SENATE BILL REPORT
ESHB 1031

As Reported By Senate Committee On:
Financial Institutions & Insurance, February 27, 2008

Title: An act relating to electronic communication devices.

Brief Description: Changing provisions concerning electronic devices.

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

Brief History: Passed House: 2/12/08, 69-28.
Committee Activity: Financial Institutions & Insurance:2/26/08, 2/27/08 [DPA].

SENATE COMMITTEE ON FINANCIAL INSTITUTIONS & INSURANCE

Majority Report: Do pass as amended.
Signed by Senators Berkey, Chair; Hobbs, Vice Chair; Benton, Ranking Minority Member; Franklin, Parlette, Prentice and Schoesler.

Staff: Diane Smith (786-7410)

Background: 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 the electrical power to send the information they contain to the reader, from the electromagnetic field emitted by the reader itself. Active RFID chips have their own power source. In both cases, the transmissions and receptions use FM radio waves.

Readers are devices that also have antennae. These reader-antennae receive the 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 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 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

---

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.

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 can 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.

The Washington Privacy Act, Chapter 9.73 RCW, 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 state 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 the copying of an identification or payment for illegal purposes.

Summary of Bill (Recommended Amendments): 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.

Identification device is defined as an item that uses radio frequency identification technology or facial recognition technology.

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

EFFECT OF CHANGES MADE BY INSTITUTIONS & INSURANCE COMMITTEE (Recommended Amendments): The striking amendment removes the reference to violations of the Consumer Protection Act; to prohibitions against scanning a person's identification device remotely by another person, governmental or business entity without a person's express, opt-in consent and exception to this prohibition; to the reference to a governmental or business entity's ability to collect, use, and store data for the purposes of completing a sales transaction or providing a service; and to the annual recommendations to the Legislature required by the Office of the Attorney General.

Appropriation: None.

Fiscal Note: Not requested.

Committee/Commission/Task Force Created: No.
Staff Summary of Public Testimony on Engrossed Substitute Bill: PRO: This bill represents four years of work. It establishes some basic rules for this new technology before it is widely deployed. It is on the cusp of being widely deployed. The technology is unique because it is unseen and covert at the chip or reader level. It is like a pick-pocket that does not have to touch your pocket to get the information out of it. Section 3 treats the criminal aspect, called "skimming." Sections 4 through 6 are where you find the rules of the road. There is a disconnect between manufacturers and those who deploy the technology. Inventory chips are used when a more secure chip is needed. Bank One's credit cards had no encryption so could be read in post office boxes. This was an early misapplication of the technology. The first passports were unencrypted and included country codes. If a higher value chip had been used, as has now been done, the aluminum foil protectors would not have been needed. Should consumers have a right to opt-in? Should deployers have a right to slip the consumer a chip? Loyalty cards are evidence of a relationship between the issuer and the shopper. This relationship should end there, and not be shared without the shopper's permission, by other retailers into whose stores the shopper may go. Labeling has dropped out. Wireless phones have 73 percent market penetration. Waving them over a reader to pay for purchases, as is done now with charge cards, is in the near future. People don't know that this contains this new technology called RFID. Its use is acceptable as long as its use is a knowing choice. The European Union and the United Kingdom have moved more quickly than we have. They have basic privacy laws for electronic data that are not seen in the U.S.A. Their RFID legislation is an add-on to their existing structure.

CON: This bill is anti-technology and anti-innovation. It is a response first of fear and then of regulation, rather than of celebration. It is a slippery slope leading to the message that innovators are not welcome here. How ironic. It punishes RFID instead of fraud and identity theft. It is unclear. It adds to the cost of doing business. Jobs will go elsewhere. Cell phones have no RFIDs. But the bill includes cell phones. There are five million cell phone customers in Washington. With passage of this bill, this product could go away in Washington. The bill

is not necessary. It does not address privacy properly because privacy is not at risk. It perpetuates myths. CDMA technology transmits using encrypted packets of information which is impossible to retrieve with an RFID reader. Existing federal and state laws address bad actors. The bill puts us at a competitive disadvantage. Bad behavior should be addressed. Section four rules out the use of RFID. Please reconsider the bill's effects on the maritime industry. RFID is used when pallets transit to and from docks, after 911. It is needed to protect equipment and the public at large. New federal TWIK cards will soon become standard. There is no recognition of the use of RFID in the pharmaceutical industry. This technology enables compliance with federal law. Pharmaceutical products must be protected from diversion and be able to be recalled with dispatch. This use is integral to public health and safety. The RF technology card would also be part of this bill and it has no personal information on it: it is the result of enormous public investment to facilitate convenient operation of toll roads. The bill is poorly conceived.

Persons Testifying: PRO: Representative Jeff Morris, prime sponsor.

CON: John Drescher, TechNet; Russel Sarazan, T-Mobile; Joyce Masamitsu, Verizon Wireless;
Terry Byington, American Electronics Association; Scott Hazelgrove, Pacific Merchant Shipping Association; Cliff Webster, Pharmaceutical Research & Manufacturers of America; Kevin Desmond, King County Transit Association.

Signed in, Unable to Testify & Submitted Written Testimony: CON: Mark Johnson, Washington Retail Association; Grant Nelson, Association of Washington Business.