health Insurance Portability and Accountability Act of 1996, 42 United States
34 Code, Chapter 7, Subchapter XI, Part C.

35 **23. Pseudonymous data.** "Pseudonymous data" means personal data that cannot be
36 attributed to a specific individual without the use of additional information, as long as the
37 additional information is kept separately from the personal data and is subject to
38 appropriate technical and organizational measures to ensure that the personal data is not
39 attributed to an identified or identifiable individual.

40 **24. Publicly available information.** "Publicly available information":

41 A. Means information that is:

1 (1) Lawfully made available to the general public through federal, state or local
2 government records;

3 (2) Made available to the general public through widely distributed media;

4 (3) Made available through a website or online service made available to all
5 members of the public, either for free or for a fee, including a website or online
6 service in which all members of the public can log on to the website or online
7 service either for free or for a fee, unless the individual who made the information
8 available via the website or online service has restricted the information to a
9 specific audience;

10 (4) Disclosed to the general public as required by federal, state or local law; or

11 (5) Collected through the visual observation of the physical presence of an
12 individual or by a device located in a public place, not including data collected by
13 a device in the individual's possession; and

14 **B. Does not include:**

15 (1) Any obscene visual depiction as described in 18 United States Code, Section
16 1460;

17 (2) Biometric data;

18 (3) Genetic information, unless the genetic information has been made available to
19 the general public by the individual to whom the genetic information pertains;

20 (4) Inferences derived from a combination of publicly available information and
21 personal data; or

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

27 **25. Sale of personal data.** "Sale of personal data" means the exchange of personal
28 data for monetary or other valuable consideration by the controller to a 3rd party. "Sale of
29 personal data" does not include:

30 A. The disclosure of personal data to a processor that processes the personal data on
31 behalf of the controller;

32 B. The disclosure of personal data to a 3rd party for purposes of providing a product
33 or service requested by the consumer;

34 C. The disclosure or transfer of personal data to an affiliate of the controller;

35 D. The disclosure of personal data when the consumer directs the controller to disclose
36 the personal data or intentionally uses the controller to interact with a 3rd party;

37 E. The disclosure of personal data that the consumer:

38 (1) Intentionally made available to the general public via a channel of mass media;
39 and

40 (2) Did not restrict to a specific audience; or

1 F. The disclosure or transfer of personal data to a 3rd party as an asset that is part of a
2 merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition,
3 bankruptcy or other transaction, in which the 3rd party assumes control of all or part
4 of the controller's assets.

5 **26. Sensitive data.** "Sensitive data" means personal data that includes:

6 A. Data revealing racial or ethnic origins, religious beliefs, mental or physical health
7 conditions or diagnoses, sexual orientation or citizenship or immigration status;

8 B. Genetic or biometric data;

9 C. Consumer health data;

10 D. Personal data collected from a consumer known to be a child;

11 E. Precise geolocation data;

12 F. A social security number, driver's license number or nondriver identification card
13 number, except that "sensitive data" does not include the last 4 digits of a social security
14 number, driver's license number or nondriver identification card number;

15 G. A consumer's account number, log-in information, financial account number or
16 credit or debit card number that, in combination with any required security code, access
17 code or password, permits access to a consumer's financial account; or

18 H. Data concerning an individual's status as a victim of a crime. For the purposes of
19 this paragraph, "victim" has the same meaning as in Title 17-A, section 2101,
20 subsection 2.

21 **27. Targeted advertising.** "Targeted advertising" means displaying an advertisement
22 to a consumer when the advertisement is selected based on personal data obtained or
23 inferred from that consumer's activities over time and across nonaffiliated publicly
24 accessible websites or online applications to predict that consumer's preferences or
25 interests. "Targeted advertising" does not include:

26 A. Advertisements based on activities within a controller's own publicly accessible
27 websites or online applications;

28 B. Advertisements based on the context of a consumer's current search query, visit to
29 a publicly accessible website or online application;

30 C. Advertisements directed to a consumer in response to the consumer's request for
31 information or feedback; or

32 D. Processing personal data solely to measure or report advertising frequency,
33 performance or reach.

34 **28. Trade secret.** "Trade secret" has the same meaning as in section 1542, subsection
35 4.

36 **§9603. Scope**

37 **1. Applicability; July 1, 2026 to December 31, 2027.** From July 1, 2026 to December
38 31, 2027, the provisions of this chapter apply to persons that conduct business in this State
39 or persons that produce products or services that are targeted to residents of this State and
40 that during the preceding calendar year:

1 A. Controlled or processed the personal data of not less than 100,000 consumers,
2 excluding personal data controlled or processed solely for the purpose of completing a
3 payment transaction; or

4 B. Controlled or processed the personal data of not less than 25,000 consumers and
5 derived more than 25% of gross revenue from the sale of personal data.

6 **2. Applicability; beginning January 1, 2028.** Beginning January 1, 2028, the
7 provisions of this chapter apply to persons that conduct business in this State or persons
8 that produce products or services that are targeted to residents of this State and that during
9 the preceding calendar year:

10 A. Controlled or processed the personal data of not less than 50,000 consumers,
11 excluding personal data controlled or processed solely for the purpose of completing a
12 payment transaction; or

13 B. Controlled or processed the personal data of not less than 25,000 consumers and
14 derived more than 25% of gross revenue from the sale of personal data.

15 **3. Exempt entities.** The provisions of this chapter do not apply to:

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

18 B. A national securities association that is registered under the federal Securities
19 Exchange Act of 1934, 15 United States Code, Section 78a et seq.;

20 C. A financial institution or affiliate of a financial institution, including a service
21 corporation, that is subject to the federal Gramm-Leach-Bliley Act, 15 United States
22 Code, Section 6801 et seq. (1999) only if that institution or affiliate is directly and
23 solely engaged in financial activities as described in 12 United States Code, Section
24 1843(k) (2023). For purposes of this paragraph, "service corporation" has the same
25 meaning as in Title 9-B, section 131, subsection 37; or

26 D. A person or entity that qualifies as a licensee under Title 24-A, section 2263,
27 subsection 8, to the extent the person or entity is in compliance with any applicable
28 data security and data privacy requirements of Title 24-A.

29 **4. Exempt data.** The provisions of this chapter do not apply to:

30 A. Nonpublic personal information regulated under and collected, processed, sold or
31 disclosed in accordance with the requirements of the federal Gramm-Leach-Bliley Act,
32 15 United States Code, Section 6801 et seq. (1999);

33 B. Protected health information under the federal Health Insurance Portability and
34 Accountability Act of 1996, 42 United States Code, Chapter 7, Subchapter XI, Part C,
35 and the regulations, rules, guidance and exemptions adopted pursuant to that Act;

36 C. Patient-identifying information as described in 42 United States Code, Section
37 290dd-2;

38 D. Identifiable private information for the protection of human subjects in research
39 under 45 Code of Federal Regulations, Part 46;

40 E. Identifiable private information that is otherwise information collected as part of
41 human subjects in research pursuant to the good clinical practice guidelines issued by

1 the International Council for Harmonisation of Technical Requirements for
2 Pharmaceuticals for Human Use or successor organization;

3 F. The protection of human subjects in research under 21 Code of Federal Regulations,
4 Parts 50 and 56, or personal data used or shared in research, as defined in 45 Code of
5 Federal Regulations, Section 164.501, that is conducted in accordance with the
6 standards set forth in paragraphs D and E, or other research conducted in accordance
7 with applicable law;

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

10 H. Information derived from health care-related information listed in this subsection
11 that is de-identified in accordance with the requirements for de-identification pursuant
12 to the federal Health Insurance Portability and Accountability Act of 1996, 42 United
13 States Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and
14 exemptions adopted pursuant to that Act;

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

21 J. Information used for public health activities and purposes as authorized by the
22 federal Health Insurance Portability and Accountability Act of 1996, 42 United States
23 Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and
24 exemptions adopted pursuant to that Act;

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

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

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

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

38 O. Data processed or maintained:

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

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

(3) That is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under paragraph A and used for the purposes of administering those benefits; or

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

5. Compliance with federal Children's Online Privacy Protection Act of 1998.
Controllers and processors that comply with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act of 1998, 15 United States Code, Section 6501 et seq., as amended, and the regulations, rules, guidance and exemptions adopted pursuant to that Act are deemed to be compliant with an obligation to obtain parental consent pursuant to this chapter.

§9604. Consumer rights

1. Consumer rights. A consumer has a right to:

A. Confirm whether or not a controller is processing the consumer's personal data and to access that personal data, unless confirmation or access would require the controller to reveal a trade secret;

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

C. Delete personal data provided by, or obtained about, the consumer;

D. Obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, when the processing is carried out by automated means, as long as the controller is not required to reveal a trade secret; and

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

(1) Targeted advertising;

(2) The sale of personal data; or

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

2. Exercise of consumer rights. A consumer may communicate and access the information necessary to exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 9605 to exercise the rights of the consumer to opt out of the processing of the consumer's personal data as specified in subsection 1, paragraph E. In the case of processing personal data of a consumer known to be a child, the parent or legal guardian may exercise consumer rights on the child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise rights on the consumer's behalf.

1 **3. Responding to exercise of consumer rights.** Except as otherwise provided in this
2 chapter, a controller shall comply with a request by a consumer to exercise the consumer's
3 rights authorized pursuant to this chapter as follows.

4 A. A controller shall respond to the consumer without undue delay, but not later than
5 the 45th day after receipt of the request. The controller may extend the response period
6 by 45 days when reasonably necessary considering the complexity and number of the
7 consumer's requests, as long as the controller informs the consumer of the extension
8 within the initial 45-day response period and of the reason for the extension.

9 B. If a controller declines to take action regarding the consumer's request, the
10 controller shall inform the consumer without undue delay, but not later than the 45th
11 day after receipt of the request, of the justification for declining to take action and
12 instructions for how to appeal the decision.

13 C. The controller shall provide information in response to a consumer's request, free
14 of charge, once during any 12-month period. If requests from a consumer are
15 manifestly unfounded, excessive or repetitive, the controller may charge the consumer
16 a reasonable fee to cover the administrative costs of complying with the request or
17 decline to act on the request. The controller bears the burden of demonstrating the
18 manifestly unfounded, excessive or repetitive nature of the request.

19 D. If a controller is unable to authenticate a request to exercise a right afforded under
20 subsection 1, using commercially reasonable efforts, the controller is not required to
21 comply with a request to initiate an action pursuant to this section and shall provide
22 notice to the consumer that the controller is unable to authenticate the request to
23 exercise the right until the consumer provides additional information reasonably
24 necessary to authenticate the consumer and the consumer's request to exercise the right.

25 E. A controller that has obtained personal data about a consumer from a source other
26 than the consumer is in compliance with a consumer's request to delete that data
27 pursuant to subsection 1, paragraph C by retaining a record of the deletion request and
28 the minimum data necessary for the purpose of ensuring that the consumer's personal
29 data remains deleted from the controller's records and not using the retained data for
30 any other purpose pursuant to the provisions of this chapter.

31 **4. Appeals.** A controller shall establish a process for a consumer to appeal the
32 controller's inaction on a request within a reasonable period of time after the consumer's
33 receipt of the decision. The appeal process must be conspicuously available and similar to
34 the process for submitting requests to initiate action pursuant to this section. Not later than
35 the 60th day after receipt of an appeal, a controller shall inform the consumer in writing of
36 action taken or not taken in response to the appeal, including a written explanation of the
37 reasons for the decisions. If the appeal is denied, the controller shall also provide the
38 consumer with an online mechanism, if available, or other method through which the
39 consumer may contact the Attorney General to submit a complaint.

40 **§9605. Authorized agent**

41 A consumer may designate another person to serve as the consumer's authorized agent,
42 and act on the consumer's behalf, to opt out of the processing of the consumer's personal
43 data for the purposes specified in section 9604, subsection 1, paragraph E. The consumer
44 may designate an authorized agent by way of, among other methods, technology, including,

1 but not limited to, an Internet link or a browser setting, browser extension or global device
2 setting, indicating the consumer's intent to opt out of such processing. A controller shall
3 comply with an opt-out request received from an authorized agent if the controller is able
4 to verify, using commercially reasonable efforts, the identity of the consumer and the
5 authorized agent's authority to act on the consumer's behalf.

6 **§9606. Actions of controllers**

7 **1. Data minimization.** A controller must comply with the requirements of this
8 subsection.

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

12 **B.** Except as otherwise provided in this chapter, a controller may not process personal
13 data for purposes that are neither reasonably necessary for, nor compatible with, the
14 disclosed purposes for which the data is processed, as disclosed to the consumer, unless
15 the controller obtains the consumer's consent. For purposes of this paragraph, a
16 controller's sale of sensitive data to one person or entity is neither necessary to nor
17 compatible with the controller's sale of sensitive data to a different person or entity.

18 **C.** A controller shall process the minimum amount of personal data that is reasonably
19 necessary, adequate or relevant for each purpose for which data is processed, as
20 disclosed to the consumer.

21 **D.** A controller shall maintain documentation sufficient to demonstrate compliance
22 with paragraphs A to C for as long as a processing activity continues and for a least 24
23 months after the controller ceases to engage in the processing activity.

24 **A controller is not required to provide a product or service that requires the personal data**
25 **of a consumer that the controller does not collect or maintain.**

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

27 **A.** Establish and implement a retention schedule that requires the deletion or de-
28 identification of personal data when the retention of that data is no longer reasonably
29 necessary and relevant to the purposes for which the data is processed, as disclosed to
30 the consumer, or as otherwise permitted by this chapter or required by law;

31 **B.** Establish, implement and maintain reasonable administrative, technical and physical
32 data security practices to protect the confidentiality, integrity and accessibility of
33 personal data appropriate to the volume and nature of the personal data;

34 **C.** In the case of the processing of sensitive data concerning a consumer known to be
35 a child, process the data in accordance with the federal Children's Online Privacy
36 Protection Act of 1998, 15 United States Code, Section 6501 et seq., and the
37 regulations, rules, guidance and exemptions adopted pursuant to that Act; and

38 **D.** Provide an effective mechanism for a consumer to revoke the consumer's consent
39 under this section that is at least as easy as the mechanism by which the consumer
40 provided the consumer's consent and, upon revocation of the consent, cease to process
41 the data as soon as practicable, but not later than 15 days after the receipt of the request.

42 **3. Prohibitions.** A controller may not:

1 A. Process sensitive data concerning a consumer unless the controller obtains the
2 consumer's consent prior to processing. Consent is not valid under this paragraph
3 unless the controller has disclosed:

4 (1) The controller's identity;

5 (2) The reason consent is required, described in plain language that is
6 understandable by a reasonable consumer;

7 (3) The specific processing purposes for which consent is sought;

8 (4) The categories of sensitive data the controller must process to effectuate the
9 processing purpose and the categories of personal data that will be processed with
10 the sensitive data to effectuate the processing purpose; and

11 (5) If applicable, the identity of all 3rd parties to whom the sensitive data may be
12 sold.

13 If a consumer has not interacted with a controller for a period of 24 months, the
14 controller may not continue to process the consumer's sensitive data unless the
15 controller obtains a new consent from the consumer in accordance with the
16 requirements of this paragraph;

17 B. Process personal data in violation of the laws of this State and federal laws that
18 prohibit unlawful discrimination against consumers;

19 C. When the controller, under the circumstances, has actual knowledge or willfully
20 disregards that the consumer is at least 13 years of age but has not attained 16 years of
21 age;

22 (1) Process the personal data of the consumer for purposes of targeted advertising;
23 or

24 (2) Sell the consumer's personal data without the consumer's consent; or

25 D. Retaliate against a consumer for exercising a consumer right in this chapter or for
26 not agreeing to the collection or processing of personal data for a separate product or
27 service, including by denying goods or services, charging different prices or rates for
28 goods or services or providing a different level of quality of goods or services to the
29 consumer.

30 **4. Loyalty and rewards programs.** A controller may offer a different price, rate,
31 level, quality or selection of goods or services to a consumer, including offering goods or
32 services for no fee, if the offering is in connection with a consumer's voluntary participation
33 in a bona fide loyalty, rewards, premium features, discounts or club card program.

34 **5. Privacy notice.** A controller shall provide consumers with an accessible, clear and
35 meaningful privacy notice in plain language that is understandable by a reasonable
36 consumer that includes:

37 A. The categories of personal data processed by the controller;

38 B. The purpose for processing personal data;

39 C. How consumers may exercise their consumer rights, including how a consumer
40 may appeal a controller's decision with regard to the consumer's request;

41 D. The categories of personal data that the controller shares with 3rd parties, if any;

1 E. The categories of 3rd parties, if any, with which the controller shares personal data;
2 and

3 F. An active e-mail address or other mechanism that the consumer may use to contact
4 the controller.

5 **6. Consumer rights request mechanism.** A controller shall establish, and shall
6 describe in a privacy notice, one or more secure and reliable means for consumers to submit
7 a request to exercise a consumer right pursuant to this chapter. The design of the secure
8 and reliable means must take into account the ways in which consumers normally interact
9 with the controller, the need for secure and reliable communication of requests and the
10 ability of the controller to verify the identity of the consumer making the request. A
11 controller may not require a consumer to create a new account in order to exercise a
12 consumer right, but may require a consumer to use an existing account.

13 **7. Notice of sale and targeted advertising; opt-out mechanism.** If a controller sells
14 personal data to a 3rd party or processes personal data for targeted advertising, the
15 controller shall clearly and conspicuously disclose such processing, as well as the manner
16 in which a consumer may exercise the right to opt out of such processing. The disclosure
17 required under this section must include:

18 A. A clear and conspicuous link titled "Do Not Sell My Personal Data" or bearing a
19 substantially similar title on the controller's publicly accessible website that directs the
20 consumer, or an agent of the consumer, to a publicly accessible website that enables
21 the consumer, or an agent of the consumer, to opt out of the sale of the consumer's
22 personal data; and

23 B. A clear and conspicuous link titled "Opt Me Out of Targeted Advertising" or bearing
24 a substantially similar title on the controller's publicly accessible website that directs
25 the consumer, or an agent of the consumer, to a publicly accessible website that enables
26 the consumer, or an agent of the consumer, to opt out of processing of the consumer's
27 personal data for targeted advertising.

28 In lieu of providing the 2 links described in paragraphs A and B, a controller may satisfy
29 the requirements of this subsection by providing a single conspicuous and clearly labeled
30 link on the controller's publicly accessible website that allows a consumer, or an agent of
31 the consumer, both to opt out of the sale of the consumer's personal data and to opt out of
32 the processing of the consumer's personal data for targeted advertising. If the controller
33 maintains a specific section or page of its publicly accessible website that allows a
34 consumer, or an agent of the consumer, to opt out of the sale of the consumer's data or the
35 processing of the consumer's data for targeted advertising and to select additional privacy
36 controls, the controller may satisfy the requirements of this subsection by providing a single
37 conspicuous and clearly labeled link on the controller's publicly accessible website titled
38 "Your Privacy Choices" or bearing a substantially similar title that directs the consumer, or
39 an agent of the consumer, to that specific section or page of its publicly accessible website.

40 **8. Universal opt-out mechanism.** No later than December 1, 2027, a controller shall
41 allow a consumer to opt out of any processing of the consumer's personal data for the
42 purposes of targeted advertising or any sale of personal data through an opt-out preference
43 signal sent, with the consumer's consent, by a platform, technology or mechanism to the
44 controller indicating the consumer's intent to opt out of any such processing or sale. The
45 platform, technology or mechanism:

- 1 A. Must be consumer-friendly and easy to use by the average consumer;
2 B. May not unfairly disadvantage another controller;
3 C. May not make use of a default setting but must require the consumer to make an
4 affirmative, freely given and unambiguous choice to opt out of any such processing or
5 sale of the consumer's personal data;
6 D. Must be as consistent as possible with another similar platform, technology or
7 mechanism required by federal or state law; and
8 E. Must enable the controller to reasonably determine whether the consumer is a
9 resident of this State and whether the consumer has made a legitimate request to opt
10 out of to the sale of the consumer's personal data or targeted advertising.
11 A controller that recognizes an opt-out preference signal that has been approved by the
12 laws of another state is in compliance with this subsection.
13 **§9607. Responsibilities of processors and controllers**
14 **1. Processor responsibilities.** A processor shall adhere to the instructions of a
15 controller and shall assist the controller in meeting the controller's obligations under this
16 chapter. Assistance provided under this section must include:
17 A. Taking into account the nature of processing and the information available to the
18 processor, by appropriate technical and organizational measures, so far as is reasonably
19 practicable, to fulfill the controller's obligation to respond to a consumer rights request;
20 B. Taking into account the nature of processing and the information available to the
21 processor, by assisting the controller in meeting the controller's obligations in relation
22 to the security of processing the personal data and in relation to the notification of a
23 breach of security, as required by chapter 210-B, of the system of the processor, in
24 order to meet the controller's obligations; and
25 C. Providing necessary information to enable the controller to conduct and document
26 data protection assessments.
27 **2. Contractual requirements.** A contract between a controller and a processor must
28 govern the processor's data processing procedures with respect to processing performed on
29 behalf of the controller. The contract must clearly set forth instructions for processing data,
30 the nature and purpose of processing, the type of data subject to processing, the duration of
31 processing and the rights and obligations of both parties. The contract must require that the
32 processor:
33 A. Ensure that each person processing personal data is subject to a duty of
34 confidentiality with respect to the data;
35 B. At the controller's direction, delete or return all personal data to the controller as
36 requested at the end of the provision of services, unless retention of the personal data
37 is required by law;
38 C. On the reasonable request of the controller, make available to the controller all
39 information in the processor's possession necessary to demonstrate the processor's
40 compliance with the obligations in this chapter;
41 D. Allow and cooperate with reasonable assessments by the controller or the
42 controller's designated assessor or arrange for a qualified and independent assessor to

1 conduct an assessment of the processor's policies and technical and organizational
2 measures in support of the obligations in this chapter, using an appropriate and
3 accepted control standard or framework and assessment procedure for the assessment.
4 The processor shall provide a report of the assessment to the controller upon request;
5 and

6 E. Engage a subcontractor pursuant to a written contract that requires the subcontractor
7 to meet the obligations of the processor with respect to the personal data.

8 **3. Processing relationship liability.** This section may not be construed to relieve a
9 controller or processor from the liabilities imposed on the controller or processor by virtue
10 of the controller's or processor's role in the processing relationship as described in this
11 chapter.

12 **4. Fact-based determination.** Determining whether a person is acting as a controller
13 or processor with respect to a specific processing of data is a fact-based determination that
14 depends upon the context in which personal data is to be processed. A person who is not
15 limited in the person's processing of personal data pursuant to a controller's instructions, or
16 who fails to adhere to the instructions, is a controller and not a processor with respect to a
17 specific processing of data. A processor that continues to adhere to a controller's
18 instructions with respect to a specific processing of personal data remains a processor. If a
19 processor begins, alone or jointly with other persons, determining the purposes and means
20 of the processing of personal data, the processor acts as a controller with respect to the
21 processing and may be subject to an enforcement action under section 9612.

22 **§9608. Data protection assessments**

23 **1. Documentation.** A controller shall conduct and document a data protection
24 assessment for each of the controller's processing activities that presents a heightened risk
25 of harm to a consumer. For the purposes of this section, "processing that presents a
26 heightened risk of harm to a consumer" includes:

27 A. The processing of personal data for the purposes of targeted advertising;

28 B. The sale of personal data;

29 C. The processing of personal data for the purposes of profiling, when profiling
30 presents a reasonably foreseeable risk of:

31 (1) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

32 (2) Financial, physical or reputational injury to consumers;

33 (3) A physical or other intrusion upon the solitude or seclusion, or the private
34 affairs or concerns, of consumers, when the intrusion would be offensive to a
35 reasonable person; or

36 (4) Other substantial injury to consumers; and

37 D. The processing of sensitive data.

38 **2. Required elements.** Data protection assessments conducted pursuant to subsection
39 1 must identify and weigh the benefits that may flow, directly and indirectly, from the
40 processing to the controller, the consumer, other stakeholders and the public against the
41 potential risks to the rights of the consumer associated with the processing, as mitigated by
42 safeguards that can be employed by the controller to reduce the risks. The controller shall

1 factor into the data protection assessment the use of de-identified data and the reasonable
2 expectations of consumers, as well as the context of the processing and the relationship
3 between the controller and the consumer whose personal data will be processed.

4 **3. Attorney General disclosure; exemption from public records.** The Attorney
5 General may require that a controller disclose a data protection assessment that is relevant
6 to an investigation conducted by the Attorney General, and the controller shall make the
7 data protection assessment available to the Attorney General. The Attorney General may
8 evaluate the data protection assessment for compliance with the responsibilities set forth in
9 this chapter. A data protection assessment is confidential and exempt from disclosure under
10 Title 1, chapter 13. To the extent information contained in a data protection assessment
11 disclosed to the Attorney General includes information subject to attorney-client privilege
12 or work product protection, the disclosure does not constitute a waiver of that privilege or
13 protection.

14 **4. Processing activity.** A single data protection assessment may address a comparable
15 set of processing operations that include similar activities.

16 **5. Reciprocity.** If a controller conducts a data protection assessment for the purpose
17 of complying with another applicable law or regulation, the data protection assessment
18 satisfies the requirements established in this section if the data protection assessment is
19 reasonably similar in scope and effect to the data protection assessment that would
20 otherwise be conducted pursuant to this section.

21 **6. Application.** A controller is not required to conduct a data protection assessment
22 under this section for any processing activity created or initiated before July 1, 2026.

23 **§9609. De-identified and pseudonymous data**

24 **1. De-identified data requirements.** A controller in possession of de-identified data
25 shall:

26 **A. Take reasonable measures to ensure that the data cannot be associated with an**
27 **individual;**

28 **B. Publicly commit to maintaining and using de-identified data without attempting to**
29 **re-identify the data; and**

30 **C. Contractually obligate recipients of the de-identified data to comply with all**
31 **provisions of this chapter.**

32 **2. De-identified data and pseudonymous re-identification of data.** This chapter
33 may not be construed to require a controller or processor to:

34 **A. Re-identify de-identified data or pseudonymous data; or**

35 **B. Maintain data in identifiable form, or collect, obtain, retain or access data or**
36 **technology, in order to be capable of associating an authenticated consumer request**
37 **with personal data.**

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

40 **A. Is not reasonably capable of associating the request with the personal data, or it**
41 **would be unreasonably burdensome for the controller to associate the request with the**
42 **personal data;**

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

4 C. Does not sell the personal data to a 3rd party or otherwise voluntarily disclose the
5 personal data to a 3rd party other than a processor, except as otherwise permitted in
6 this section.

7 **4. Pseudonymous data requirements.** The rights afforded under section 9604,
8 subsection 1 do not apply to pseudonymous data in cases when the controller is able to
9 demonstrate that information necessary to identify the consumer is kept separately and is
10 subject to effective technical and organizational controls that prevent the controller from
11 accessing the information.

12 **5. Contractual oversight.** A controller that discloses pseudonymous data or de-
13 identified data shall exercise reasonable oversight to monitor compliance with contractual
14 commitments to which the pseudonymous data or de-identified data is subject and shall
15 take appropriate steps to address breaches of those contractual commitments.

16 **§9610. Geofence**

17 A person may not use a geofence to establish a virtual perimeter within 1,750 feet of
18 any facility that provides in-person health care services for the purpose of identifying,
19 tracking, collecting data from or sending any notification regarding the consumer's
20 consumer health data to a consumer that enters within that virtual perimeter. This
21 subsection does not prohibit the operator of a facility that provides in-person health care
22 services from implementing a geofence around the facility.

23 **§9611. Controller and processor; duties and obligations**

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

26 A. Comply with federal laws or regulations or the laws and rules of the State;

27 B. Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or
28 summons by federal or Maine governmental authorities or governmental authorities of
29 a federally recognized Indian tribe in this State;

30 C. Cooperate with federal, tribal or Maine law enforcement agencies concerning
31 conduct or activity that the controller or processor reasonably and in good faith believes
32 may violate federal laws or regulations or the laws and rules of the State;

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

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

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

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

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

1 I. Prevent, detect, protect against or respond to security incidents, identity theft, fraud,
2 harassment, malicious or deceptive activities or illegal activity or preserve the integrity
3 or security of systems or investigate, report or prosecute those responsible for an action
4 described in this paragraph;

5 J. Engage in public or peer-reviewed scientific or statistical research in the public
6 interest that adheres to all other applicable ethics and privacy laws and is approved,
7 monitored and governed by an institutional review board that determines, or similar
8 independent oversight entities that determine;

9 (1) Whether the deletion of the information is likely to provide substantial benefits
10 that do not exclusively accrue to the controller;

11 (2) Whether the expected benefits of the research outweigh the privacy risks; and

12 (3) Whether the controller has implemented reasonable safeguards to mitigate
13 privacy risks associated with research, including risks associated with re-
14 identification;

15 K. Assist another controller, processor or 3rd party with obligations under this chapter;
16 or

17 L. Process personal data for reasons of public interest in the area of public health, but
18 solely to the extent that the processing is:

19 (1) Subject to suitable and specific measures to safeguard the rights of the
20 consumer whose personal data is being processed; and

21 (2) Under the responsibility of a professional subject to confidentiality obligations
22 under federal or state laws or local ordinances.

23 **2. Internal use.** The obligations imposed on controllers or processors under this
24 chapter do not restrict a controller's or processor's ability to collect, use or retain data for
25 internal use to:

26 A. Conduct internal research to develop, improve or repair products, services or
27 technology;

28 B. Effectuate a product recall;

29 C. Identify and repair technical errors that impair existing or intended functionality;
30 or

31 D. Perform internal operations that are reasonably aligned with the expectations of the
32 consumer or reasonably anticipated based on the consumer's existing relationship with
33 the controller, or are otherwise compatible with processing data in furtherance of the
34 provision of a product or service specifically requested by a consumer or the
35 performance of a contract to which the consumer is a party.

36 **3. Evidentiary privilege.** The obligations imposed on controllers or processors under
37 this chapter do not apply when compliance with this chapter by the controller or processor
38 would violate an evidentiary privilege under the laws of this State. This chapter may not
39 be construed to prevent a controller or processor from providing personal data concerning
40 a consumer to a person covered by an evidentiary privilege under the laws of this State as
41 part of a privileged communication.

1 **4. Liability.** A controller or processor that discloses personal data to a 3rd-party
2 processor or 3rd-party controller in accordance with this chapter has not violated this
3 chapter if the 3rd-party processor or 3rd-party controller that receives and processes the
4 personal data violates this chapter, as long as, at the time the disclosing controller or
5 processor disclosed the personal data, the disclosing controller or processor did not have
6 actual knowledge that the receiving 3rd-party processor or 3rd-party controller would
7 violate this chapter. A 3rd-party controller or 3rd-party processor receiving personal data
8 from a controller or processor in compliance with this chapter is likewise not in violation
9 of this chapter for the transgressions of the controller or processor from which the 3rd-party
10 controller or 3rd-party processor receives the personal data.

11 **5. Exemptions.** This chapter may not be construed to:

12 A. Impose an obligation on a controller or processor that adversely affects the rights
13 or freedoms of a person, including, but not limited to, the rights of a person:

14 (1) To freedom of speech or freedom of the press guaranteed in the United States
15 Constitution, Amendment I; or

16 (2) Under Title 16, section 61; or

17 B. Apply to a person's processing of personal data in the course of the person's purely
18 personal or household activities.

19 **6. Limitations.** Personal data processed by a controller or processor pursuant to this
20 section may be processed only to the extent that the processing is:

21 A. Reasonably necessary and proportionate to the purposes listed in this section; and

22 B. Adequate, relevant and limited to what is necessary in relation to the specific
23 purposes listed in this section. Personal data collected, used or retained pursuant to
24 subsection 2 must, when applicable, take into account the nature and purpose of the
25 collection, use or retention. The data must be subject to reasonable administrative,
26 technical and physical measures to protect the confidentiality, integrity and
27 accessibility of the personal data and to reduce reasonably foreseeable risks of harm to
28 consumers relating to the collection, use or retention of personal data.

29 **7. Controller burden.** If a controller processes personal data pursuant to an
30 exemption in this section, the controller bears the burden of demonstrating that the
31 processing qualifies for the exemption and complies with the limitations in subsection 6.

32 **8. Clarification of roles.** Processing personal data for the purposes expressly
33 identified in this section does not solely make a legal entity a controller with respect to the
34 processing.

35 **§9612. Enforcement**

36 **1. Violation as unfair trade practice; exclusive Attorney General enforcement.** A
37 violation of this chapter constitutes an unfair trade practice under the Maine Unfair Trade
38 Practices Act, except that the provisions of Title 5, section 207, subsection 2 do not apply
39 to this chapter and except as provided in subsections 2 and 3. The Attorney General has the
40 exclusive authority to enforce violations of this chapter under the Maine Unfair Trade
41 Practices Act.

1 **2. Notice.** Notwithstanding any provision of Title 5, section 209 to the contrary, at
2 least 30 days prior to commencement of any action under the Maine Unfair Trade Practices
3 Act to enforce this chapter, the Attorney General shall notify the person against whom an
4 action may be brought of the intended action and give the person an opportunity to confer
5 with the Attorney General in person or by counsel or other representative as to the intended
6 action. Notice must be sent by mail, postage prepaid, to the person's usual place of business,
7 or if the person has no usual place of business, to the person's last known address. The
8 Attorney General may proceed without notice as required by this subsection upon a
9 showing of facts by affidavit of immediate irreparable harm to the consumers of the State.

10 **3. No private right of action.** Notwithstanding Title 5, section 213, this chapter may
11 not be construed as creating a private right of action against any person based on a violation
12 of any provision of this chapter.

13 **§9613. Maine Privacy Fund established**

14 **1. Establishment; purpose.** The Maine Privacy Fund, referred to in this section as the
15 "fund," is established within the Department of the Attorney General as a nonlapsing fund
16 to providing funding for the staff and activities of the department necessary to enforce the
17 provisions of this chapter.

18 **2. Administration.** The Department of the Attorney General shall administer the
19 fund. The fund must be established and held separate and apart from any other funds or
20 money of the State or the department and must be used and administered exclusively for
21 purposes authorized in this section. The fund consists of:

22 A. Any civil penalties, attorney's fees or costs awarded to the State in an action brought
23 by the Attorney General to enforce a violation of this chapter;

24 B. Sums that may be appropriated by the Legislature to the fund or transferred by the
25 Treasurer of State to the fund;

26 C. Interest earned on fund balances; and

27 D. Other funds received from any public or private source, including grants, gifts,
28 bequests and donations.

29 **Sec. 2. 35-A MRSA c. 94,** as amended, is repealed.

30 **Sec. 3. Report.** By January 1, 2028, the Attorney General shall submit a report to the
31 joint standing committee of the Legislature having jurisdiction over judiciary matters
32 regarding the operation and implementation of the Maine Revised Statutes, Title 10,
33 chapter 1057. The report must include, at a minimum, the following information:

34 1. The number of notices the Attorney General has issued under Title 10, section 9612,
35 subsection 2 and the nature of the violations alleged in the notices;

36 2. The number of persons sent a notice described in subsection 1 that conferred with
37 the Attorney General during the notice period described in Title 10, section 9612,
38 subsection 2 in a manner that alleviated the need for a civil action under the Maine Unfair
39 Trade Practices Act;

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

1 4. Any recommendations the Attorney General has for improving the operation of Title
2 10, chapter 1057.

3 The joint standing committee of the Legislature having jurisdiction over judiciary
4 matters may report out legislation related to the report to the Second Regular Session of the
5 133rd Legislature.

6 **Sec. 4. Effective date.** This Act takes effect July 1, 2026.

7 SUMMARY

8 This bill enacts the Maine Consumer Data Privacy Act, which takes effect July 1, 2026.
9 The Act regulates the collection, use, processing, disclosure, sale and deletion of
10 nonpublicly available personal data that is linked or reasonably linkable to an individual
11 who is a resident of the State, referred to in the Act as a "consumer," by a person that
12 conducts business in this State or that produces products or services targeted to residents
13 of this State, referred to in the Act as a "controller." Under the Act, a controller must limit
14 the collection of personal data to what is adequate, relevant and reasonably necessary in
15 relation to the purposes for which the controller processes that data, as disclosed in a
16 privacy notice specifying the categories of personal data processed by the controller, the
17 purposes for processing the personal data, the categories of personal data transferred to 3rd
18 parties and the categories of 3rd parties to whom personal data is shared. The Act also
19 requires a controller to process the minimum amount of personal data reasonably necessary,
20 adequate or relevant for each disclosed processing purpose.

21 A consumer has the right, under the Act, to confirm whether a controller is processing
22 the consumer's personal data; to require the controller to correct inaccuracies in or delete
23 the consumer's personal data; to obtain a copy of the consumer's personal data; and to opt
24 out of the processing of the consumer's personal data for purposes of targeted advertising,
25 sale or profiling in furtherance of decisions about the consumer's access to financial or
26 lending services, housing, insurance, education, criminal justice, employment
27 opportunities, health care services and essential goods and services. The privacy notice
28 must describe how a consumer may exercise these rights. The controller must obtain the
29 affirmative, informed consent of a consumer before processing the consumer's sensitive
30 data, including data revealing the consumer's race or ethnic origins, religious beliefs,
31 mental or physical health conditions or diagnoses, sexual orientation or citizenship or
32 immigration status; genetic or biometric data; precise geolocation data; complete social
33 security, driver's license or nondriver identification card number; specific financial or
34 account access information; data of a known child who has not attained 13 years of age; or
35 data concerning the consumer's status as the victim of a crime. If the controller knows that
36 the consumer has not attained 13 years of age, the controller may not process the consumer's
37 data for any purpose without parental consent. If the controller knows or willfully
38 disregards that the consumer is at least 13 years of age but has not attained 16 years of age,
39 the controller may not process the consumer's data for targeted advertising and must obtain
40 the consumer's consent before processing the consumer's data for sale.

41 The Act prohibits a controller from processing data in a manner that discriminates
42 against a person in violation of state or federal law. A controller is also prohibited from
43 retaliating against a consumer for exercising the consumer's rights under the Act, except
44 that a controller may offer different prices or selection of goods in connection with a

1 consumer's voluntary participation in a bona fide loyalty or discount program. A controller
2 must establish, implement and maintain reasonable data security practices and a retention
3 schedule that requires the deletion or de-identification of personal data when retention of
4 the data is no longer reasonably necessary and relevant to the purposes for which data is
5 processed or when deletion of the data is required by law. Beginning July 1, 2026, if a
6 controller engages in a data processing activity that presents a heightened risk of harm to a
7 consumer, including processing any data for targeted advertising, sale or profiling or any
8 processing of sensitive data, the controller must conduct and document a data protection
9 assessment to identify and weigh the benefits and potential risks of the processing activity.
10 The controller may be required to disclose the data protection assessment to the Attorney
11 General, who must keep it confidential, when the assessment is relevant to an investigation
12 conducted by the Attorney General. The Act further prohibits any person from establishing
13 a geofence within 1,750 feet of any in-person health care facility in the State, other than
14 the operator of the facility, for the purpose of identifying, tracking, collecting data from or
15 sending a notification regarding consumer health data to consumers who enter that area.

16 The provisions of the Act do not apply to specifically enumerated persons, including
17 the State, political subdivisions of the State and federally recognized Indian tribes in the
18 State; financial institutions or their affiliates subject to the federal Gramm-Leach-Bliley
19 Act that are directly and solely engaged in financial activities; state-licensed and authorized
20 insurers that are in compliance with applicable Maine laws governing insurer data security
21 and data privacy; and persons that both processed the personal data of fewer than 25,000
22 consumers in the preceding calendar year and derived no more than 25% of gross revenue
23 from the sale of personal data. The Act also does not apply to persons that controlled or
24 processed the personal data for purposes other than completing payment transactions of
25 fewer than 100,000 consumers in the preceding calendar year, except that, beginning
26 January 1, 2028, this exception applies only to persons that controlled or processed the
27 personal data for purposes other than completing payment transactions of fewer than
28 50,000 consumers in the preceding calendar year.

29 In addition, the provisions of the Act do not apply to specifically enumerated types of
30 data, including: nonpublic personal information regulated under the federal Gramm-Leach-
31 Bliley Act; protected health information under the federal Health Insurance Portability and
32 Accountability Act of 1996; personal data regulated by the Family Educational Rights and
33 Privacy Act of 1974; data processed and maintained by the controller regarding an
34 applicant for employment or employee to the extent the data is collected and used within
35 the context of that role; and data necessary for the controller to administer benefits. The
36 Maine Consumer Data Privacy Act also does not prohibit controllers from engaging in
37 specifically enumerated activities, including complying with Maine or federal law;
38 complying with investigations or subpoenas from governmental authorities including the
39 Federal Government and the government of the State or a federally recognized Indian tribe
40 in the State; cooperating with federal, Maine or tribal law enforcement agencies; providing
41 a product or service specifically requested by the consumer; protecting life and physical
42 safety of consumers and preventing or responding to security incidents; and conducting
43 internal product research, effectuating a product recall or performing other internal
44 operations aligned with the expectations of a consumer.

45 Violations of the Act may be enforced exclusively by the Attorney General under the
46 Maine Unfair Trade Practices Act. Absent a showing of immediate irreparable harm, the

1 Attorney General is required to provide a potential defendant with at least 30 days' notice
2 prior to initiating an enforcement action, during which time the potential defendant may
3 confer with the Attorney General to avoid the action. Any civil penalties, attorney's fees
4 or costs awarded to the State for a violation of the Act must be deposited in the Maine
5 Privacy Fund, which is established to provide funding for the enforcement staff and
6 activities of the Department of the Attorney General. The Act further requires the Attorney
7 General to submit a report by January 1, 2028 to the joint standing committee of the
8 Legislature having jurisdiction over judiciary matters regarding the operation and
9 implementation of the Act. The committee may report out legislation related to the report
10 to the Second Regular Session of the 133rd Legislature.

11 The bill also repeals the current law governing the privacy of broadband Internet access
12 service customer personal information because broadband Internet access service providers
13 are subject to the provisions of the Act.

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 Kott	FALMOUTH LD 1822	x		
Michael Kebede	MAINE ACLU	1822	1224	
Sen. Tracy Stewart	ARROSTOCK LD 1284	x		
Blenda O'Neil Esq	Attorney General's Office	1822	1224	
Jean Guin 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	BLANN : / SAISON	1224	1822	
Bruce Generosity	Automobile dealers			
Nate Goutier	Hospitality Maine	1224	1822	

P. 1 of 2

JOINT STANDING COMMITTEE ON JUDICIARY

TESTIMONY SHEET

LD or CONFIRMATION: DATA Privacy LDs 1084, 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 1224	
Michael Santorelli	ALCP - NY Law School			
Lisa Lavasseur	Internet Society LAB			
Lisa Marquies	VP Planned Parenthood	1822		
Matt Schwartz	Consumer Reports			
Anielle Garcia	"Check My Ads" Institute			
Zachary Taylor	Consumer Data Industry			
Toby Landreau	Findhelp			
Kenley Joseph	Multicultural Media			
Eric Null	Center for Democracy	1822		
Andrew Kingian	State Privacy & Security			
Christopher Gilrein	Technet			
Brian Langley	Elsworth SMALL BUSINESS OWNER	1224		
Robbie McLuckie	Consumer Healthcare Products			

P. 2 of 2



HOUSE OF REPRESENTATIVES

2 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0002
(207) 287-1440
TTY: (207) 287-4469

Rachel Henderson

5 Bernadine Street
Rumford, ME 04276
Phone: (207) 381-4237
Rachel.Henderson@legislature.maine.gov

LD1088 - An Act to Enact the Maine Consumer Data privacy Act

*Testimony of Rep. Henderson - Rumford
May 5th, 2025*

Senator Carney, Representative Kuhn, and distinguished members of the Joint Standing Committee on Judiciary. I am Rachel Henderson, and I have the distinct honor of representing the people of District-78 in the Maine House, which is comprised of the beautiful towns of Bethel, Byron, Hanover, Milton TWP, Roxbury, and my home town of Rumford.

I stand before you today to introduce my bill:
LD1088 An Act to Enact the Maine Consumer Data Privacy Act

History:

For the last few years the Maine Legislature has spent considerable time hearing, working, and trying to craft a Comprehensive Data Privacy Law.

This bill, and other privacy legislation being considered by the Judiciary Committee this session, cover complex issues and need to be worked out thoroughly with the business community and privacy experts.

In the 131st the Joint Standing Committee on the Judiciary we did just that. We heard a series of bills related to privacy, while none of those bills were enacted into law, there are a few things that became evident:

1. No Privacy Law. There is no comprehensive State Law that directs businesses on how to handle our private information. Many states have already adopted comprehensive privacy legislation and many more are moving to enact similar legislation this session. It is time for Maine to do the same.

House District 78 Bethel, Byron, Hanover, Milton Township, Roxbury, and Rumford



HOUSE OF REPRESENTATIVES

2 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0002
(207) 287-1440
TTY: (207) 287-4469

Rachel Henderson

5 Bernadine Street
Rumford, ME 04276
Phone: (207) 381-4237
Rachel.Henderson@legislature.maine.gov

Maine does have the Internet Service Provider law (ISP). The ISP-only act applies only to a narrow subset of companies and information.

2. Consistency. The Privacy Law that is enacted **MUST** be the same standard for all businesses, not one set of restrictions for Internet Service Providers, then an entirely separate set of guidelines for every other business.

3 Uniformity. The law Maine enacts must be similar in nature to those of other states, particularly to our neighboring New England states. Maine businesses need to remain competitive, especially in cities near the New Hampshire border, and consistent regulations across the region will help ensure they can do so effectively.

- **Facilitates Business Operations:** When laws are similar across states, businesses can develop unified compliance strategies rather than tailoring their data practices to each state's unique requirements. This reduces complexity and costs associated with legal compliance, making it easier for companies to operate across state lines.
 - **Reduces Legal Uncertainty:** Divergent laws can create confusion for businesses about what is required to stay compliant. Similar laws provide clarity, helping companies understand their obligations and reducing the risk of inadvertent violations.
 - **Enhances Consumer Protection:** Consistent standards across *neighboring* states ensure that consumers receive similar protections regardless of where they are within that region. This promotes competitive fairness and builds consumer trust in data handling practices.
 - **Encourages Data Privacy Innovation:** Uniform laws can foster a more predictable regulatory environment that encourages innovation in privacy and data security technologies, as companies know what standards they need to meet across multiple jurisdictions.
 - **Prevents Regulatory Arbitrage:** Businesses might otherwise choose to operate in states with less stringent laws to avoid stricter regulations elsewhere. Similar
- House District 78 Bethel, Byron, Hanover, Milton Township, Roxbury, and Rumford



HOUSE OF REPRESENTATIVES

2 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0002
(207) 287-1440
TTY: (207) 287-4469

Rachel Henderson

5 Bernadine Street
Rumford, ME 04276
Phone: (207) 381-4237
Rachel.Henderson@legislature.maine.gov

laws help prevent this "race to the bottom," ensuring a baseline level of privacy protection.

- **Supports Cross-Border Data Flows:** Many digital services and data exchanges occur across state lines. Similar laws make it easier to manage data transfers and uphold privacy rights without navigating a patchwork of conflicting regulations.

Meaning businesses that operate in multiple states need to share information and data between their offices or systems in different places. When the rules about privacy and data sharing are similar everywhere, it makes it much easier for these companies to do their work without running into legal problems or having to follow a bunch of different, complicated rules. This helps them serve customers better and run their business more efficiently across the U.S..

What LD1088 Does:

The Maine Consumer Data Privacy Act is a new law that will begin on July 1, 2026, aimed at protecting the personal information of residents in Maine.

Rules are set for businesses that collect, use, share, or sell personal data linked to Maine residents, requiring them to be transparent about what data they collect and why.

Businesses must limit the amount of personal information they gather to only what is necessary for their stated purposes and must obtain clear permission before processing sensitive data like health, biometric, or location information, especially for children and teenagers.

Businesses will need to implement security measures to protect personal data and delete it when no longer needed or required by law. For activities that pose higher risks to consumers, companies will have to assess and document how they protect data, with these assessments potentially reviewed by the state's attorney general



HOUSE OF REPRESENTATIVES

2 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0002
(207) 287-1440
TTY: (207) 287-4469

Rachel Henderson

5 Bernadine Street
Rumford, ME 04276
Phone: (207) 381-4237
Rachel.Henderson@legislature.maine.gov

Consumers will have rights under this law to see what data companies hold about them, correct inaccuracies, delete their data, and choose not to have their data used for targeted advertising or sold to third parties.

Discrimination Is Prohibited in LD1088, based on personal data and retaliation against consumers who exercise their rights.

Exempt from some provisions are certain entities, like the government, financial institutions, and health care providers, for example.

Use of geofences around healthcare facilities to track health data, is banned in LD1088.

The Attorney General can prosecute violations of the law, and must give businesses notice and time to fix issues before taking enforcement action.

Repeals previous ISP Law, since they will now be covered under LD1088.

Overall, the law aims to give Maine residents more control over their personal information and ensure businesses handle data responsibly.

This bill is important to all our constituents, seeking to establish important information, and privacy rights that have been taken out of our hands through the companies who profit off our data. Currently, Maine citizens have no choice. This bill seeks to give Maine people control over their information and create a more transparent relationship between businesses and their customers. The bill is based on the Connecticut framework for comprehensive privacy legislation.

This bill is past due. We can find a way that protects privacy and allows businesses to interact with consumers online in a mutually beneficial way. Mainers

House District 78 Bethel, Byron, Hanover, Milton Township, Roxbury, and Rumford



HOUSE OF REPRESENTATIVES

2 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0002
(207) 287-1440
TTY: (207) 287-4469

Rachel Henderson

5 Bernadine Street
Rumford, ME 04276
Phone: (207) 381-4237
Rachel.Henderson@legislature.maine.gov

are worried about how their personal data is being used and sold. We need to alleviate their concerns.

Thank you for your consideration.

Rep. Rachel Henderson

**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-placer-ai/>.

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

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.

MAINE COMMUNITY COLLEGE SYSTEM
UNIVERSITY OF MAINE SYSTEM

MEMORANDUM TO
JOINT STANDING COMMITTEE ON JUDICIARY

TO: The Honorable Anne Carney, Senate Chair; The Honorable Amy Kuhn, House Chair
Joint Standing Committee on Judiciary

FROM: William Fletcher, General Counsel, Maine Community College System on behalf of
the Maine Community College System and the University of Maine System

RE: L.D. 1224, *An Act to Comprehensively Protect Consumer Privacy*
L.D. 1088, *An Act to Enact the Maine Consumer Privacy Act*

DATE: May 5, 2025

Senator Carney, Representative Kuhn, and Members of the Joint Standing Committee on Judiciary, please accept this memorandum on behalf of the Maine Community College System ("MCCS") and the University of Maine System ("UMS") regarding L.D. 1224, *An Act to Comprehensively Protect Consumer Privacy* and L.D. 1088, *An Act to Enact the Maine Consumer Privacy Act*.

As public postsecondary education institutions, we appreciate the intent of this bill and recognize the importance of data privacy. MCCS and UMS already maintain data privacy and safeguarding of personal data, consistent with a robust set of existing federal laws and regulations, and we are committed to doing all that we can to protect the privacy of the data of the students we serve, our faculty, and staff. However, we believe adding another regulatory framework over the existing layers of federal law and regulation will complicate and undermine our ability to serve our students.

Therefore, we respectfully request that this Committee expressly exempt Maine's public postsecondary institutions from the applicability of LD 1224 and LD 1088, just as many other states with data privacy laws have provided exemptions to their institutions of higher education, and as provided for in LD 1822.

Thank you for your consideration. Should you have any questions, please contact Becky Smith, Director of Government and Community Relations for the Maine Community College System at bsmith@maineccc.edu or (207) 629-4015.

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.