FINAL BILL REPORT
ESHB 1031

C 138 L 08

Synopsis as Enacted

Brief Description: Changing provisions concerning electronic devices.

Sponsors: By House Committee on Technology, Energy & Communications (originally sponsored by Representatives Morris, Hudgins, Moeller, Linville, B. Sullivan and Chase).

House Committee on Technology, Energy & Communications
Senate Committee on Financial Institutions & Insurance

Background:

Radio Frequency Identification.
Radio Frequency Identification (RFID) is a tagging and tracking technology that uses tiny electronic devices, called tags or chips, that are equipped with antennae. Passive RFID chips receive power from the electromagnetic field emitted by a reader in order to send the information contained on the chip to the reader. Active RFID chips have their own power source. Both active and passive RFID chips use radio waves to transmit and receive information.

Readers are devices that also have antennae. These reader-antennae receive information from the tag. The information gathered by the reader can be stored or matched to an existing record in a database. Most RFID chips can be read at a distance and often without the knowledge of the person who carries the item containing the RFID chip.

There are no federal or state laws that specifically prohibit or restrict the use of RFID.

Facial Recognition Technology.
Facial recognition technology is a type of technology that attaches numerical values to a person's different facial features and creates a unique faceprint. This faceprint can be checked against a database of existing persons' faceprints to identify a person.

Federal Privacy Laws.
Federal law contains a number of protections with respect to individual privacy.

The federal Privacy Act of 1974 protects unauthorized disclosure of certain federal government records pertaining to individuals. It also gives individuals the right to review records about themselves, to find out if these records have been disclosed, and to request corrections or amendments of these records, unless the records are legally exempt. The federal Privacy Act applies to the information gathering practices of the federal government, but does not apply to state or local governments or to the private sector.

In addition to the federal Privacy Act, there are other federal laws that limit how personal information may be disclosed. The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to give their customers privacy notices that explain the financial institution's information collection and sharing practices. Generally, if a financial institution shares a consumer's information, it must give the consumer the ability to "opt-out" and withhold their information from being shared.

The Fair Credit Reporting Act (FCRA) generally requires that credit reporting agencies follow reasonable procedures to protect the confidentiality, accuracy, and relevance of credit information. To accomplish this, the FCRA establishes a framework of fair information practices for personal information maintained by credit reporting agencies that includes the right to access and correct data, data security, limitations on use, requirements for data destruction, notice, consent, and accountability. In addition, the Health Insurance Portability and Accountability Act (HIPAA) limits the sharing of individual health and personal information.

Washington's Privacy Laws.
The Washington Privacy Act restricts the interception or recording of private communications or conversations. As a general rule, it is unlawful for any person to intercept or record a private communication or conversation without first obtaining the consent of all parties participating in the communication or conversation. There are some limited exceptions to this general rule that allow the communication or conversation to be intercepted and recorded when only one party consents, or allow it to be intercepted pursuant to a court order.

Certain persons and activities are exempt from the Washington Privacy Act, including common carriers in connection with services provided pursuant to its tariffs on file with the Washington Utilities and Transportation Commission and emergency 911 service.

In addition to the Washington Privacy Act, Washington law contains a number of provisions with respect to invasions of privacy, including provisions related to identity theft, computer theft, stalking, and "skimming" crimes, which refers an identification or payment card being copied for illegal purposes.

Summary:

Scanning of an Identification Device.
It is a class C felony for a person to intentionally scan another person's identification device remotely, without that person's prior knowledge and consent, for the purpose of fraud, identity theft, or another illegal purpose.

Definitions.
An identification device is defined as an item that uses radio frequency identification technology (RFID) or facial recognition technology.

RFID is defined as a technology that uses radio waves to transmit data remotely to readers.

Data is defined as personal information, numerical values associated with a person's facial features, or unique personal identifier numbers stored on an identification device.

Personal information is defined as an individual's first name or first initial and last name in combination with any one of the following data elements, when either the name or the data elements are not encrypted: (1) social security number; (2) driver's license number or Washington identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Personal information does not include information that is lawfully made available to the general public from federal, state, or local government records.

Votes on Final Passage:

House	69	28	
Senate	47	0	(Senate amended)
House	93	0	(House concurred)

Effective: June 12, 2008