

# Washington State House Gives Nod to Privacy Bill

The state's house of representatives approved a bill that would make RFID "skimming" a felony and prohibit capturing data from an RFID tag in an identity card without the cardholder's permission.

By Claire Swedberg

Feb. 15, 2008—A revised version of legislation intended to protect the privacy of individuals using RFID tags with "unique personal identifier numbers" passed the Washington State House of Representatives on Wednesday. [House Bill \(HB\) 1031](#)—intended to limit collection of personal information from an RFID tag without the tag holder's knowledge or consent—passed with 69 to 27 votes. The bill is now headed for the State Senate and, if approved, to the office of Governor Christine Gregoire.

This is the second round for HB 1031. An earlier version failed to pass a House vote in March 2007 (see [Washington's RFID Bill Halted](#)). In its original form, HB 1031 was rejected because of its broad scope, says the bill's primary sponsor, State Representative Jeff Morris (D-Mount Vernon). Known at that time as the "Electronic Bill of Rights," the first version did not offer exemptions for a host of users, including emergency responders, university researchers and service providers such as cable companies. The revised bill also has eliminated mention of a labeling requirement ("A person shall not sell, use, or distribute an item that contains an electronic communication device without labeling such item with a notice stating that such item contains an electronic device capable of engaging in electronic communication"). Such a requirement was opposed by business associations and technology vendors, who argue that they already have labeling conduct codes in place through organizations such as EPCglobal.

The revised bill would make it a Class C felony to intentionally read the data encoded to an RFID tag in possession of a person without that individual's knowledge and consent, for the purpose of fraud, identity theft or some other illegal or unapproved purpose—a process known as "skimming." With this bill, skimming refers to capturing personal data about a tag's holder, such as the details on a loyalty card, driver's license or other identity card. It does not refer to capturing data from EPC RFID tags attached to products that do not hold the consumer's data. Class C felony in Washington State has a maximum penalty of five years in prison and a \$10,000 fine. If the bill is signed into law, it would be the first legislation on the state level to make skimming a felony, says Morris.

On the other hand, use of data for marketing purposes, by a retailer would be a civil offense with a fine of up to \$10,000 for each violation at the attorney general's discretion.

If, for example, a consumer holding an RFID-enabled loyalty card from one store enters a second store, that second store could not make use of the data stored on the loyalty card under the bill. Also, when a consumer applies for a loyalty card or other identification card containing an RFID tag, the application process must inform the consumer about the use of RFID technology and the user would need to sign that notification to indicate acceptance.

After the House rejected the first version of the bill, Morris says, he met with stakeholder groups and "went through the process of refining it down." Now, he says, the bill includes exemptions for multiple interests, including those who provide emergency services. The exemptions allow the use of RFID-tagged identification bracelets for emergency patients, as well as permit the use of RFID tags to track items or people in research projects carried out by the [University of Washington](#) or other institutions. Service providers, such as cable companies that put RFID chips in desktop boxes to chronicle viewing patterns for ratings purposes, are also exempt, as are penal institutions.

HB 1031 also calls for the state's attorney general to make an annual review of personally invasive technologies and present the findings to lawmakers.

The State Senate will hold its first hearing on the bill in two weeks, and Morris says it is too early to predict the Senate's response. "We have been talking about this for four years in the House," he says, adding that some members have little or no knowledge of the technology. He notes that Governor Gregoire's office is monitoring the bill's progress. "My hope is she would sign it," he says.

Some groups that opposed the original SB 1031 are neutral to version passed by the House, says Morris, including the [Washington Technology Industry Association](#) and the [Smart Card Alliance](#). Members of the cellular communications industry, which is preparing to introduce mobile phones with Near Field Communication (NFC) RFID technology, oppose the current bill, he says.

RELATED\_ARTICLES In describing the importance of privacy-protecting measures for RFID users, Morris says, "The issue here is the rights of the consumer. The buyer can only beware if they are aware of what technology is being used."

On Jan. 30, California's state senate passed a similar bill, [Senate Bill \(SB\) 31](#), which proposes that a person or entity that intentionally remotely reads another person's RFID-enabled identification document without prior consent shall be punished by imprisonment for up to one year, a fine of not more than \$1,500." The bill has now gone to the California State Assembly. The state has crafted other RFID-related measures as well. In 2007, California Governor Arnold Schwarzenegger signed into law a bill prohibiting anyone from forcibly implanting RFID tags under someone's skin (see [RFID News Roundup: California Bans Forced Human Tagging](#)), but in 2006, he vetoed SB 768, which would have put restrictions on RFID systems used by government agencies in the state (see [Calif. Gov Terminates RFID ID Bill](#)).

Copyright ©2005 RFID Journal, Inc. All Rights Reserved