FINAL BILL REPORT
SHB 1011

PARTIAL VETO
C 66 L 09
Synopsis as Enacted

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).

House Committee on Technology, Energy & Communications
Senate Committee on Financial Institutions, Housing & 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. RFIC chips are used in many different applications, including supply chain management, payment devices, identification documents, and asset tracking.

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

---

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.

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 his or her 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 emergency 911 service and common carriers in connection with services provided pursuant to its tariffs on file with the Washington Utilities and Transportation.

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.

In 2008 the Legislature passed two laws related to RFID. It is a class C felony to either:

- 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
- read or capture information contained on another person's identification document using radio waves without that person's knowledge or consent.

Summary:

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 its 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.

Votes on Final Passage:

House	96	1
Senate	41	4

Effective: July 26, 2009

Partial Veto Summary: The Governor vetoed the section that required the Attorney General to make annual recommendations to the Legislature with respect to potentially invasive technologies that may warrant further action by the Legislature.