

# Washington State Governor Signs Anti-Skimming Law

The new law makes it a felony to scan an RFID tag belonging to another person without that individual's consent, and use that data for an illegal purpose. The bill's sponsor plans to introduce additional RFID legislation.

By Claire Swedberg

March 27, 2008—Washington State Governor Christine Gregoire signed a bill into law Wednesday that will make "skimming"—the unauthorized reading of data stored on an RFID tag—for criminal purposes such as fraud, identity theft or stalking. The new legislation, which goes into effect July, 2008, is the first of its kind to be approved in the United States and makes violation of the law a Class C felony, with violators subject to five years in prison and a \$10,000 fine. (The California state legislature is considering its own anti-skimming bill, [SB 31](#), which would make it a crime to intentionally reading a person's RFID data without his or her knowledge or consent, regardless of intent, and would impose a sentence of up to one year of jail and a fine of \$1,500.)

The law prohibits, for example, a thief from using an RFID interrogator to captured RFID data from chips in someone's home to learn about the home's occupants and what they may have purchased. Another illegal scenario would be use RFID technology to stalk someone by means of the RFID chip embedded in that individual's driver's license or passport.

The Washington State law is a scaled-down version of [House Bill 1031](#) that would have also required that consumers "opt-in" to using RFID technology. In other words, retailers would be required to notify consumers and obtain signatures of approval to use RFID technology such as with a customer loyalty card that contains an RFID chip with an ID number that links to the consumer's information and spending habits. The bill approved by the House in February (see [Washington State House Gives Nod to Privacy Bill](#)) had included the following language: "If a governmental or business entity intends to collect, use, or retain the 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.... In obtaining consent, the governmental or business entity shall unambiguously disclose that, by consenting, that person agrees to have the governmental or business entity collect, use, or retain data gathered from the identification device." The state's senate, however, had removed those provisions, as well as others, prior to passing the bill earlier this month.

State Rep. Jeff Morris (D-Mount Vernon), who sponsored the bill, says he is pleased with the newly approved anti-skimming law, but intends to introduce new legislation at the beginning of the next session, in January 2009, that would again address the opt-in measure and could make it a crime to use RFID for marketing purposes without alerting and gaining consent from consumers.

By December 2008, Morris says he hopes to present three separate bills to the House for review in the 2009 session. The first would revisit the opt-in provision removed by the Senate this year. He says the opt-in

measure failed to pass through the Senate in 2008 because of heavy lobbying by the technology industry, as well as the fact that the Senate members—many of whom were unfamiliar with the technology—had only 60 days to review the bill.

The second bill will address labeling, requiring notification on labels when products have RFID chips, and the third will address deactivation issues which would require retailers to deactivate an RFID chip before the consumer leaves the facility. Both of those provisions had been included in a previous version of the bill considered but were later removed by the Assembly. When it comes to deactivation, Morris says, he will work with the RFID industry to discuss what technology can and cannot be readily deactivated in stores. Working with the industry, Morris says, has always been part of his strategy. "This is to protect both the consumers and the industry," he says. "My intent from the beginning has been that if you don't have rules of deployment up front, someone [using RFID] will do something stupid and there will be a backlash."

Dan Mullen, president of automatic-identification trade association [AIM Global](#), says he did not feel the legislation was necessary. Nonetheless, he was glad to see that the anti-skimming law is directed at criminal activity more than the RFID industry. When it comes to privacy issues, however, he says, "The question needs to be asked whether legislation is already there to protect consumers, and is there anything really unique about RFID to require further legislation."

RELATED\_ARTICLES Mullen does not agree with the need for an opt-in measure. "I don't think that's necessary at this point. We're looking at ways to use vendors' tools to create education and notification, and you'll see AIM Global doing more of that," he says. AIM Global has developed an RFID emblem that can be displayed near an RFID chip to help users locate the chip itself when attempting to capture a transmission with an RFID interrogator. He says his organization is now working to gain [International Standards Organization](#) (ISO) approval for a similar generic RFID emblem for the consumer market that could be used to alert consumers that an RFID chip is present. That emblem is being reviewed by an ISO technology committee, he says.

Morris argues that industry efforts to protect consumer rights are not enough and that there needs to be a law to ensure consumers privacy is protected both from those with criminal intent and those with a marketing agenda. "Industry says punish the criminal activity, not the technology. My question is, if you slip in a consumer chip without them knowing it, is that a crime, or not?"

Copyright ©2005 RFID Journal, Inc. All Rights Reserved