Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Technology, Energy & Communications Committee

HB 1031

Brief Description: Changing provisions concerning electronic devices.

Sponsors: Representatives Morris, Hudgins, Moeller, Linville, B. Sullivan and Chase.

Brief Summary of Bill

- Requires that a person selling, issuing, or distributing items containing an electronic communication device must post a notice and label the item.
- Allows a consumer to request access to any personal information gathered through an electronic communication device and to contest, amend, or seek to remove the information.
- Prohibits a person from combining or linking a consumer's personal information with information gathered from an electronic communication device.
- Prohibits disclosure to third parties of information gathered by an electronic communication device.
- Creates civil and criminal penalties.

Hearing Date: 1/10/07

Staff: Kara Durbin (786-7133).

Background:

Overview of Federal Privacy Laws:
Federal law contains a number of protections with respect to individual privacy.

The 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

---

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.

find out if these records have been disclosed, and to request corrections or amendments of these records, unless the records are legally exempt. The 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 & 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 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. 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.

Summary of Bill:

Consumers are granted the following rights with respect to electronic privacy:

- To receive notice of an entity's information practices before personal information is collected;
- To receive choices as to how personal information collected from an individual may be used;

- To access one's personal information and to contest the accuracy of such information;
- To expect that collectors of data will implement security measures;
- To seek private remedies if any of the above-mentioned rights are violated.

Definition of electronic communication device
An electronic communication device is defined as any device that can transfer signs, signals, writing, images, sound, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system, but does not include: a written or oral communication; a tone-only paging device; or a communication from a tracking device.

Definition of person
Person is defined as an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture government, government subdivision, agency or instrumentality, public corporation, or any other legal or commercial entity.

Notice
Any person that sells, issues, or distributes items containing an electronic communication device must post a notice informing the consumer of the use of such technology. The notice must disclose the following information:

1. The item contains or may contain an electronic communication device;
2. The consumer has the legal right to request that an item containing an electronic communication device be removed or deactivated before the item leaves the premises; and
3. The consumer has the right to request a copy of all personal information collected about himself or herself through an electronic communication device, including the identity of any person who has had access to the consumer's personal information.

Labeling
A person must not sell, use, or distribute an item that contains an electronic communication device without labeling the item with a notice stating that a) the item contains an electronic communication device capable of engaging in electronic communication; and b) the device can transmit personal information to an independent reader or scanner both before and after purchase or issuance.

Requesting review of personal information
A consumer may request all stored personal information pertaining to himself or herself, including the identity of any individual or entity who has had access to the consumer's personal information.

After reviewing one's personal information, the consumer must be given the opportunity to contest the accuracy of his or her personal data, correct or amend the data, and request that the information be removed or destroyed from the database, unless removal or destruction would be contrary to state or federal law.

Removal or deactivation
Upon request by a consumer, a person who sells, issues, or distributes an item containing an electronic communication device must remove or deactivate the device before the consumer

leaves the premises. Any costs associated with removal or deactivation cannot be passed on to the consumer.

Requiring use
A consumer shall not be coerced into keeping an electronic communication device active on the item in order for the consumer to be able to exchange, return, repair, or service the item.

A consumer shall not be coerced into retaining an active electronic communication device as a condition of employment.

Reactivation
Once an electronic communication device has been deactivated, it must not be reactivated without the express, written consent of the consumer associated with the item.

Linking of personal information
A person must not combine or link a consumer's personal information with information gathered by, or contained within, a device capable of engaging in electronic communication.

Security measures
Any person who sells or utilizes an electronic communication device must implement adequate security measures to ensure that information is secure from unauthorized access, loss or tampering. These security measures should be consistent with industry standards that are commensurate with the amount and sensitivity of the information being stored on the system.

Unauthorized scanning
A person may not use an electronic communication device to remotely scan, or attempt to scan, an item associated with a consumer without the consumer's knowledge.

Other prohibited uses
A person may not disclose, either directly or through an affiliate, a consumer's personal information associated with information gathered by, or contained within, a device capable of engaging in electronic communication. A person also may not use, either directly or through an affiliate or nonaffiliated third party, information gathered by, or contained within, a device capable of engaging in electronic communication in order to identify a consumer.

Penalties:
An injured person may bring a civil action in district or superior court to seek an injunction and to seek up to $500 per violation, or actual damages, whichever is greater. The court may triple the damage award (up to $1,500 per violation) if the defendant has engaged in a pattern and practice of violating any of the provisions of this bill.

Willful violation of this bill constitutes a gross misdemeanor. If willful violation occurs in conjunction with the commission of another unlawful act, then the offense is a class B felony.

Appropriation: None.

Fiscal Note: Revised fiscal note requested on proposed substitute (H-2116.1) February 15, 2007.

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