HOUSE BILL REPORT
ESHB 1031

As Passed House:
February 12, 2008

Title: An act relating to electronic communication devices.

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).

Brief History:
Committee Activity:
Technology, Energy & Communications: 1/10/07, 2/23/07 [DPS].
Floor Activity:
Passed House: 2/12/08, 69-28.

Brief Summary of Engrossed Substitute Bill

- Prohibits the unauthorized scanning of an identification device remotely, unless an exception applies.
- Restricts the collection and retention of certain types of data by a governmental or business entity, unless the person associated with the data consents

HOUSE COMMITTEE ON TECHNOLOGY, ENERGY & COMMUNICATIONS

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 9 members: Representatives Morris, Chair; McCoy, Vice Chair; Crouse, Ranking Minority Member; McCune, Assistant Ranking Minority Member; Eddy, Hudgins, Hurst, Takko and VanDeWege.

Minority Report: Without recommendation. Signed by 2 members: Representatives Ericksen and Hankins.

Staff: Kara Durbin (786-7133).

Background:

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.

Overview of 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 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.

Washington's Privacy Act

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 when an identification or payment card is copied for illegal purposes.

Radio Frequency Identification

Radio Frequency Identification (RFID) is a tagging and tracking technology that uses tiny electronic devices equipped with antennae, which can transmit identifying information to a remote reader. The information gathered by the reader can be stored or matched to an existing

record in a database. Most RFID tags can be read at a distance and often without the knowledge of the person who carries the item containing the RFID tag.

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.

Summary of Engrossed Substitute Bill:

Prohibition on Unauthorized 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, unless an exception applies.

It is a violation of the Consumer Protection Act for a person or governmental or business entity to intentionally scan a person's identification device remotely, without that person's prior knowledge and consent, unless an exception applies.

These prohibitions do not apply if a governmental or business entity issuing an identification device to a person obtains that person's express, opt-in consent.

Exceptions:
An identification device may be scanned for the following purposes:

- triage or medical care during a disaster and immediate hospitalization or immediate outpatient care directly related to a disaster;
- health or safety reasons if scanned by an emergency responder or health care professional;
- emergency purposes, if the identification device has been issued to a patient;court-ordered electronic monitoring;
- incarceration purposes; and
- security research, experimentation, or scientific inquiry, provided that the scanning of the identification device occurs in the course of an act of good faith.

Lost identification devices may be read by law enforcement, government personnel, or those parties specifically authorized by law enforcement or government personnel when the owner of the identification device is unavailable for notice, knowledge, or consent.

In addition, law enforcement personnel may read a person's identification device: (1) after an accident if the person is unavailable to provide notice, knowledge, or consent; and (2) pursuant to a search warrant.

A person or entity may inadvertently collect data from another identification device in the course of operating its own identification device system, provided that: (1) the data is not

disclosed to any other party; (2) the data is not used for any purpose; and (3) the data is not stored or is promptly destroyed.

Data Collection and Retention:
A governmental or business entity may collect, use, and store data for the purposes of completing a sales transaction or providing a service.

If the government entity intends to collect, use or retain data associated with a person after a sales transaction or service has been completed, the governmental or business entity first must obtain express, opt-in consent from the person associated with the data. Consent must be obtained in writing or electronically. In obtaining the person's consent, it must be clearly stated that information associated with the person will be collected and maintained.

A person may opt-out of the collection of data at any time.

These restrictions do not apply if a governmental or business entity issuing an identification device to a person obtains that person's express, opt-in consent.

Reporting:
The Office of the Attorney General is required to make recommendations annually on other personally invasive technologies that may warrant further legislative action.

Definitions:
"Identification device" means as an item that uses radio frequency identification technology or facial recognition technology.

"Radio frequency identification" means a technology that uses radio waves to transmit data remotely to readers.

"Facial recognition" means a technology that attaches numerical values to a person's different facial features, creating a unique faceprint, which can be checked against a database of existing persons' faceprints.

"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.

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony:

Testimony on proposed substitute bill heard January 10, 2007

(In support) I am really pleased to see this bill coming forward. This bill attempts to strike a good balance between the needs for privacy and the needs for businesses to transact electronically. This is the right timing for this. We need to protect people's privacy. Privacy policies are critical, but consumers need to know that they retain their privacy and that they're not being tracked through the merchandise they purchase. I strongly support this bill. I feel the notice and labeling provisions are very important.

(In support with concerns) It is important that we get ahead of this technology and not wait for the violations to start occurring. We have worked with other sponsors on legislation with respect to RFID and will continue to support such efforts. We hope these protections can be put in place.

(With concerns) This would impact our automatic meter readers.

(Opposed) We are committed to protecting our customer's confidential information. We are concerned that there may be some unintended consequences with this bill. We are already heavily regulated regarding customer proprietary network information. This is unnecessarily burdensome. This could require complex changes to our business practices, yet we're not sure whether there's a problem with the capture of data from wireless phones. This bill should focus on nefarious use of customer information. We have strong privacy policies already in place. We have significant concerns with this bill. We believe RFID will be a part of our financial future. These RFID devices will continue to be embedded in debit and credit cards. These devices are convenient and secure. We believe this bill could cause great havoc on financial transactions. This would significantly inhibit the ability for debit and credit card transactions to occur. We believe RFID has some very good potential uses. Security issues are better addressed at the design level. This bill is moving in the right direction but it raises too many questions. Government use of RFID is much more concerning than the private sector. Supply chain visibility is a great use of RFID as well as anti-counterfeit purposes. We don't want to stifle this industry prematurely. We support state consumer protections, but don't feel this is the appropriate approach. We'd prefer to see bans on unauthorized use of the technology.

Testimony on proposed substitute heard on February 16, 2007

(In support) I wanted to get comments in the record based on the new draft. I have removed the watermarking and disclosure provisions of the bill. I want to get key components into code and then take a closer look at other issues over the interim. I have held five workgroup meetings during session, and I held meetings before session. There has been a varying level

of participation in this bill from the stakeholders. I think this is a critical issue for us to understand and I think the bill has come a long way.

We applaud you for bringing this bill forward to address the privacy risks associated with these types of technologies. We encourage you to incorporate new technologies and to pursue additional enforcement mechanisms. Victims are being found through readily available data sources. Unique identifiers can still become identifiable. We would like to see this bill limit the collection of personal data. We strongly urge you to see this effort through. It is interesting that there is so much opposition to this straightforward bill. It is providing for labeling and notice to consumers. The technology is great, but we must protect the privacy of our consumers. Consumers should have notice of the presence of the readers. Tag numbers can be collected, collated and used to identify consumers. These tag numbers should be included in the bill.

(In support with concerns) This is just a starting point. Adding RFID to items that we carry around allow those items to become associated with our person. We believe we should have control over who accesses that information. This is extremely important. It is important for the state to put some parameters around this technology. We appreciate the notice, but would like notice to be given whether the device transmits personal information or not. We appreciate the labeling and deactivation provisions. We would like to see the private cause of action and the Attorney General enforcement mechanism.

(With concerns) We appreciate that you have worked very hard on this bill. We have seen a narrowing of the focus on this bill to RFID devices. However, we are concerned that this language may still include some wireless devices. This bill, if it includes wireless devices, could have a devastating impact on our industry. We will lose customers if we give up their personal information. We support the responsible use of RFID technology.

(Opposed) High-tech crimes often require a high-tech solution. We already have sophisticated data protocols and don't feel that our customers' private information is at risk. This is a greatly improved bill. Compliance looks possible and it is much narrower. This does create some new business risks. We would prefer to see the Attorney General enforce the bill rather than a private right of action. We cannot support the bill as currently drafted because we feel it is aimed at the retail sector, but it also negatively impacts the health care sector. The health care industry is already highly regulated in terms of disclosure of personal information. We don't feel like an additional law is needed. Smart cards are much more secure than RFID tags. We feel this bill will stifle the use of beneficial technologies like RFID. Instead, it should crack down on nefarious use. We are opposed to the bill in the current draft because it encompasses access cards and proximity cards. They don't carry personal information on them. Labeling and deactivation for automobile application is difficult. Key fobs and tire pressure devices are implicated and it is problematic for us to have to label and possibly deactivate them.

Persons Testifying:

January 10, 2007

(In support) Representative Morris, prime sponsor; Leslie Simons Michelassi, Consumers Against Supermarket Privacy Invasion and Numbering; and Jeff Benton.

(In support with concerns) Jennifer Shaw, American Civil Liberties Union of Washington.

(With concerns) Dave Warren, Washington Public Utility Districts Association.

(Opposed) Russell Sarazen, T-Mobile; Steve Gano, Cingular Wireless; Denny Eliason, Washington Bankers Association; Lew McMurran, Washington Software Alliance; Mark Johnson, Washington Retail Association; Allison Fleming, EPC Global; Caroline Silviera, Grocery Manufacturer's Association; and Nancy Atwood, American Electronics Association.

February 16, 2007
(In support) Representative Morris, prime sponsor; and Leslie Simons Michelassi, Consumers Against Supermarket Privacy Invasion and Numbering.

(In support with concerns) Teresa Atkinson, Washington State Coalition Against Domestic Violence; Jennifer Shaw, American Civil Liberties Union of Washington; Art Butler, WebTec.

(With concerns) Russell Sarazen, T-Mobile; Peter Their, Washington State Transit Association; and Candace Carlson, King County Metro Transit.

(Opposed) Joyce Masamitsu, Verizon Wireless; Dan Youmans, Cingular Wireless; Lew McMurran, Washington Software Alliance; Tom Byron, Washington State Hospital Association; Nancy Atwood, American Electronics Association; James Sheire, NXP Semiconductors; Mark Johnson, Washington Retail Association; Cliff Webster, HID Global, General Motors and PhRMA; and Nancee Wildermuth, Sprint Nextel, Regence Blue Shield and the Alliance of Auto Manufacturers.

Persons Signed In To Testify But Not Testifying: None.