

RFID, Electronic Eavesdropping and the Law

Existing laws in the United States could be amended to protect consumer privacy.

Feb. 14, 2005—As radio frequency identification enters the mainstream, consumer advocates are raising concerns about the potential use of the technology for electronic eavesdropping. In Europe, there are strong laws governing the use of data gathered on consumer. In the United States, no such overarching legislation exists. So the question is: What laws currently on the books, if any, in the United States could protect consumers against invasion of privacy using RFID systems? And what are the legal ramifications for companies that use the technology in a retail setting?.

RFID is a threat to privacy, according to consumer advocates, because RFID tags can be hidden inside objects without customer knowledge (see [RFID Position Statement of Consumer Privacy and Civil Liberties Organizations](#)). This would make it possible for someone to read an RFID tag for the lifetime of a product without the consumer even having knowledge of the tag's existence. Advocacy groups also voice a concern that the RFID readers, like the tags themselves, can be hidden from consumer sight.

Today, most products are identified by the Universal Product Code (UPC), but the UPC does not distinguish between like products. To a computer system scanning a UPC, for example, two DVDs sharing the same title are the same. With the advent of the Electronic Product Code (EPC), these same DVDs could be distinguished from one another and the individual item or product could be uniquely identified. Consumer groups worry that individual items can be registered via a global item system and linked to the purchaser of an item. They anticipate the creation of massive databases containing RFID tag data that can link tags and people and then be used for invasive marketing, according to the "RFID Position Statement of Consumer Privacy and Civil Liberties Organizations."

Similarly, consumer groups fear that the unique identifying data in an RFID tag could be used to track and profile individuals. By monitoring tagged items, the groups caution, the government could possibly track individuals more easily and corporations could further intrude on individuals' private lives. Consumer groups believe that RFID technology may potentially interfere with an individual's right to travel in relative anonymity.

Several states have already begun discussing legislation to protect consumers' rights (see [The Law of the Land](#)). In February 2004, the Utah House of Representatives approved a bill known as the [Radio Frequency Identification—Right to Know Act \(H.B. 251\)](#), but the Utah State Senate failed to vote on it the following month. Similar legislation was introduced in California and passed by the state's senate (see [Bowen Seeks Balance in RFID Law](#)), but the state assembly failed to pass the legislation (see [California RFID Legislation Rejected](#)).

Federal Statutes

The federal Electronic Communication Privacy Act (ECPA) can be and probably will be amended to cover some of the privacy concerns mentioned above. Title III/ECPA already outlaws wiretapping and other forms of electronic eavesdropping, possession of wiretapping or electronic eavesdropping equipment, and use or disclosure of information obtained through illegal wiretapping or electronic eavesdropping. Further,

information secured through court-ordered wiretapping or electronic eavesdropping cannot be disclosed to obstruct justice, according to a report entitled *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, written by Gina Stevens and Charles Doyle, and published by the Library of Congress's Congressional Research Service (see [Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping](#)). In essence, this act prohibits any person from intentionally intercepting, or endeavoring to intercept wire, oral or electronic communications by using an electronic, mechanical or other device unless the conduct is specifically authorized or expressly not covered.

Although wiretapping is not identical to RFID, it shares an abundance of similarities that may carry over to RFID technology. The capturing of wire, oral or electronic communications will be in violation of the ECPA only if "the conversation or other form of communication intercepted is among those kinds which the statute protects, in oversimplified terms--telephone (wire), face to face (oral) and computer (electronic)," Stevens and Doyle wrote. In this case, RFID technology will likely fall under the electronic category.

The Wiretap Act (Title 18, section 2701, of the U.S. Code) sets the stage for accessing information and the ramifications of doing so. It defines what constitutes a criminal act (e.g., intentional access to electronic communication without authorization) and stipulates punishment by imprisonment or fine. In some instances, for an act to be deemed criminal, a person performing that act must demonstrate both intent and action. *Mens rea*, or "guilty mind," is critical in such a case. Obtaining the information is not in itself a crime; intention plays a major part in defining this type of crime.

Typically, to prosecute someone for obtaining information, there would have to be an overwhelming amount of proof that the person's intentions for obtaining this information were to commit a crime. It would seem that cases and legislation dealing with Internet and personal computer issues would be related to RFID technology via analogy.

The Wiretap Act presents an overview of the possible legalities that may be applicable to RFID technology. The Wiretap Act indicates that anyone who intercepts electronic communication will be held in violation of the statute if proper consent has not been obtained. As RFID technology will be classified as electronic communication, it is reasonable to assume that it, too, cannot be employed to obtain and use information legally unless consent is given. The statute refers specifically to wiretapping. RFID is incredibly similar in its use, however, in that those persons using a wiretap or RFID technology are trying to gather information.

RFID technology and its implementation must be guided by strong principles of fair information practices, so wrote the organizations endorsing "RFID Position Statement of Consumer Privacy and Civil Liberties Organizations." Privacy guidelines published by the [Organization for Economic Co-operation and Development](#) (OECD) offers some useful guidelines related to the disclosure of RFID technology use and the purpose behind its use. Once businesses equip products and goods of any kind with RFID tags, businesses will have a duty to disclose the use of this technology to their customers.

RFID users must make public their policies and practices involving the use and maintenance of RFID systems, and there should be no secret databases. Individuals have a right to know when products or items in the retail environment contain RFID tags or readers. They also have the right to know the technical specifications of those devices. Labeling must be clearly displayed and easily understood. Any tag reading that occurs in the retail environment must be transparent to all parties. There should be no tag-reading in secret, urge the organizations endorsing the "RFID Position Statement." Additionally, these organizations say that users of this technology should make public the purpose for which the readers and tags are being used .

Contracts

Just as citizens and organizations can consent to the use of wiretapping and electronic eavesdropping, so they can consent to the use of RFID technology. In the case of RFID, the consent is apt to be considered a contract

between the consumer and the business. One can anticipate both express and implied contracts. (“A contract is express if its terms are stated by the parties, either orally or in writing,” according to *American Jurisprudence, Second Edition*). “An implied contract is one in which some or all of the terms are inferred from the conduct of the parties and the circumstances of the case, though not expressed in words.”)

Customers and patrons of retailers that use RFID will have to be made aware of the fact that the products sold in that store are being electronically tracked. This will, in turn, necessitate that the retailer attains consent from patrons. The consent can be obtained through written agreement that gives rise to an express contract. In such a case, the patron will likely have to sign or orally consent to the use of RFID tags. This consent may be just implied, however. If so, it will give rise to an implied contract. Such a contract would likely arise from the fact that the retailer had disclosed the RFID technologies used in the store, and a contract would automatically be agreed upon by the patrons shopping in that store.

Principles of Fair Information Practice

RFID technology not only has the ability to track products and persons, it also has the ability to collect individual information. As such, the Federal Trade Commission’s Fair Information Practice Principles would seem to play a role in the legalities of RFID.

In its Fair Information Practice Principles, the FTC writes about the collection and use of personal information and addresses “the safeguards required to assure those practices are fair and provide adequate privacy protection.” Government agencies in the past quarter century have deliberated about the way in which entities gather and use personal information. A succession of reports and guidelines have identified five central principles of privacy protection:

1. Notice and awareness of collection of information.
2. Choice and consent of how this information can be used.
3. Access to the individual’s gathered information and the ability to contest the accuracy of the collected data.
4. Integrity and security of the collected data.
5. Enforcement of the aforementioned principles.

Because RFID technology can be used as a marketing tool, a tracking device and a way to collect personal information, these Fair Information Practice Principles will play an active role in addressing some of the vital concerns that have arisen with the evolving RFID technology.

Searches, Seizures and Law Enforcement Uses

RFID may be an effective tool in criminal investigations. It is conceivable, for example, that an RFID chip could be used to identify the original purchaser of an item found at a crime scene, as noted in an article entitled “Inventory Tracking Chips Raise Privacy Concerns” that appeared in the April 7 edition of the *Winnipeg Free Press*. The technology could also be used to identify someone in a crowd, the article observed. Crime-scene investigators might find RFID useful for keeping track of the evidence collected from crime scenes. Finally, RFID technology would be useful in deterring shoplifting and other theft. While this technology appears promising, however, it is not foolproof. Evidence from an RFID sensor would be hard to refute, but malfunctions can happen in any technology.

Conclusions

As RFID technology rapidly becomes a mainstream part of the retail industry, it may well revolutionize production and operations management throughout the world. The technology, however, comes with risk. The risk is it could be used to invade consumer privacy. People may be monitored unknowingly by businesses or the government, and personal liberties jeopardized. To protect consumer privacy rights, advocacy groups are banding together to stipulate fair and forthright use of this new technology. States are trying to regulate the RFID industry by drafting legislation that is in keeping with the demands of the consumer advocacy groups.

RFID technology fast approaches the massive implementation phase in a number of industry sectors, and the legal issues that come to life with the uses of it are vast. The definition of privacy will eventually define technological crimes. While RFID technology will likely enable the creation of new crimes by thieves, blackmailers and stalkers, it will also enable new methods of crime prevention and investigation. Although the law is always inevitably a few steps behind technology, it always catches up. In time, laws will closely guide both manufacturers and users of RFID technology.

Dr. Reuven R. Levary is a Professor of Decision Sciences, Cook school of Business, Saint Louis University, St. Louis MO 63108. David Thompson, Kristen Kot and Julie Brothers are completing a joint JD/MBA degrees at Saint Louis University. To comment on this article, click on the link below.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved