HOUSE BILL REPORT
SHB 1011

As Passed House:
March 3, 2009

Title: An act relating to regulating the use of identification devices.

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

Sponsors: House Committee on Technology, Energy & Communications (originally sponsored by Representatives Morris, Chase, Hasegawa, Kagi, Darneille, Upthegrove, Hudgins and Moeller).

Brief History:
Committee Activity:
Technology, Energy & Communications: 1/14/09, 2/16/09 [DPS].
Floor Activity
Passed House: 3/3/09, 96-1.

Brief Summary of Substitute Bill

- Prohibits a government or business entity from remotely reading an identification device, unless the government or business entity, or one of their affiliates, is the same entity that issued the identification device, or an exception applies.
- Makes the unlawful scanning of an identification device a violation of the Consumer Protection Act.

HOUSE COMMITTEE ON TECHNOLOGY, ENERGY & COMMUNICATIONS

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 11 members: Representatives McCoy, Chair; Eddy, Vice Chair; Crouse, Ranking Minority Member; Finn, Hasegawa, Hudgins, Jacks, McCune, Morris, Takko and Van De Wege.

Minority Report: Without recommendation. Signed by 4 members: Representatives Haler, Assistant Ranking Minority Member; Carlyle, Condotta and Herrera.

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.

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.

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 (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 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 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 Substitute Bill:

A government or business entity is prohibited from remotely reading an identification device using radio frequency identification (RFID) technology, unless the government or business entity, or one of their affiliates, is the same entity that issued the identification device.

This prohibition does not apply to a person remotely reading 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 if the owner is unavailable for notice, knowledge or consent, and the device is read by law enforcement or government personnel.

The unlawful reading of an identification device is a violation of the Consumer Protection Act.

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

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.

Staff Summary of Public Testimony:

(In support) This is the third year the Technology, Energy and Communications Committee has taken up this issue. There are many good applications for this technology. Consumers should have some ability to know where this technology exists and when it is on their person. Consumers should be able to make a conscious choice as to whether they want to accept a radio frequency identification (RFID) chip. They should not be slipped a chip without their knowledge. The exemptions recognize legitimate uses, such as use by law enforcement or for public safety purposes.

(Opposed) This issue is better suited for a national solution. It will be expensive for retailers to comply with these provisions. This legislation is premature. We are not sure what problem we are trying to solve. Loyalty cards are issued through an opt-in model and do not currently contain RFID chips. These RFID tags are an important tool in preventing shoplifting and controlling inventory. It is also a technology that helps us ensure food integrity and safety. Products regulated by the federal Food and Drug Administration should be exempt. Consumers are not being slipped chips without their knowledge.

State chartered banks should not be placed at a competitive disadvantage by having to comply with the opt-in provisions.

The bill places burdens on businesses in terms of compliance. Many benefits of RFID technology may be stifled. We supported last year's RFID bill, which criminalized illegal behavior. We are concerned about how credit reporting agencies will comply with these provisions and other requirements under federal law.

Persons Testifying: (In support) Representative Morris, prime sponsor.

(Opposed) Mark Johnson, Washington Retail Association; Holly Chisa, Northwest Grocery Association; Carolyn Logue, Washington Food Industry; Danny Eliason, Washington Bankers Association; Tom McBride, Technology Association of America; Lew McMurran,

Washington Technology Industry Association; John Drescher, TechNet; Grant Nelson, Association of Washington Business; and Cliff Webster, Consumer Data Industry Association.

Persons Signed In To Testify But Not Testifying: (In support) Shankar Narayan, American Civil Liberties Union.