03/16/2023   0935s

2023 SESSION

23-0857
06/04

SENATE BILL   *255-FN*

AN ACT   relative to the expectation of privacy.

SPONSORS: Sen. Carson, Dist 14; Sen. Innis, Dist 7; Sen. Soucy, Dist 18; Sen. Rosenwald, Dist
                 13; Sen. Chandley, Dist 11; Sen. Ricciardi, Dist 9; Rep. Edwards, Rock. 31; Rep.
                 Filiault, Ches. 7; Rep. McGough, Hills. 12; Rep. Luneau, Merr. 9

COMMITTEE: Judiciary

ANALYSIS

This bill creates a new chapter detailing a consumer expectation of privacy.

- -

Explanation: Matter added to current law appears in **bold italics.**
                 Matter removed from current law appears [in brackets and struckthrough.]
                 Matter which is either (a) all new or (b) repealed and reenacted appears in regular type.

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Twenty Three

AN ACT   relative to the expectation of privacy.

Be it Enacted by the Senate and House of Representatives in General Court convened:

1   1 New Chapter; Expectation of Privacy. Amend RSA by inserting after chapter 507-G the
2   following new chapter:
3   CHAPTER 507-H
4   EXPECTATION OF PRIVACY
5   507-H:1 Definitions. In this chapter:
6   I. "Affiliate" means a legal entity that shares common branding with another legal entity, or
7   is controlled by, or is under common control with, another legal entity.
8   II. "Control" or "Controlled" means ownership of, or the power to vote, more than 50 percent
9   of the outstanding shares of any class of voting security of a company; control in any manner over
10   the election of a majority of the directors or of individuals exercising similar functions; or, the power
11   to exercise controlling influence over the management of a company.
12   III. "Authenticate" means to use reasonable means to determine that a request to exercise
13   any of the rights afforded under section 507-H:4, I(a)-(d) of this chapter is being made by, or on
14   behalf of, the consumer who is entitled to exercise such consumer rights with respect to the personal
15   data at issue.
16   IV. "Biometric data" means data generated by automatic measurements of an individual's
17   biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique
18   biological patterns, or characteristics that are used to identify a specific individual. "Biometric data"
19   does not include a digital or physical photograph, an audio or video recording, or any data generated
20   from a digital or physical photograph, or an audio or video recording, unless such data is generated
21   to identify a specific individual.
22   V. "Business associate" has the same meaning as provided in the Health Insurance
23   Portability and Accountability Act (HIPAA).
24   VI. "Child" has the same meaning as provided in the Children's Online Privacy Protection
25   Act (COPPA).
26   VII. "Consent" means a clear affirmative act signifying a consumer's freely given, specific,
27   informed and unambiguous agreement to allow the processing of personal data relating to the
28   consumer. "Consent" may include a written statement, including by electronic means, or any other
29   unambiguous affirmative action. "Consent" does not include acceptance of a general or broad terms
30   of use or similar document that contains descriptions of personal data processing along with other,

1 unrelated information; hovering over, muting, pausing or closing a given piece of content; or, an

2 agreement obtained through the use of deceptive design patterns (also known as "dark patterns").

3 VIII. "Consumer" means an individual who is a resident of this state. "Consumer" does not

4 include an individual acting in a commercial or employment context or as an employee, owner,

5 director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government

6 agency whose communications or transactions with the controller occur solely within the context of

7 that individual's role with the company, partnership, sole proprietorship, nonprofit or government

8 agency.

9 IX. "Controller" means an individual who, or legal entity that, alone or jointly with others

10 determines the purpose and means of processing personal data.

11 X. "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501, et.

12 seq., and any amendments, regulations, rules, guidance and exemptions adopted under that act.

13 XI. "Covered entity" has the same meaning as provided in HIPAA.

14 XII. "Dark pattern" or "deceptive design pattern" means a user interface designed or

15 manipulated with the substantial effect of subverting or impairing user autonomy, decision-making

16 or choice, and includes, but is not limited to, any practice the Federal Trade Commission refers to as

17 a "dark pattern".

18 XIII. "Decisions that produce legal or similarly significant effects concerning the consumer"

19 means decisions made by the controller that result in the provision or denial by the controller of

20 financial or lending services, housing, insurance, education enrollment or opportunity, criminal

21 justice, employment opportunities, health care services or access to essential goods or services.

22 XIV. "De-identified data" means data that cannot reasonably be used to infer information

23 about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such

24 individual, if the controller that possesses such data takes reasonable measures to ensure that such

25 data cannot be associated with an individual; publicly commits to process such data only in a de-

26 identified way and not attempt to re-identify such data; and, contractually obligates any recipients of

27 such data to satisfy the criteria under this paragraph.

28 XV. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42

29 USC 1320d et. seq., as amended.

30 XVI. "Identified or identifiable individual" means an individual who can be readily

31 identified, directly or indirectly.

32 XVII. "Institution of higher education" means any individual who, or school, board,

33 association, limited liability company or corporation that, is licensed or accredited to offer one or

34 more programs of higher learning leading to one or more degrees.

35 XVIII. "Nonprofit organization" means any organization that is exempt from taxation under

36 Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any

37 subsequent corresponding internal revenue code of the United States, as amended.

1   XIX. "Personal data" means any information that is linked or reasonably linkable to an

2 identified or identifiable individual. "Personal data" does not include de-identified data or publicly

3 available information.

4   XX. "Precise geolocation data" means information derived from technology, including, but

5 not limited to, global positioning system level latitude and longitude coordinates or other

6 mechanisms, that directly identifies the specific location of an individual with precision and accuracy

7 within a radius of 1,750 feet. "Precise geolocation data" does not include the content of

8 communications or any data generated by or connected to advanced utility metering infrastructure

9 systems or equipment for use by a utility.

10   XXI. "Process" or "processing" means any operation or set of operations performed, whether

11 by manual or automated means, on personal data or on sets of personal data, such as the collection,

12 use, storage, disclosure, analysis, deletion or modification of personal data.

13   XXII. "Processor" means an individual who, or legal entity that, processes personal data on

14 behalf of a controller.

15   XXIII. "Profiling" means any form of automated processing performed on personal data to

16 evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's

17 economic situation, health, personal preferences, interests, reliability, behavior, location or

18 movements.

19   XXIV. "Protected health information" has the same meaning as provided in HIPAA.

20   XXV. "Pseudonymous data" means personal data that cannot be attributed to a specific

21 individual without the use of additional information, provided such additional information is kept

22 separately and is subject to appropriate technical and organizational measures to ensure that the

23 personal data is not attributed to an identified or identifiable individual.

24   XXVI. "Publicly available information" means information that is lawfully made available

25 through federal, state, municipal government records, or widely distributed media, and a controller

26 has a reasonable basis to believe a consumer has lawfully made available to the general public.

27   XXVII. "Sale of personal data" means the exchange of personal data for monetary or other

28 valuable consideration by the controller to a third party. "Sale of personal data" does not include:

29   (a) The disclosure of personal data to a processor that processes the personal data on

30 behalf of the controller;

31   (b) The disclosure of personal data to a third party for purposes of providing a product or

32 service requested by the consumer;

33   (c) The disclosure or transfer of personal data to an affiliate of the controller;

34   (d) The disclosure of personal data where the consumer directs the controller to disclose

35 the personal data or intentionally uses the controller to interact with a third party;

36   (e) The disclosure of personal data that the consumer intentionally made available to the

37 general public via a channel of mass media, and did not restrict to a specific audience; or,

1   (f) The disclosure or transfer of personal data to a third party as an asset that is part of

2   a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition,

3   bankruptcy or other transaction, in which the third party assumes control of all or part of the

4   controller's assets.

5   XXVIII. "Sensitive data" means personal data that includes data revealing racial or ethnic

6   origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation

7   or citizenship or immigration status; the processing of genetic or biometric data for the purpose of

8   uniquely identifying an individual; personal data collected from a known child; or, precise

9   geolocation data.

10   XXIX. "Targeted advertising" means displaying advertisements to a consumer where the

11   advertisement is selected based on personal data obtained or inferred from that consumer's activities

12   over time and across nonaffiliated Internet web sites or online applications to predict such

13   consumer's preferences or interests. "Targeted advertising" does not include:

14   (a) Advertisements based on activities within a controller's own Internet web sites or

15   online applications;

16   (b) Advertisements based on the context of a consumer's current search query, visit to an

17   Internet web site, or online application;

18   (c) Advertisements directed to a consumer in response to the consumer's request for

19   information or feedback; or,

20   (d) Processing personal data solely to measure or report advertising frequency,

21   performance, or reach.

22   XXX. "Third party" means an individual or legal entity, such as a public authority, agency or

23   body, other than the consumer, controller or processor or an affiliate of the processor or the

24   controller.

25   507-H:2 Application. This chapter applies to persons that conduct business in this state or

26   persons that produce products or services that are targeted to residents of this state that (a)

27   controlled or processed the personal data of not less than 100,000 consumers, excluding personal

28   data controlled or processed solely for the purpose of completing a payment transaction; or (b)

29   controlled or processed the personal data of not less than 25,000 consumers and derived more than

30   25 percent of their gross revenue from the sale of personal data.

31   507-H:3 Exclusions.

32   I. This chapter shall not apply to any:

33   (a) Body, authority, board, bureau, commission, district or agency of this state or of any

34   political subdivision of this state;

35   (b) Nonprofit organization;

36   (c) Institution of higher education;

1   (d) National securities association that is registered under 15 U.S.C. section 78o-3 of the

2 Securities Exchange Act of 1934, as amended;

3   (e) Financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15

4 U.S.C. 6801 et seq.; or,

5   (f) A covered entity or business associate, as defined in 45 C.F.R. 160.103.(b).

6   II. The following information and data shall be exempt from this chapter:

7   (a) Protected health information under HIPAA;

8   (b) Patient-identifying information for purposes of 42 U.S.C. section 290dd-2;

9   (c) Identifiable private information for purposes of the federal policy for the protection of

10 human subjects under 45 C.F.R. 46;

11   (d) Identifiable private information that is otherwise information collected as part of

12 human subjects research pursuant to the good clinical practice guidelines issued by the

13 International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human

14 Use;

15   (e) The protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal

16 data used or shared in research, as defined in 45 C.F.R. 164.501, that is conducted in accordance

17 with the standards set forth in this chapter, or other research conducted in accordance with

18 applicable law;

19   (f)   Information and documents created for purposes of the Health Care Quality

20 Improvement Act of 1986, 42 U.S.C. 11101 et seq.;

21   (g)   Patient safety work product for purposes of the Patient Safety and Quality

22 Improvement Act, 42 U.S.C. 299b-21 et seq., as amended;

23   (h) Information derived from any of the health care related information listed in this

24 subsection that is deidentified in accordance with the requirements for de-identification pursuant to

25 HIPAA;

26   (i)   Information originating from and intermingled to be indistinguishable with, or

27 information treated in the same manner as, information exempt under this section that is

28 maintained by a covered entity or business associate, program or qualified service organization, as

29 specified in 42 U.S.C. 290dd-2, as amended;

30   (j) Information used for public health activities and purposes as authorized by HIPAA,

31 community health activities and population health activities;

32   (k) The collection, maintenance, disclosure, sale, communication or use of any personal

33 information bearing on a consumer's credit worthiness, credit standing, credit capacity, character,

34 general reputation, personal characteristics or mode of living by a consumer reporting agency,

35 furnisher or user that provides information for use in a consumer report, and by a user of a

36 consumer report, but only to the extent that such activity is regulated by and authorized under the

37 Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.;

1   (l)   Personal data collected, processed, sold or disclosed in compliance with the Driver's

2   Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq., as amended;

3   (m)   Personal data regulated by the Family Educational Rights and Privacy Act, 20

4   U.S.C. 1232g et seq., as amended;

5   (n)   Personal data collected, processed, sold or disclosed in compliance with the Farm

6   Credit Act, 12 U.S.C. 2001 et seq., as amended;

7   (o)   Data processed or maintained in the course of an individual applying to, employed by

8   or acting as an agent or independent contractor of a controller, processor or third party, to the extent

9   that the data is collected and used within the context of that role; as the emergency contact

10   information of an individual under this chapter used for emergency contact purposes; or, that is

11   necessary to retain to administer benefits for another individual relating to the individual who is the

12   subject of the information under HIPPA and used for the purposes of administering such benefits;

13   and,

14   (p)   Personal data collected, processed, sold or disclosed in relation to price, route or

15   service, as such terms are used in the Airline Deregulation Act, 49 U.S.C. 40101 et seq., as amended,

16   by an air carrier subject to the act, to the extent this chapter is preempted by the Airline

17   Deregulation Act, 49 U.S.C. 41713, as amended.

18   III.   Controllers and processors that comply with the verifiable parental consent

19   requirements of COPPA shall be compliant with any obligation to obtain parental consent pursuant

20   to this chapter.

21   507-H:4 Consumer Expectation of Privacy.

22   I. A consumer shall have the right to:

23   (a)   Confirm whether or not a controller is processing the consumer's personal data and

24   access such personal data, unless such confirmation or access would require the controller to reveal a

25   trade secret;

26   (b)   Correct inaccuracies in the consumer's personal data, taking into account the nature

27   of the personal data and the purposes of the processing of the consumer's personal data;

28   (c)   Delete personal data provided by, or obtained about, the consumer;

29   (d)   Obtain a copy of the consumer's personal data processed by the controller, in a

30   portable and, to the extent technically feasible, readily usable format that allows the consumer to

31   transmit the data to another controller without hindrance, where the processing is carried out by

32   automated means, provided such controller shall not be required to reveal any trade secret; and

33   (e)   Opt-out of the processing of the personal data for purposes of targeted advertising,

34   the sale of personal data, except as provided in RSA 507-H:6, or profiling in furtherance of solely

35   automated decisions that produce legal or similarly significant effects concerning the consumer.

36   II.   A consumer may exercise rights under this section by a secure and reliable means

37   established by the controller and described to the consumer in the controller's privacy notice. A

1   consumer may designate an authorized agent in accordance with RSA 507-H:5 to exercise the rights

2   of such consumer to opt-out of the processing of such consumer's personal data for purposes of RSA

3   507-H:4, III(e) on behalf of the consumer. In the case of processing personal data of a known child,

4   the parent or legal guardian may exercise such consumer rights on the child's behalf. In the case of

5   processing personal data concerning a consumer subject to a guardianship, conservatorship, or other

6   protective arrangement, the guardian or the conservator of the consumer may exercise such rights

7   on the consumer's behalf.

8   III. Except as otherwise provided in this chapter, a controller shall comply with a request by

9   a consumer to exercise the consumer rights authorized pursuant to this chapter as follows:

10   (a) A controller shall respond to the consumer without undue delay, but not later than

11   45 days after receipt of the request. The controller may extend the response period by 45 additional

12   days when reasonably necessary, considering the complexity and number of the consumer's requests,

13   provided the controller informs the consumer of any such extension within the initial 45-day

14   response period and of the reason for the extension.

15   (b) If a controller declines to take action regarding the consumer's request, the controller

16   shall inform the consumer without undue delay, but not later than 45 days after receipt of the

17   request, of the justification for declining to take action and instructions for how to appeal the

18   decision.

19   (c) Information provided in response to a consumer request shall be provided by a

20   controller, free of charge, once per consumer during any twelve-month period. If requests from a

21   consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer

22   a reasonable fee to cover the administrative costs of complying with the request or decline to act on

23   the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive

24   or repetitive nature of the request.

25   (d) If a controller is unable to authenticate a request to exercise any of the rights

26   afforded under sections I (a)-(d) of this section using commercially reasonable efforts, the controller

27   shall not be required to comply with a request to initiate an action pursuant to this section and shall

28   provide notice to the consumer that the controller is unable to authenticate the request to exercise

29   such right or rights until such consumer provides additional information reasonably necessary to

30   authenticate such consumer and such consumer's request to exercise such right or rights. A

31   controller shall not be required to authenticate an opt-out request, but a controller may deny an opt-

32   out request if the controller has a good faith, reasonable and documented belief that such request is

33   fraudulent. If a controller denies an opt-out request because the controller believes such request is

34   fraudulent, the controller shall send a notice to the person who made such request disclosing that

35   such controller believes such request is fraudulent, why such controller believes such request is

36   fraudulent and that such controller shall not comply with such request.

1   (e) A controller that has obtained personal data about a consumer from a source other

2 than the consumer shall be deemed in compliance with a consumer's request to delete such data

3 pursuant to RSA 507-H:4, I(c) by retaining a record of the deletion request and the minimum data

4 necessary for the purpose of ensuring the consumer's personal data remains deleted from the

5 controller's records and not using such retained data for any other purpose pursuant to this chapter,

6 or opting the consumer out of the processing of such personal data for any purpose except for those

7 exempted pursuant this chapter.

8   IV. A controller shall establish a process for a consumer to appeal the controller's refusal to

9 take action on a request within a reasonable period of time after the consumer's receipt of the

10 decision.   The appeal process shall be conspicuously available and similar to the process for

11 submitting requests to initiate action pursuant to this section. Not later than 60 days after receipt

12 of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in

13 response to the appeal, including a written explanation of the reasons for the decisions. If the appeal

14 is denied, the controller shall also provide the consumer with an online mechanism, if available, or

15 other method through which the consumer may contact the attorney general to submit a complaint.

16   507-H:5 Consumer Agents. A consumer may designate another person to serve as the

17 consumer's authorized agent, and act on such consumer's behalf, to opt-out of the processing of such

18 consumer's personal data for one or more of the purposes specified in RSA 507-H:4, I(e). The

19 consumer may designate such authorized agent by way of, among other things, a technology,

20 including, but not limited to, an Internet link or a browser setting, browser extension or global

21 device setting, indicating such consumer's intent to opt-out of such processing. A controller shall

22 comply with an opt-out request received from an authorized agent if the controller is able to verify,

23 with commercially reasonable effort, the identity of the consumer and the authorized agent's

24 authority to act on such consumer's behalf.

25   507-H:6 Controller Responsibilities.

26   I. A controller shall:

27   (a) Limit the collection of personal data to what is adequate, relevant and reasonably

28 necessary in relation to the purposes for which such data is processed, as disclosed to the consumer;

29   (b) Except as otherwise provided in this chapter, not process personal data for purposes

30 that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such

31 personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's

32 consent;

33   (c)   Establish, implement and maintain reasonable administrative, technical and

34 physical data security practices to protect the confidentiality, integrity and accessibility of personal

35 data appropriate to the volume and nature of the personal data at issue;

1   (d) Not process sensitive data concerning a consumer without obtaining the consumer's

2 consent, or, in the case of the processing of sensitive data concerning a known child, without

3 processing such data in accordance with COPPA;

4   (e) Not process personal data in violation of the laws of this state and federal laws that

5 prohibit unlawful discrimination against consumers;

6   (f) Provide an effective mechanism for a consumer to revoke the consumer's consent

7 under this section that is at least as easy as the mechanism by which the consumer provided the

8 consumer's consent and, upon revocation of such consent, cease to process the data as soon as

9 practicable, but not later than fifteen days after the receipt of such request; and

10   (g) Not process the personal data of a consumer for purposes of targeted advertising, or

11 sell the consumer's personal data without the consumer's consent, under circumstances where a

12 controller has actual knowledge, and wilfully disregards, that the consumer is at least thirteen years

13 of age but younger than sixteen years of age. A controller shall not discriminate against a consumer

14 for exercising any of the consumer rights contained in this chapter, including denying goods or

15 services, charging different prices or rates for goods or services or providing a different level of

16 quality of goods or services to the consumer.

17   II. Nothing in this section shall be construed to require a controller to provide a product or

18 service that requires the personal data of a consumer which the controller does not collect or

19 maintain, or prohibit a controller from offering a different price, rate, level, quality or selection of

20 goods or services to a consumer, including offering goods or services for no fee, if the offering is in

21 connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium

22 features, discounts or club card program.

23   III. A controller shall provide consumers with a reasonably accessible, clear and meaningful

24 privacy notice that includes:

25   (a) The categories of personal data processed by the controller;

26   (b) The purpose for processing personal data;

27   (c) How consumers may exercise their consumer rights, including how a consumer may

28 appeal a controller's decision with regard to the consumer's request;

29   (d) The categories of personal data that the controller shares with third parties, if any;

30   (e) The categories of third parties, if any, with which the controller shares personal data;

31 and

32   (f) An active electronic mail address or other online mechanism that the consumer may

33 use to contact the controller.

34   IV. If a controller sells personal data to third parties or processes personal data for targeted

35 advertising, the controller shall clearly and conspicuously disclose such processing, as well as the

36 manner in which a consumer may exercise the right to opt-out of such processing.

1   V.(a) A controller shall establish, and shall describe in a privacy notice, one or more secure

2 and reliable means for consumers to submit a request to exercise their consumer rights pursuant to

3 this chapter. Such means shall take into account the ways in which consumers normally interact

4 with the controller, the need for secure and reliable communication of such requests and the ability

5 of the controller to verify the identity of the consumer making the request. A controller shall not

6 require a consumer to create a new account in order to exercise consumer rights, but may require a

7 consumer to use an existing account. Any such means shall include:

8   (1)(A) Providing a clear and conspicuous link on the controller's Internet web site to

9 an Internet web page that enables a consumer, or an agent of the consumer, to opt-out of the

10 targeted advertising or sale of the consumer's personal data; and

11   (B)   Not later than January 1, 2025, allowing a consumer to opt-out of any

12 processing of the consumer's personal data for the purposes of targeted advertising, or any sale of

13 such personal data, through an opt-out preference signal sent, with such consumer's consent, by a

14 platform, technology or mechanism to the controller indicating such consumer's intent to opt-out of

15 any such processing or sale. Such platform, technology or mechanism shall:

16   (i) Not unfairly disadvantage another controller;

17   (ii) Not make use of a default setting, but, rather, require the consumer to

18 make an affirmative, freely given and unambiguous choice to opt-out of any processing of such

19 consumer's personal data pursuant to this chapter;

20   (iii) Be consumer-friendly and easy to use by the average consumer;

21   (iv) Be as consistent as possible with any other similar platform, technology

22 or mechanism required by any federal or state law or regulation; and

23   (v) Enable the controller to accurately determine whether the consumer is a

24 resident of this state and whether the consumer has made a legitimate request to opt-out of any sale

25 of such consumer's personal data or targeted advertising.

26   (2) If a consumer's decision to opt-out of any processing of the consumer's personal

27 data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out

28 preference signal sent in accordance with RSA 507-H:6, V(a)(1)(A) conflicts with the consumer's

29 existing controller-specific privacy setting or voluntary participation in a controller's bona fide

30 loyalty, rewards, premium features, discounts or club card program, the controller shall comply with

31 such consumer's opt-out preference signal but may notify such consumer of such conflict and provide

32 to such consumer the choice to confirm such controller-specific privacy setting or participation in

33 such program.

34   (b) If a controller responds to consumer opt-out requests received pursuant to RSA 507-

35 H:6, V(a)(1) by informing the consumer of a charge for the use of any product or service, the

36 controller shall present the terms of any financial incentive offered pursuant to 507-H:6, II for the

37 retention, use, sale or sharing of the consumer's personal data.

1 507-H:7 Processor Responsibilities.

2 I. A processor shall adhere to the instructions of a controller and shall assist the controller

3 in meeting the controller's obligations under this chapter. Such assistance shall include:

4 (a) Taking into account the nature of processing and the information available to the

5 processor, by appropriate technical and organizational measures, insofar as is reasonably

6 practicable, to fulfill the controller's obligation to respond to consumer rights requests;

7 (b) Taking into account the nature of processing and the information available to the

8 processor, by assisting the controller in meeting the controller's obligations in relation to the security

9 of processing the personal data and in relation to the notification of a breach of security or of the

10 system of the processor, in order to meet the controller's obligations; and

11 (c) Providing necessary information to enable the controller to conduct and document

12 data protection assessments.

13 II. A contract between a controller and a processor shall govern the processor's data

14 processing procedures with respect to processing performed on behalf of the controller. The contract

15 shall be binding and clearly set forth instructions for processing data, the nature and purpose of

16 processing, the type of data subject to processing, the duration of processing and the rights and

17 obligations of both parties. The contract shall also require that the processor:

18 (a) Ensure that each person processing personal data is subject to a duty of

19 confidentiality with respect to the data;

20 (b) At the controller's direction, delete or return all personal data to the controller as

21 requested at the end of the provision of services, unless retention of the personal data is required by

22 law;

23 (c) Upon the reasonable request of the controller, make available to the controller all

24 information in its possession necessary to demonstrate the processor's compliance with the

25 obligations in this chapter;

26 (d) After providing the controller an opportunity to object, engage any subcontractor

27 pursuant to a written contract that requires the subcontractor to meet the obligations of the

28 processor with respect to the personal data; and

29 (e) Allow, and cooperate with, reasonable assessments by the controller or the

30 controller's designated assessor, or the processor may arrange for a qualified and independent

31 assessor to conduct an assessment of the processor's policies and technical and organizational

32 measures in support of the obligations under this chapter, using an appropriate and accepted control

33 standard or framework and assessment procedure for such assessments. The processor shall provide

34 a report of such assessment to the controller upon request.

35 III. Nothing in this section shall be construed to relieve a controller or processor from the

36 liabilities imposed on the controller or processor by virtue of such controller's or processor's role in

37 the processing relationship, as described in this chapter.

1   IV. Determining whether a person is acting as a controller or processor with respect to a

2   specific processing of data is a fact-based determination that depends upon the context in which

3   personal data is to be processed. A person who is not limited in such person's processing of personal

4   data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller

5   and not a processor with respect to a specific processing of data. A processor that continues to

6   adhere to a controller's instructions with respect to a specific processing of personal data remains a

7   processor. If a processor begins, alone or jointly with others, determining the purposes and means of

8   the processing of personal data, the processor is a controller with respect to such processing and may

9   be subject to an enforcement action under RSA 507-H:11.

10   507-H:8 Heightened Risk of Harm.

11   I. A controller shall conduct and document a data protection assessment for each of the

12   controller's processing activities that presents a heightened risk of harm to a consumer. For the

13   purposes of this section, processing that presents a heightened risk of harm to a consumer includes:

14   (a) The processing of personal data for the purposes of targeted advertising;

15   (b) The sale of personal data;

16   (c) The processing of personal data for the purposes of profiling, where such profiling

17   presents a reasonably foreseeable risk of unfair or deceptive treatment of, or unlawful disparate

18   impact on, consumers, financial, physical or reputational injury to consumers, a physical or other

19   intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such

20   intrusion would be offensive to a reasonable person, or other substantial injury to consumers; and

21   (d) The processing of sensitive data.

22   II. Data protection assessments conducted pursuant to RSA 507-H:8, I shall identify and

23   weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the

24   consumer, other stakeholders and the public against the potential risks to the rights of the consumer

25   associated with such processing, as mitigated by safeguards that can be employed by the controller

26   to reduce such risks. The controller shall factor into any such data protection assessment the use of

27   de-identified data and the reasonable expectations of consumers, as well as the context of the

28   processing and the relationship between the controller and the consumer whose personal data will be

29   processed.

30   III.   The attorney general may require that a controller disclose any data protection

31   assessment that is relevant to an investigation conducted by the attorney general, and the controller

32   shall make the data protection assessment available to the attorney general. The attorney general

33   may evaluate the data protection assessment for compliance with the responsibilities set forth in

34   this chapter. Data protection assessments shall be confidential and shall be exempt from disclosure

35   under RSA 91-A. To the extent any information contained in a data protection assessment disclosed

36   to the attorney general includes information subject to attorney-client privilege or work product

37   protection, such disclosure shall not constitute a waiver of such privilege or protection.

1   IV.   A single data protection assessment may address a comparable set of processing

2   operations that include similar activities.

3   V. If a controller conducts a data protection assessment for the purpose of complying with

4   another applicable law or regulation, the data protection assessment shall be deemed to satisfy the

5   requirements established in this section if such data protection assessment is reasonably similar in

6   scope and effect to the data protection assessment that would otherwise be conducted pursuant to

7   this section.

8   VI. Data protection assessment requirements shall apply to processing activities created or

9   generated after July 1, 2024, and are not retroactive.

10   507-H:9 De-Identifed Data.

11   I. Any controller in possession of de-identified data shall:

12   (a)   Take reasonable measures to ensure that the data cannot be associated with an

13   individual;

14   (b)   Publicly commit to maintaining and using de-identified data without attempting to

15   reidentify the data; and

16   (c)   Contractually obligate any recipients of the deidentified data to comply with all

17   provisions of this chapter.

18   II. Nothing in this chapter shall be construed to:

19   (a) Require a controller or processor to re-identify de-identified data or pseudonymous

20   data; or

21   (b)   Maintain data in identifiable form, or collect, obtain, retain or access any data or

22   technology, in order to be capable of associating an authenticated consumer request with personal

23   data.

24   III. Nothing in this chapter shall be construed to require a controller or processor to comply

25   with an authenticated consumer rights request if the controller:

26   (a) Is not reasonably capable of associating the request with the personal data or it

27   would be unreasonably burdensome for the controller to associate the request with the personal

28   data;

29   (b) Does not use the personal data to recognize or respond to the specific consumer who

30   is the subject of the personal data, or associate the personal data with other personal data about the

31   same specific consumer; and

32   (c) Does not sell the personal data to any third party or otherwise voluntarily disclose

33   the personal data to any third party other than a processor, except as otherwise permitted in this

34   section.

35   IV. The rights afforded under RSA 507-H:4, I(a)-(d) shall not apply to pseudonymized data

36   in cases where the controller is able to demonstrate that any information necessary to identify the

1 consumer is kept separately and is subject to effective technical and organizational controls that

2 prevent the controller from accessing such information.

3   V.   A controller that discloses pseudonymous data or de-identified data shall exercise

4 reasonable oversight to monitor compliance with any contractual commitments to which the

5 pseudonymous data or deidentified data is subject and shall take appropriate steps to address any

6 breaches of those contractual commitments.

7 507-H:10 Controller Responsibilities and Obligations.

8   I. Nothing in this chapter shall be construed to restrict a controller's or processor's ability to:

9   (a) Comply with federal, state or municipal ordinances or regulations;

10   (b)   Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or

11 summons by federal, state, municipal or other governmental authorities;

12   (c)   Cooperate with law enforcement agencies concerning conduct or activity that the

13 controller or processor reasonably and in good faith believes may violate federal, state or municipal

14 ordinances or regulations;

15   (d) Investigate, establish, exercise, prepare for or defend legal claims;

16   (e) Provide a product or service specifically requested by a consumer;

17   (f)   Perform under a contract to which a consumer is a party, including fulfilling the

18 terms of a written warranty;

19   (g) Take steps at the request of a consumer prior to entering into a contract;

20   (h) Take immediate steps to protect an interest that is essential for the life or physical

21 safety of the consumer or another individual, and where the processing cannot be manifestly based

22 on another legal basis;

23   (i) Prevent, detect, protect against or respond to security incidents, identity theft, fraud,

24 harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security

25 of systems or investigate, report or prosecute those responsible for any such action;

26   (j)   Engage in public or peer-reviewed scientific or statistical research in the public

27 interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and

28 governed by an institutional review board that determines, or similar independent oversight entities

29 that determine,

30   (1) Whether the deletion of the information is likely to provide substantial benefits

31 that do not exclusively accrue to the controller,

32   (2) The expected benefits of the research outweigh the privacy risks, and

33   (3)   Whether the controller has implemented reasonable safeguards to mitigate

34 privacy risks associated with research, including any risks associated with re-identification;

35   (k) Assist another controller, processor or third party with any of the obligations under

36 this chapter; or

1   (l) Process personal data for reasons of public interest in the area of public health,

2 community health or population health, but solely to the extent that such processing is

3   (1) Subject to suitable and specific measures to safeguard the rights of the consumer

4 whose personal data is being processed, and

5   (2) Under the responsibility of a professional subject to confidentiality obligations

6 under federal, state or local law.

7   II. The obligations imposed on controllers or processors under this chapter shall not restrict

8 a controller's or processor's ability to collect, use or retain data for internal use to:

9   (a) Conduct internal research to develop, improve or repair products, services or

10 technology;

11   (b) Effectuate a product recall;

12   (c) Identify and repair technical errors that impair existing or intended functionality; or

13   (d) Perform internal operations that are reasonably aligned with the expectations of the

14 consumer or reasonably anticipated based on the consumer's existing relationship with the

15 controller, or are otherwise compatible with processing data in furtherance of the provision of a

16 product or service specifically requested by a consumer or the performance of a contract to which the

17 consumer is a party.

18   III. The obligations imposed on controllers or processors under this chapter shall not apply

19 where compliance by the controller or processor with said sections would violate an evidentiary

20 privilege under the laws of this state. Nothing in this chapter shall be construed to prevent a

21 controller or processor from providing personal data concerning a consumer to a person covered by

22 an evidentiary privilege under the laws of the state as part of a privileged communication.

23   IV. A controller or processor that discloses personal data to a processor or third-party

24 controller in accordance with this chapter shall not be deemed to have violated said sections if the

25 processor or third-party controller that receives and processes such personal data violates said

26 sections, provided, at the time the disclosing controller or processor disclosed such personal data, the

27 disclosing controller or processor did not have actual knowledge that the receiving processor or third-

28 party controller would violate said sections. A third-party controller or processor receiving personal

29 data from a controller or processor in compliance with this chapter is likewise not in violation of said

30 sections for the transgressions of the controller or processor from which such third-party controller

31 or processor receives such personal data.

32   V. Nothing in this chapter shall be construed to:

33   (a) Impose any obligation on a controller or processor that adversely affects the rights or

34 freedoms of any person, including, but not limited to, the rights of any person to freedom of speech or

35 freedom of the press guaranteed in the First Amendment to the United States Constitution; or

36   (b) Apply to any person's processing of personal data in the course of such person's

37 purely personal or household activities.

1   VI. Personal data processed by a controller pursuant to this section may be processed to the

2 extent that such processing is:

3   (a) Reasonably necessary and proportionate to the purposes listed in this section; and

4   (b)   Adequate, relevant and limited to what is necessary in relation to the specific

5 purposes listed in this section. Personal data collected, used or retained under RSA 507-H:10, I(b),

6 where applicable, take into account the nature and purpose or purposes of such collection, use or

7 retention. Such data shall be subject to reasonable administrative, technical and physical measures

8 to protect the confidentiality, integrity and accessibility of the personal data and to reduce

9 reasonably foreseeable risks of harm to consumers relating to such collection, use or retention of

10 personal data.

11   VII. If a controller processes personal data pursuant to an exemption in this section, the

12 controller bears the burden of demonstrating that such processing qualifies for the exemption and

13 complies with the requirements in RSA 507-H:10, VI.

14   VIII. Processing personal data for the purposes expressly identified in this section shall not

15 solely make a legal entity a controller with respect to such processing.

16   507-H:11 Notice; Enforcement.

17   I.   The attorney general shall have exclusive authority to enforce violations under this

18 chapter.

19   II.   The attorney general shall, prior to initiating any action for a violation under this

20 chapter, issue a notice of violation to the controller if the attorney general determines that a cure is

21 possible. If the controller fails to cure such violation within 60 days of receipt of the notice of

22 violation, the attorney general may bring an action pursuant to this section.

23   III. In determining whether to grant a controller or processor the opportunity to cure an

24 alleged violation described under this chapter, the attorney general may consider:

25   (1) The number of violations;

26   (2) The size and complexity of the controller or processor;

27   (3) The nature and extent of the controller's or processor's processing activities;

28   (4) The substantial likelihood of injury to the public;

29   (5) The safety of persons or property; and

30   (6) Whether such alleged violation was likely caused by human or technical error.

31   IV. Nothing in this chapter shall be construed as providing the basis for, or be subject to, a

32 private right of action for violations under this chapter.

33   V. A violation under this chapter shall constitute an unfair method of competition or any

34 unfair or deceptive act or practice in the conduct of any trade or commerce within this state under

35 RSA 358-A:2 and shall be enforced by the attorney general.

36   2 Effective Date. This act shall take effect January 1, 2025.

SB 255-FN- FISCAL NOTE

AS AMENDED BY THE SENATE (AMENDMENT #2023-0935s)

AN ACT   relative to the expectation of privacy.

FISCAL IMPACT: [X] State   [   ] County   [   ] Local   [   ] None

STATE:	Estimated Increase / (Decrease)			
	FY 2023	**FY 2024**	**FY 2025**	**FY 2026**
Appropriation	$0	$0	$0	$0
Revenue	$0	$0	$0	$0
Expenditures	$0	$0	Indeterminable Increase	Indeterminable Increase
Funding Source:	[X] General	[ ] Education	[ ] Highway	[ ] Other

METHODOLOGY:

This bill creates a new chapter detailing a consumer expectation of privacy. The Department of Justice indicates a violation of this chapter shall be deemed a violation of New Hampshire Consumer Protection Act, RSA 358-A. The Attorney General has the exclusive authority to enforce violations of this chapter. Prior to any enforcement action, the Attorney General shall issue a notice of violation and a right to cure the violation within 60 days. The Department states the proposed statute would increase the number of investigations, prosecutions and litigation matters handled by the Department. However, because the degree of increase cannot be estimated, the fiscal impact is indeterminable. The Department assumes, due to the complexity of the review, it would likely require significant additional resources.

The Judicial Branch states the fiscal impact on the Branch is indeterminable as it is unable to make any assumptions as to the number of new cases would be filed as a result of the bill or the level of complexity of such litigation.

AGENCIES CONTACTED:

Department of Justice and Judicial Branch