SHB 1031 - H AMD **985**
By Representative Morris

ADOPTED 2/12/2008

Strike everything after the enacting clause and insert the following:

"NEW SECTION. **Sec. 1.** The legislature finds that Washington state, from its inception, has recognized the importance of maintaining individual privacy. The legislature further finds that protecting the confidentiality and privacy of an individual's personal information, especially when collected from the individual without his or her knowledge or consent, is critical to maintaining the safety and well-being of its citizens. The legislature recognizes that inclusion of identification devices that broadcast data or enable data or information to be collected or scanned either secretly or remotely, or both, will greatly magnify the potential risk to individual privacy, safety, and economic well-being that can occur from unauthorized interception and use of personal information. The legislature further recognizes that these types of technologies, whether offered by the private sector or issued by the government, can be pervasive.

NEW SECTION. **Sec. 2.** The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Identification device" means an item that uses radio frequency identification technology or facial recognition technology.

(2) "Person" means a natural person.

(3) "Personal information" has the same meaning as in RCW 19.255.010.

(4) "Data" means personal information, numerical values associated with a person's facial features, or unique personal identifier numbers stored on an identification device.

(5) "Radio frequency identification" means a technology that uses radio waves to transmit data remotely to readers.

(6) "Facial recognition" means a technology that attaches numerical values to a person's different facial features, creating a unique faceprint, which can be checked against a database of existing persons' faceprints.

(7) "Reader" means a scanning device that is capable of using radio waves to communicate with an identification device and read the data transmitted by that identification device.

(8) "Remotely" means that no physical contact between the identification device and the reader is necessary in order to transmit data.

(9) "Unique personal identifier number" means a randomly assigned string of numbers or symbols that is encoded on the identification device and is intended to identify the identification device.

NEW SECTION. **Sec. 3.** (1) Except as provided in section 5 of this act, a person that intentionally scans another person's identification device remotely, without that person's prior knowledge and prior consent, for the purpose of fraud, identity theft, or for any other illegal purpose, shall be guilty of a class C felony.

NEW SECTION. **Sec. 4.** (1) Except as provided in section 5 of this act, a person, governmental or business entity may not intentionally scan a person's identification device remotely for any purpose without that person's prior knowledge and consent.

(2) The legislature finds that the practices covered by this section are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. A violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW.

NEW SECTION. **Sec. 5.** Sections 3 and 4 of this act shall not apply to the following:

(1) The scanning of an identification device for triage or medical care during a disaster and immediate hospitalization or immediate outpatient care directly relating to a disaster;

(2) The scanning of an identification device by an emergency responder or health care professional for reasons relating to the health or safety of that person;

(3) The scanning of a person's identification device issued to a patient for emergency purposes;

(4) The scanning of an identification device of a person pursuant to court-ordered electronic monitoring;

(5) The scanning of an identification device of a person who is incarcerated in a correctional institution, juvenile detention facility, or mental health facility;

(6) The scanning of an identification device by law enforcement or government personnel who need to read a lost identification device when the owner is unavailable for notice, knowledge, or consent, or those parties specifically authorized by law enforcement or government personnel for the limited purpose of reading a lost identification device when the owner is unavailable for notice, knowledge, or consent;

(7) The scanning of an identification device by law enforcement personnel who need to read a person's identification device after an accident in which the person is unavailable for notice, knowledge, or consent;

(8) The scanning of an identification device by a person or entity that in the course of operating its own identification device system collects data from another identification device, provided that the inadvertently received data comports with all of the following:

(a) The data is not disclosed to any other party;

(b) The data is not used for any purpose; and

(c) The data is not stored or is promptly destroyed;

(9) The scanning of a person's identification device in the course of an act of good faith security research, experimentation, or scientific inquiry, including, but not limited to, activities

useful in identifying and analyzing security flaws and vulnerabilities; and

(10) The scanning of an identification device by law enforcement personnel who need to scan a person's identification device pursuant to a search warrant.

NEW SECTION. **Sec. 6.** (1) A governmental or business entity may collect, use, and store data associated with a person for the purposes of completing a sales transaction or providing a service.

(2) If a governmental or business entity intends to collect, use, or retain the data associated with a person after a sales transaction or service has been completed, the governmental or business entity first must obtain express, opt-in consent from the person associated with the data. The person's consent must be obtained either in writing or electronically. In obtaining the person's consent, the governmental or business entity shall unambiguously disclose that, by consenting, the person agrees to have the governmental or business entity collect, use, or retain data associated with them.

(3) A person may, at any time, opt out of the collection of data through either written or electronic means.

NEW SECTION. **Sec. 7.** Sections 3, 4, and 6 of this act do not apply if a governmental or business entity issuing an identification device to a person obtains that person's express, opt-in consent in writing or electronically. In obtaining consent, the governmental or business entity shall unambiguously disclose that, by consenting, that person agrees to have the governmental or business entity collect, use, or retain data gathered from the identification device.

NEW SECTION. **Sec. 8.** The office of the attorney general shall, on an annual basis, make recommendations to the legislature on other personally invasive technologies that may warrant further legislative action.

NEW SECTION. **Sec. 9.** If any provision of this act is found to be in conflict with federal law or regulations, the conflicting provision of this act is declared to be inoperative solely to the extent of the conflict, and that finding or determination shall not affect the operation of the remainder of this act.

NEW SECTION. **Sec. 10.** Sections 2 through 8 of this act are each added to a new chapter in Title 19 RCW."

Correct the title.

EFFECT: Strikes the provisions of the underlying bill.

Makes it a class C felony to intentionally scan another person's identification device remotely, without their knowledge and consent, for the purpose of fraud, identity theft, or some other illegal purpose.

Makes it a violation of the Consumer Protection Act to intentionally scan a person's identification device remotely for any purpose, without their consent.

Creates exceptions under which the scanning of an identification document is permissible, such as scanning by health care professionals, emergency responders, law enforcement, and scanning that occurs inadvertently.

Allows a governmental or business entity to use data collected from an identification device to complete a sales transaction or provide a service.

Requires a governmental or business entity to obtain the consent of the person associated with the data if the governmental or business entity intends to use or retain the data after the sale transaction or service has been completed.

Allows a person to opt-out of data being collected from an identification device.

Allows a governmental or business entity to scan or collect data from an identification device if the person being issued the identification device consents.

Requires the Attorney General's office to make recommendations to the Legislature annually on other personally invasive technologies that may warrant legislative action.