WASHINGTON POLICY CENTER
Improving lives through market solutions

LEGISLATIVE MEMO

Balancing Technology and Privacy in 2009

By Carl Gipson
Director, Center for Small Business, Technology and Telecommunications
January 2009

Radio Frequency Identification (RFID) tags, developed over twenty years ago, have become a well-used tool in many different industries. Acting as a next-generation bar code, an RFID system consists of a small microchip and an antenna placed on a product that sends information a short distance via radio waves. Similar to a bar code, the RFID chip holds inventory information related to the product to which it is attached. An RFID-tagged product can be easily tracked as it moves through the various stages of commerce; but the distance the information is transmitted varies from direct contact to no more than several feet, which helps control who gets access to the data on the tag.

Currently, RFID is rarely used to store any personal information—it is used primarily for tracking warehouse information like retail or medical supply inventories. While it is possible to store personal information on an RFID chip, outside of the health care industry (hospital patient information, etc.) it is very rare to find an example where any personal information is encapsulated onto RFID chips. But privacy concerns have led several states to introduce legislation dictating the type of information RFID chips may contain, or limiting how this relatively new technology may be used.

In Olympia, a series of bills have been introduced to alleviate the privacy concerns regarding the possible abuse of using of personal information in connection with RFID chips. They are House Bills 1006, 1011 and 1044.

Among what these bills would do includes:

- ☐ Regulate the use of identification devices;
- ☐ Require a written opt-in submission guideline for any government or business using an RFID chip that holds personal information (there are certain exceptions);
- ☐ Limitations on any business or government entity's usage of data stored on an RFID chip without the person's expressly written consent;
- ☐ Require any business or government entity to conspicuously label any device that contains an RFID chip that is not disabled upon sale or issuance of the good;
- ☐ Require the Information Services Board to develop state privacy and usage standards for RFID technology.

These bills are intended to ensure consumers are aware of how their personal data will be used by private businesses or government, in large part because abuses of this information can be catastrophic to a person's credit, finances, etc. In an age of growing identity theft, backers of this proposal fear an escalation of fraud through new technological means.

P.O. Box 3643, Seattle, WA 98124-3643 • PH 888-WPC-9272 • FX 206-624-8038 • www.washingtonpolicy.org

However, even though personal data is seldom stored on RFID chips, a myriad of privacy laws are already on the books in dealing with the collection and dissemination of that kind of information. Federal legislation already regulates the financial, health care and credit reporting industries. The Washington Privacy Act restricts the interception or recording of private communications or conversations. Other laws deal with identity theft, computer theft, and stalking or consumer credit card copying crimes.

One improvement in this year's bill (HB1011) is that the definition of "Radio Frequency Identification" is narrowed to specifically target only RFID-type technologies. Previously, privacy bills on RFID would have affected many other wireless devices, like cell phones.

Policymakers should focus on people who commit crimes of identity theft, rather than trying to micromanage the technology itself. Legitimate manufacturers and users of RFID technology agree that abusing consumers' private data, especially in a competitive marketplace, would be unethical and bad for business. Using the International Standards Organization, the RFID industry is already setting national and international standards for itself. On the domestic side, the FCC already regulates and certifies RFID devices. The penalties to a company for not complying with FCC regulations are quite severe.

According to a report by the Federal Trade Commission, many RFID businesses are voluntarily self-regulating themselves through EPCglobal – an industry standardization group for Electronic Product Codes. [1] Members of EPCglobal subject themselves to their adopted guidelines, which calls for consumer notice, choice, education and it instructs companies to implement effective security practices.[2]

The private sector is not the only entity tapping into this technology. In the summer of 2007, the Washington State Department of Licensing decided to deploy a technology trial of an RFID-enabled driver's license. One of the reasons behind this trial is to assess whether an RFID-enabled driver's license is a reasonable alternative to a passport for Washington drivers who cross the Canadian border regularly. The new license possesses a digital watermark and other authenticators. The RFID chip used in the license has a broadcast range of twenty feet and the licenses are available now, but they are completely voluntary.

RFID technology is also being used for the voluntary electronic tolling system on the new Tacoma Narrows Bridge, as well as the HOT lanes pilot project on SR 167.

Backers of this type of regulation are also advocating that consumers be provided with a preemptive "opt-in" right. This means that any business must gain the consumer's consent prior to selling any RFID-enabled products to them. But again, the predominant use of RFID tags is in the logistics of moving goods and supply chain management, not in selling to customers.

A public policy stance often used with a technology that may not be completely understood by policymakers is called the "precautionary principle." This principle states that if a certain technology or method is not fully understood by policymakers—or a sufficient consensus is not reached—the policy should be immediately discontinued until there is a sufficient consensus.

[1] http://www1.ftc.gov/os/2005/03/050308rfidrpt.pdf
[2] http://www.epcglobalinc.org/home

P.O. Box 3643, Seattle, WA 98124-3643 • PH 888-WPC-9272 • FX 206-624-8038 • www.washingtonpolicy.org

One of the problems with the precautionary principle in RFID technology is that no policymakers can account for how the technology will improve in the future. Computing power and technology components increase in efficiency exponentially every few years. Cutting today's technologies off at an early stage could short circuit efforts to improve privacy, while at the same time fulfilling the technological needs of the industries that rely upon RFID. Already there are many examples from around the world on how RFID-enabled products and services are enhancing customer service or saving consumers and businesses both time and money, as well as increasing security in other sectors of business (day care for instance). In fact, RFID today represents a $5.3 billion industry.

New technology can present challenges to businesses, governments and citizens because everyone must agree on standardization and protections to personal privacy. But reacting to legitimate privacy concerns through the cost-prohibitive regulation of a product harms the business community and consumers. The cure is not to prohibit, but to work with the private sector to develop a "best practices" approach to privacy concerns and to crack down on anyone who willfully misuses any personal consumer information. In fact, many companies and RFID makers are already doing this.

RFID tags are used to track products and inventory, not people. It is understandable to be hesitant about a technology many people outside the technology and retail sectors do not readily understand. But regulating a technology out of existence because of fears about privacy invasions hurts economic growth and business efficiencies.

RFID will probably end up being largely regulated on the national level, therefore, Washington state runs the risk of segmenting a bourgeoning industry by regulating differently from most other states. The new Obama administration has suggested that it will place technology and privacy concerns higher than the previous administration, so rushing into regulating differently than the federal government could very well discourage RFID use and development in this state.

Most businesses that collect data for the use of marketing or other legal purposes have a stated privacy policy. Consumers must also do their part in educating themselves about their rights in voluntarily disseminating their own personal information. As is the case with all technological advancements, responsible users of advanced technology have the capability to accomplish great things and improve the lives of consumers and society at large. There also exist those that wish to do harm to others.

Simply regulating a technology in the name of consumer protection does not guarantee that criminals will not try to break the law in the future. Establishing data protection standards—already being done by private standards organizations—and enforcing the current criminal laws will benefit consumers and businesses, while still providing the benefits from new technology.

Carl Gipson is director for small business and technology at Washington Policy Center. He can be reached at 206.937.9691 or cgipson@washingtonpolicy.org. Nothing in this document should be construed as any attempt to aid or hinder any legislation before any legislative body. For more information visit our website at www.washingtonpolicy.org.