78th OREGON LEGISLATIVE ASSEMBLY--2015 Regular Session

SENATE AMENDMENTS TO SENATE BILL 601

By COMMITTEE ON JUDICIARY

April 24

On page 1 of the printed bill, line 3, delete "646A.602 and 646A.604" and insert "646A.602, 646A.604 and 646A.622".

On page 2, line 8, restore "in combination with" and delete the boldfaced material.

Delete lines 21 through 24 and insert:

"(E) Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction;

"(F) A consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or

"(G) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer.".

On page 3, line 20, delete ", maintains or otherwise possesses".

In line 22, before "personal" insert "or licenses".

In line 38, delete "100" and insert "250".

In line 40, after "of" insert ", or under license of,".

In line 42, delete "and the Attorney General".

In line 44, delete the boldfaced material.

In line 45, after "person" insert "that owns or licenses personal information".

On page 4, line 8, after "person" insert "that owns or licenses personal information".

In line 24, delete "and social media sites".

In line 25, delete "or a presence on a social media site".

In line 32, delete the comma.

In line 33, delete "maintained, licensed or possessed" and insert "or licensed".

On page 5, line 13, delete "breach of security" and after "procedures" insert "for a breach of security".

In lines 14 through 16, delete the boldfaced material and insert "the person's primary or functional federal regulator adopts, promulgates or issues in rules, regulations, procedures, guidelines or guidance, if the rules, regulations, procedures, guidelines or guidance" and restore the bracketed material.

In lines 23 and 24, delete the boldfaced material and insert "disclosure requirements at least as thorough as the protections and disclosure requirements provided under".

After line 27, insert:

"(d)(A) Except as provided in subparagraph (B) of this paragraph, a covered entity, as defined in 45 C.F.R. 160.103, as in effect on the effective date of this 2015 Act, that is governed under 45

C.F.R. parts 160 and 164, as in effect on the effective date of this 2015 Act, if the covered entity sends the Attorney General a copy of the notice the covered entity sent to consumers under ORS 646A.604 or a copy of the notice that the covered entity sent to the primary functional regulator designated for the covered entity under the Health Insurance Portability and Availability Act of 1996, (P.L. 104-191, 110 Stat. 1936, 42 U.S.C. 300(gg), 29 U.S.C. 118 et seq., 42 U.S.C. 1320(d) et seq., 45 C.F.R. parts 160 and 164).

“(B) A covered entity is subject to the provisions of this section if the covered entity does not send a copy of a notice described in subparagraph (A) of this paragraph to the Attorney General within a reasonable time after the Attorney General requests the copy.”.

In line 29, delete “that is subject to enforcement under ORS 646.632”.

After line 31, insert:

“**SECTION 3.** ORS 646A.622 is amended to read:

“646A.622. (1) [*Any*] **A** person that owns, maintains or otherwise possesses data that includes a consumer’s personal information that [*is used*] **the person uses** in the course of the person’s business, vocation, occupation or volunteer activities [*must*] **shall** develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, [*including disposal of the data*] **including safeguards that protect the personal information when the person disposes of the personal information**.

“(2) [*The following shall be deemed in compliance*] **A person complies** with subsection (1) of this section **if the person**:

“(a) [*A person that*] Complies with a state or federal law [*providing*] **that provides** greater protection to personal information than [*that provided by*] **the protections that** this section **provides**.

“(b) [*A person that is subject to and*] Complies with regulations promulgated [*pursuant to*] **under** Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 to 6809) as [*that Act existed on October 1, 2007*] **in effect on the effective date of this 2015 Act, if the person is subject to the Act**.

“(c) [*A person that is subject to and*] Complies with regulations [*implementing*] **that implement** the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164) as [*that Act existed on October 1, 2007*] **in effect on the effective date of this 2015 Act, if the person is subject to the Act**.

“(d) [*A person that*] Implements an information security program that includes [*the following*]:

“(A) Administrative safeguards such as [*the following, in which the person*]:

“(i) [*Designates*] **Designating** one or more employees to coordinate the security program;

“(ii) [*Identifies*] **Identifying** reasonably foreseeable internal and external risks;

“(iii) [*Assesses the sufficiency of*] **Assessing whether existing** safeguards [*in place to*] **adequately** control the identified risks;

“(iv) [*Trains and manages employees in the*] **Training and managing employees in** security program practices and procedures;

“(v) [*Selects*] **Selecting** service providers **that are** capable of maintaining appropriate safeguards, and [*requires those safeguards by contract*] **requiring the service providers by contract to maintain the safeguards**; and

“(vi) [*Adjusts*] **Adjusting** the security program in light of business changes or new circumstances;

“(B) Technical safeguards such as [*the following, in which the person*]:

"(i) [*Assesses*] **Assessing** risks in network and software design;

"(ii) [*Assesses*] **Assessing** risks in information processing, transmission and storage;

"(iii) [*Detects, prevents and responds*] **Detecting, preventing and responding** to attacks or system failures; and

"(iv) [*Regularly tests and monitors*] **Testing and monitoring regularly** the effectiveness of key controls, systems and procedures; and

"(C) Physical safeguards such as [*the following, in which the person*]:

"(i) [*Assesses*] **Assessing** risks of information storage and disposal;

"(ii) [*Detects, prevents and responds*] **Detecting, preventing and responding** to intrusions;

"(iii) [*Protects*] **Protecting** against unauthorized access to or use of personal information during or after [*the collection, transportation and destruction or disposal of the*] **collecting, transporting, destroying or disposing of the personal** information; and

"(iv) [*Disposes*] **Disposing** of personal information after [*it is no longer needed*] **the person no longer needs the personal information** for business purposes or as required by local, state or federal law by burning, pulverizing, shredding or modifying a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed.

"(3) A person complies with subsection (2)(d)(C)(iv) of this section if the person contracts with another person engaged in the business of record destruction to dispose of personal information in a manner **that is** consistent with subsection (2)(d)(C)(iv) of this section.

"(4) Notwithstanding subsection (2) of this section, a person that is an owner of a small business as defined in ORS 285B.123 (2) complies with subsection (1) of this section if the person's information security and disposal program contains administrative, technical and physical safeguards and disposal measures **that are** appropriate [*to*] **for** the size and complexity of the small business, the nature and scope of [*its*] **the small business's** activities, and the sensitivity of the personal information [*collected*] **the small business collects** from or about consumers.".

In line 32, delete "3" and insert "4".

On page 6, delete lines 5 through 7 and insert:

"**SECTION 5. The amendments to ORS 646.607, 646A.602, 646A.604 and 646A.622 by sections 1 to 4 of this 2015 Act apply to breaches of security that occur on or after the effective date of this 2015 Act.**".