12 of 45 DOCUMENTS



Law.com (Online)

November 9, 2004 Tuesday

**LENGTH:** 1163 words

**HEADLINE:** Tag Sale: Selling Out Your Privacy

**BYLINE:** Harry A. Valetk,letters to the editor@corp.law.com, Special to the special to law

**BODY:**

Today more than ever, people are concerned about how much personal information is available to companies both online and offline. E-ZPass toll plaza signals, monitored email, spyware and face-recognition systems are just a few examples.

But new tracking technology invisibly embedded in everyday products could soon take the current concern to a whole new level. Radio frequency identification (RFID) tracking technology uses electronic tags to automatically identify and track animals, goods and even, people.

RFID TECHNOLOGY IN ACTION

Farmers and pet owners currently use RFID tags to identify animals. Top Mexican officials use implantable RFID tags to access secure areas. Finland authorities developed RFID chips for travel cards, and the European Central Bank plans to use them on Euro banknotes in 2005. Dry cleaners and airline luggage systems may soon use RFID tags to benefit from its versatile, wireless tracking technology. Last month, the Food and Drug Administration approved RFID tags for implantable use in humans, and the State Department announced that in 2005 it will use RFID tags in passports.

To be sure, RFID technology has incalculable advantages. Unlike the familiar bar code, which requires manual

scanning of individual items, RFID inventory control systems can automatically log merchandise in bulk as it arrives at the loading dock. Tiny electronic product code (EPC) tags attached to individual items can be read by radio from distances of 20 to 30 feet.

By the same token, this revolutionary inventory management tool could introduce new privacy concerns for consumers. RFID tags are so small they can function without a consumer's knowledge or consent. They have the potential to gather unprecedented amounts of in-store product information that can be linked to a merchant's customer database, and later shared with third-party corporate partners.

Consumers advocates fear that merchants could associate this product data with any personal information taken at checkout. They could then use this information to target customers by name when they later appear within the vicinity of one of their stores wearing unobtrusively tagged merchandise, such as a sweater or watch. That information could prove invaluable in assessing personal consumer preferences and predicting individual consumer purchasing habits.

Absent any provision for disabling these tags, critics worry that RFID could expose consumers to unforeseen risks by allowing tech-savvy burglars to inventory victims' houses from a distance or adapt the technology to track victims through their RFID'd belongings that have RFID chips.

## SURVEY OF RFID PROPOSALS

Balancing these varying concerns, policy-makers are taking action. In fact, several states -- California, Utah, and Missouri among them -- have already proposed several bills to regulate RFID, but none have yet been passed.

Missouri's proposal would require that retailers who sell RFID-tagged products label those items conspicuously. Utah's bill goes one step further. It would not only require notice to consumers about the presence of RFID tags, but also it would require manufacturers and distributors to alert and teach retailers about how to kill the tags.

Still, California's bill is the most comprehensive. Merchants would have to get consumer consent before using RFID tags to track purchases, and all RFID tags must be deactivated before the consumer leaves the store. Additionally, under California's approach, it seems that consumers could not consent to the use of their information beyond those uses identified in the bill. Critics of California's approach argue that it's overprotective, because consumers are not given the discretion to choose to benefit from post-purchase conveniences like no-receipt returns.

## CHILDREN'S PRIVACY

Aside from these legislative proposals, existing privacy protection laws might also apply to any information collected, used or disclosed by merchants using RFID tags. For example, the Children' s Online Privacy Protection Act (COPPA) prohibits Web site operators from collecting or disclosing personal information from children 12 years and under without first getting verifiable parental consent.

COPPA defines the term "operator" as any person who operates a Web site located on the Internet that collects or maintains personal information about users or on whose behalf such information is collected. The term "Internet" is likewise broadly defined to include the myriad of computer and telecommunications facilities, including equipment and operating software, which make up the interconnected worldwide network of networks that use IP to communicate information of all kinds by wire or radio.

Depending on how RFID tracking systems evolve in the marketplace, COPPA could conceivably apply. A merchant using the telecommunications technology in RFID tags to collect in-store product information from a child, and then associating that product information with personal information, may find itself violating federal law, unless it first gets

parental consent.

WHAT LIES AHEAD?

It's still too early at this point to determine how RFID will evolve in the marketplace. The key for the business community is to identify the real privacy risks associated with RFID versus those risks perceived by consumers. Indeed, only by addressing the real privacy risks head-on will companies be able to maximize on RFID technology.

For now, attorneys could offer the following tips when counseling clients on how to implement RFID technology:

- Notice, notice, notice. Companies should inform consumers about any products containing RFID tags by clearly labeling those products. They should also have privacy statements disclosing all of the company's information practices. Most legal risks can be avoided if consumers receive adequate notice and choice. Full disclosure goes a long way in demystifying new technology.
- Deactivate at checkout. Consider the benefits of deactivating RFID tags at the point of sale. Keeping RFID functional after in-store purchase without a consumer's knowledge or consent could expose companies to creative liability claims and unwelcome scrutiny by advocacy groups and public officials.
- Ask the right questions. Companies should actively review how the information gathered by RFID tags in their products will be managed. Companies should ask how the information will be stored, accessed, protected and shared to fend off any potential privacy violation claims.
- Educate. Companies should educate consumers about RFID technology and provide them with choice on how information is collected through RFID tags.Harry A. Valetk is the Director of Privacy Online for ESRB in New York City. He is an adjunct assistant professor at the Bernard M. Baruch College, Zicklin School of Business, and a former trial attorney with the U.S. Department of Justice. The opinions expressed in this article author's, and are not necessarily those of ESRB. Email: (harry@valetk.com)

**LOAD-DATE:** March 9, 2012