L.D. 946

Date: (Filing No. S-)

ENERGY, UTILITIES AND TECHNOLOGY

Reproduced and distributed under the direction of the Secretary of the Senate.

STATE OF MAINE

SENATE

129TH LEGISLATURE

FIRST REGULAR SESSION

COMMITTEE AMENDMENT " " to S.P. 275, L.D. 946, Bill, "An Act To Protect the Privacy of Online Customer Information"

Amend the bill by striking out everything after the enacting clause and inserting the following:

'**Sec. 1. 5 MRSA c. 8** is enacted to read:

CHAPTER 8

PRIVACY OF PERSONAL DATA

§171. Definitions

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

1. Affiliate. "Affiliate" means a legal entity that controls, is controlled by or is under common control with another legal entity.

2. Consent. "Consent" means a clear affirmative act signifying a specific, informed and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear affirmative act.

3. Consumer. "Consumer" means a natural person who is a resident of the State acting only in an individual or household context. "Consumer" does not include a natural person from whom personal data is collected while that natural person is acting in a commercial or employment context.

4. Controller. "Controller" means a natural or legal person that, alone or jointly with others, determines the purposes and means of the processing of personal data.

5. Deidentified data. "Deidentified data" means:

A. Data that cannot be linked to a known natural person without additional information that is kept separately; or

B. Data:

(1) That has been modified to a degree that the risk of reidentification of a known natural person is small;

(2) That is subject to a public commitment by the controller not to attempt to reidentify the data; and

(3) To which has been applied one or more enforceable controls to prevent reidentification. Enforceable controls to prevent reidentification may include legal, administrative, technical or contractual controls.

6. Designated request address. "Designated request address" means an e-mail address, online form, toll-free telephone number or other reasonable method that a consumer may use to request the information required to be provided pursuant to this chapter.

7. Disclose. "Disclose" means to release, transfer, share, disseminate or otherwise communicate orally, in writing or by electronic or any other means to a 3rd party a consumer's personal data. "Disclose" does not include the disclosure of personal data by a controller to a 3rd party:

A. Under a written contract authorizing the 3rd party only to use or disclose the personal data to perform services on behalf of the controller;

B. Based on a good faith belief that disclosure is required to comply with applicable law, regulation, legal process or court order or is reasonably necessary to address fraud, risk management, security, an emergency or technical issues; to protect the controller's rights or property; or to protect against illegal activities; or

C. In connection with a proposed or actual sale to or merger with the 3rd party, bankruptcy of the controller or sale of all or part of the controller's assets to the 3rd party.

8. Online service. "Online service" means an information service provided over the Internet that processes personal data.

9. Personal data. "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include deidentified data or publicly available information. For the purposes of this subsection, "publicly available information" means information that is lawfully made available from federal, state or local government records.

10. Process. "Process" means to collect, use, store, disclose, analyze, delete or modify personal data.

11. Processor. "Processor" means a natural or legal person that processes personal data on behalf of a controller.

12. Sale. "Sale" means the exchange of personal data for monetary consideration by a controller to a 3rd party for purposes of licensing or selling personal data at the 3rd party's discretion to additional 3rd parties. "Sale" does not include:

A. The disclosure of personal data to a processor;

B. The disclosure of personal data to a 3rd party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer or otherwise in a manner that is consistent with a consumer's reasonable expectations considering the context in which the consumer provided the personal data to the controller;

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

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

13. Sensitive data. "Sensitive data" means:

A. A social security number or financial information that would allow use of or access to a consumer's bank or credit card account;

B. Personal data revealing a person's religious beliefs, mental or physical health diagnosis, medical records, sexual history or sexual orientation;

C. Genetic or biometric data that can uniquely identify a natural person; or

D. The personal data of a child under 13 years of age.

14. Third party. "Third party" means a natural or legal person, public authority, agency or body other than the consumer, the controller, the processor of the controller or an affiliate of the processor or of the controller.

15. Verified request. "Verified request" means a request made by a consumer to exercise a right or rights set forth in this chapter that can be reasonably authenticated by the controller using commercially reasonable means.

§172. Consumer rights

1. Right to transparency. A controller that collects personal data through the Internet about consumers who use or visit its commercial website or online service shall, in the controller's customer service agreement or incorporated addendum or any other readily available mechanism accessible to the consumer, provide a notice that:

A. Identifies all categories of personal data that the controller or the controller's processor processes about individual consumers collected through its commercial website or online service;

B. Identifies all categories of 3rd parties to whom the controller may disclose that personal data;

C. Discloses whether a 3rd party may collect personal data about an individual consumer's online activities over time and across different commercial websites or online services when the consumer uses the commercial website or online service of the controller;

D. Provides a description of the procedure for an individual consumer who uses or visits the commercial website or online service to review and request changes to inaccurate personal data that is collected by the controller as a result of the consumer's use or visits to the commercial website or online service;

E. Describes the procedure by which the controller notifies consumers who use or visit its commercial website or online service of material changes to the notice required to be made available through this subsection;

F. States the effective date of the notice; and

G. Provides a description of a consumer's rights, as required by this chapter, accompanied by one or more designated request addresses.

2. Right to know. A controller that sells a consumer's personal data collected through the consumer's use of or visit to the controller's commercial website or online service shall make the following information available to the consumer free of charge upon receipt of a verified request from the consumer:

A. All categories of the consumer's personal data that were sold; and

B. All categories of 3rd parties that received the consumer's personal data through a sale of the consumer's personal data by the controller.

3. Right to opt out of sale of personal data. A controller that sells the personal data of a consumer collected through the consumer's use of or visit to the controller's commercial website or online service shall clearly and conspicuously post on its commercial website or online service a designated request address or link to the designated request address through which a consumer may opt out of the sale of the consumer's personal data to 3rd parties by making a verified request. A controller may not require a consumer to establish an account with the controller in order to opt out of the sale of the consumer's personal data.

§173. Risk assessments for use of personal data

1. Risk assessment required. A controller shall conduct a risk assessment of each processing activity performed by the controller or the controller's processor that involves personal data. A controller shall conduct an additional risk assessment any time there is a change in processing that materially increases the risk to consumers. The risk assessment must take into account the category of personal data being processed by the controller or the controller's processor, including the extent to which the personal data is sensitive data or otherwise sensitive in nature, and the context in which the personal data is being processed. Risk assessments conducted under this subsection must identify and weigh the benefits that may flow directly and indirectly from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of consumers associated with such processing, as mitigated by safeguards that can be employed by the controller or the controller's processor to reduce such risks. The use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data is processed, must factor into the risk assessment.

The controller shall make the results of a risk assessment available to the Attorney General upon request. A risk assessment conducted under this subsection is confidential and not a public record pursuant to Title 1, section 402, subsection 3.

2. Consumer consent requirements. If the risk assessment conducted under subsection 1 determines that the potential risks to consumer privacy are substantial and

outweigh the interests of the controller, the consumer, other stakeholders and the public in the processing of the personal data of the consumer, the controller may engage in such processing only if the consumer provides consent to the processing or if the processing is covered by an exemption or limitation under section 175. Processing of personal data for a business purpose is presumed to be permissible unless it involves the processing of sensitive data and the risk of processing cannot be reduced through the use of appropriate administrative and technical safeguards. To the extent the controller seeks consumer consent for processing, the consent must be as easy to withdraw as to give.

§174. Response to verified requests

A controller that receives a verified request from a consumer through a designated request address under this chapter shall provide a response to the consumer within 60 days of the controller's authentication of the request. Upon an authenticated verified request from a consumer for information pertaining to sales of personal data, a controller shall provide the consumer information pertaining to all sales of the consumer's personal data pursuant to this chapter that occurred in the 12 months prior to the date of the consumer's verified request. This section does not apply to personal data disclosed or sold prior to July 1, 2021.

§175. Exemptions and limitations

1. Restrictions limited. Nothing in this chapter restricts a controller's or processor's ability to:

A. Comply with federal, state or local laws, rules or regulations;

B. Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, local or other governmental authorities;

C. Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or local law;

D. Investigate, exercise or defend legal claims;

E. Protect the vital interests of the consumer or of another natural person;

F. Prevent, detect or respond to identity theft, fraud or other malicious or illegal activity, safeguard intellectual property rights or verify identities; or

G. Assist another entity with any of the activities set forth in paragraphs A to F.

2. Requirements limited. Nothing in this chapter requires a controller or processor to reidentify deidentified data or to collect, retain, use, link or combine personal data concerning a consumer that the controller or processor would not otherwise collect, retain, use, link or combine in the ordinary course of business.

3. Application limited. Nothing in this chapter applies to:

A. Personal data collected, processed, sold or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994, 18 United States Code, Sections 2721 to 2725 (2019); or

B. The sale or provision of personal data to or from a consumer reporting agency if that data is reported in, or used to generate, a consumer report as defined by 15 United States Code, Section 1681a(d) as long as use of that data is limited in accordance with the federal Fair Credit Reporting Act, 15 United States Code, Sections 1681 to 1681x (2019).

§176. Enforcement

The Attorney General has exclusive authority to enforce this chapter. Whenever the Attorney General has reason to believe that a controller is not complying with any requirement of this chapter, the Attorney General may provide written notice of the alleged violation to the controller. If the controller fails to cure the alleged violation within 30 days of receipt of the notice, the Attorney General may bring an action in the name of the State against the controller to restrain by temporary or permanent injunction any failure to comply with this chapter, and the court may make such other orders or judgments as may be necessary to restore to any person who has suffered any ascertainable loss by reason of the failure to comply any money or property, real or personal, that may have been acquired by means of the failure to comply. Nothing in this chapter serves as the basis or grounds for a private right of action under this or any other law.

Sec. 2. Appropriations and allocations. The following appropriations and allocations are made.

ATTORNEY GENERAL, DEPARTMENT OF THE

Administration - Attorney General 0310

Initiative: Establishes one Assistant Attorney General position and one Cyber Investigator position and provides funding for related All Other costs.

GENERAL FUND	**2019-20**	**2020-21**
POSITIONS - LEGISLATIVE COUNT	2.000	2.000
Personal Services	$194,595	$267,244
All Other	$7,119	$9,492
GENERAL FUND TOTAL	$201,714	$276,736

Sec. 3. Effective date. This Act takes effect July 1, 2021.'

Amend the bill by relettering or renumbering any nonconsecutive Part letter or section number to read consecutively.

SUMMARY

This amendment replaces the bill. The amendment includes a transparency requirement under which a controller, defined as a person who controls personal data collected through the Internet about individual consumers who use or visit the controller's website or online service, is required to make certain disclosures to the consumers regarding the categories of data that are processed, the manner in which the data may be

shared with 3rd parties and any rights the consumer may have to review and request changes to inaccurate data collected by the controller. The amendment includes a right-to-know provision that requires controllers who sell personal data collected from individual consumers who use or visit the controller's website or online service to make available to the consumers, free of charge, all categories of data sold and all categories of 3rd parties who received the data. Additionally, the amendment requires controllers who sell personal data to 3rd parties to conspicuously post a designated address and provide consumers a right to opt out of the sale of the consumer's data by issuing a verified request through the designated address. Finally, the amendment requires consumer consent with regard to the sharing of certain sensitive information or information that is sensitive in nature, subject to a risk assessment by the controller. The amendment provides an effective date of July 1, 2021. The amendment also adds an appropriations and allocations section.

FISCAL NOTE REQUIRED

(See attached)