

RFID and Privacy: Finding the Right Balance

By Julie S. England



Radio Frequency Identification (RFID) is a technology that wirelessly connects people or objects with the automated systems used everyday. RFID might unlock a door for an employee, tell a person where a package is located or confirm that the medicine just purchased at the pharmacy is authentic. It also helps move traffic more efficiency through highway toll plazas, subway systems and even on ski slopes.

As new technologies, like RFID, become commonplace in the supply chain, for example, people sometimes have a tendency to hypothesize “what if” scenarios that can stretch the limits of science and practical application. Perceived breaches of privacy must be addressed by the industry: providers of the technology, retailers implementing the technology, and government bodies. For RFID to become generally accepted, misconceptions about what the technology can and cannot do must be corrected.

The responsibilities of the industry are to protect the privacy of our customers and individuals, and to make this world a better place with RFID. The key to success is finding the right balance. It is the responsibility of manufacturers, retailers and other vendors to continue to work with customers, industry partners and governments to create the technological and regulatory structures that will protect confidentiality and individual choice.

Industry associations are dedicated to ensuring full compliance with all relevant personal privacy and security regulations. The industry is well aware of concerns regarding privacy and security which is why industry members are working to address these concerns where RFID technology-based solutions are appropriate. AIM Global believes that policies and procedures should be put into place, namely:

- The right to know whether products contain RFID tags.
- The right to have RFID tags removed or deactivated when they purchase products.
- The right to opt out of RFID-enabled services.
- The right to access an RFID tag’s stored data.
- The right to know when, where and why the tags are being read.

EPCglobal has also recognized the concerns of individuals with regard to their privacy and has addressed this with Generation 2 specifications where “tag kill” and “password protect” features are included in the specifications. Using the “tag kill” feature, data that is programmed onto the tag at the manufacturer can be decommissioned with passwords at the retail location. With the password protection write feature, a pharmaceutical dispenser or retailer can decommission the National Drug Code (NDC) by overwriting it so it is zeroed out prior to check-out. When the NDC is decommissioned, consumer privacy is protected because no identifying product code is on the

tag. However, the unique ID and EPC serial number of the product can remain on the tag in the event of a product recall.

The RFID industry understands that if consumers do not trust or find value in a new technology it will not be adopted. E-tailing is a great example. While online retail was part of the early vision of the Internet, it took several years for consumers to become comfortable with online purchasing. Only after the industry created privacy policies, put information and financial safeguards in place, and empowered consumers to control the process, did transactions on the Internet become commonplace.

When consumers understand a technology and trust the companies providing these new services, the adoption curve is steep. Core to this trust is the empowerment of consumers to control, restrict, access and change the information that drives these applications.

As the market moves toward wide-scale adoption of RFID, the industry needs to respond with information, safeguards and empowerment. The industry should listen to and understand what consumers want and need, and more importantly, what they don't want. Technology can respond with the right protections and safeguards, and processes can create secure and safe environments for these transactions.

Julie England is a vice president of Texas Instruments and the general manager of Texas Instruments RFid Systems. In this capacity, she is responsible for shaping the overall strategy for and directing TI's RFID business, which is the world's largest integrated manufacturer of wireless identification transponders. TI is investing in a range of RFID products including retail supply chain, pharmaceutical, contactless payment and electronic identification programs. The most secure RFID products produced by TI have security and encryption features. The encryption is sanctioned by the NSA and includes 128-bit encryption to meet the stringent requirements for contactless payment applications and government ID programs. In addition TI RFID is investing in next-generation technology to stay one step ahead of the market and the privacy and security needs of customers.

Julie S. England, Vice President and General Manager, Texas Instruments RFid Systems™