Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Technology, Energy & Communications Committee

HB 1011

Brief Description: Regulating the use of identification devices by governmental and business entities.

Sponsors: Representatives Morris, Chase, Hasegawa, Kagi, Darneille, Upthegrove, Hudgins and Moeller.

Brief Summary of Bill

- Makes the scanning of a person's identification device unlawful, unless that person has provided opt-in consent or an exception applies.
- Prohibits the collection, use, or storage of data without obtaining opt-in consent, unless it is for completing a sale or providing a service.
- Makes the unlawful scanning of an identification device a violation of the Consumer Protection Act.
- Requires the Attorney General's Office to report annually on personally invasive technologies.

Hearing Date: 1/14/09

Staff: Kara Durbin (786-7133)

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.

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

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.

Facial Recognition Technology

Facial recognition technology 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.

There are no federal laws that regulate the collection and processing of personal information gathered through RFID.

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 to an identification or payment card being copied for illegal purposes.

In 2008, the Legislature passed two laws related to RFID. It is a class C felony to either:
(1) scan another person's identification device remotely for the purpose of fraud or identity theft, if accomplished without that person's knowledge and consent; or
(2) read or capture information contained on another person's identification document using radio waves without that person's knowledge or consent.

Summary of Bill:

Opt-in Consent
A governmental or business entity, or an individual, may not intentionally scan a person's identification device remotely without that person's opt-in consent. Opt-in consent may be secured in writing or electronically. In obtaining consent, the government or business entity must disclose that, by consenting, the person agrees to have the governmental or business entity collect, use, or retain data gathered from the identification device for any purpose.

Opt-in consent is not required in order to scan an identification device for one of the following purposes:

- Triage or medical care during a disaster;
- Health or safety, if scanned by an emergency responder or health care professional;
- Incarceration;
- Responding to an accident, if the person is unavailable for notice, knowledge, or consent;
- Court-ordered electronic monitoring;
- Law enforcement, if conducted pursuant to a search warrant;
- Research, if the scanning is conducted in the course of good faith security research, experimentation or scientific inquiry; and
- Inadvertent scanning by a person or entity in the process of operating its own identification device system, if certain conditions are met.

A lost identification device also may be read without obtaining opt-in consent if the owner is unavailable for notice, knowledge or consent, and the device is read by law enforcement or government personnel.

A violation of the opt-in consent provisions of the bill is a violation of the Consumer Protection Act.

Collection of Data From an Identification Device
A governmental or business entity may not collect, use or store data associated with a person for purposes other than completing a sales transaction or providing a service, unless opt-in consent is secured from the person associated with the data. Opt-in consent may be secured in writing or electronically. In obtaining consent, the government or business entity must disclose that, by

consenting, the person agrees to have the governmental or business entity collect, use, or retain data associated with them.

A person who has provided opt-in consent may opt-out at any time in writing or electronically.

Reporting
The Attorney General's Office must report annually to the Legislature on personally invasive technologies that may warrant legislative action.

Definition of Radio Frequency Identification
The definition of "radio frequency identification" is amended. Radio frequency identification is defined as the use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag. This communication can occur through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it.

Appropriation: None.

Fiscal Note: Not requested.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.