Where the RFID Industry Has Failed

Anyone reading my blog recently knows that I’m frustrated by some of what is being written and said about radio frequency identification. While I believe reporters and researchers have a duty to get their facts straight, the reality is that the RFID industry can’t depend on that happening. It’s up to the

industry to educate people if it wants the technology to be more widely adopted. Here are the key falsehoods that I believe need to be addressed.

All RFID is the same. Potential end users, journalists and others do not understand that there are vast differences in the performance and uses of passive high-frequency (HF) tags, passive ultrahigh-frequency (UHF) tags and the many types of active RFID tags. During an interview with a journalist, I was asked about implantable tags. I said they were passive LF tags that had a read range of approximately a foot, so they could not be used for tracking. His response: "Yes, but I've heard there are new active tags that have a read range of 300 feet or more." I then had to explain that you could not implant an active tag with a battery in a human being.

I've seen many articles on privacy that confuse the secure, short-range HF tags used in passports and the longer-range UHF tags (which do not yet support security features) utilized in PASS cards. Most people equate RFID with passive UHF technology, because that was what got a lot of media attention when Wal-Mart Stores announced plans to use it (see Wal-Mart Relaunches EPC RFID Effort, Starting With Men's Jeans and Basics).

RFID is invisible. One of the things that worries people most about RFID is the idea that governments and/or corporations will embed transponders in documents, clothing and other items, and then track individuals without their knowledge. Opponents of the technology often say the tags can be hidden.

Yes, tags *can* be hidden—but that does not mean *RFID* can be hidden. That's because RFID readers emit energy to power up passive tags so that they can respond with their serial number.

Let's say, for example, that a corporation embeds tags in shoes in an effort to identify and track customers in its retail stores via reader antennas in the floor. Any suspicious hacker or journalist could use a reader bought online to show energy is being emitted from the floor at the precise UHF frequencies used by RFID systems. They could also detect hidden tags in clothing by pointing the reader at their closet. A retailer caught using RFID without informing customers would face an enormous PR nightmare. (I would like to point out that cameras can be hidden behind mirrors, and there is no way to detect those.)

Reading a tag is equivalent to infringing privacy. In almost all cases, you can not identify a person by reading an RFID tag. That's because tags only carry serial numbers linked to identities in secure databases. I can think of two exceptions. Some older RFID-enabled credit cards have the person's name and credit card number stored on the transponder—but that's the same information on a credit card that you hand over to a worker at a store or restaurant. The tag in a passport does contain some personal information, but in response to security concerns, many passports now have a foil liner to prevent someone from skimming this information.
In all other cases, you need to use some other method to identify a person and then associate a tag ID in something he or she carries, in order to track that individual. Yet, the misunderstanding that reading a tag is equivalent to infringing privacy—often combined with "all RFID is the same"—persists, and is a favorite target of hackers, bloggers and some academics. (It's also one of the reasons I've felt so frustrated lately.) For a taste of how this myth is spread, see A Privacy Expert's Misguided View of RFID, Academic Navel

Gazing Continues and PBS NewsHour Misinforms Viewers on RFID.

Many products have embedded RFID tags. I've read numerous articles that assume a lot of goods have embedded tags, or that quote so-called experts making this claim. In the *PBS NewsHour* piece on cybersecurity that I took issue with, for example, hacker Chris Paget said on camera, "You can find out all kinds of information about them from these RFID tags that are being issued to you by the government, by stores, and products you buy all over the place."

The problem with that notion is that almost no products currently have RFID tags embedded in them. And the few items that consumers might purchase with tags have them in hangtags or labels designed to be cut off, or in packaging that is thrown away. What's more, goods sold at Walmart that have RFID tags in their hangtags, labels or exterior packaging will carry the EPCglobal seal, indicating the presence of an RFID tag.

RFID opponents worry that criminals, overzealous government officials or nefarious businesspeople could sit in a parking lot and read tags on labels and packaging as consumers leave a store, or that they could scan an individual's garbage cans. This strikes me as very unlikely. All the perpetrators would obtain is a serial number—and even if criminals knew enough to figure out which product those numbers represented, it would be of little value to them. Criminals target people and homes that are vulnerable, not those with the nicest merchandise.

As I wrote in last week's Editor's Note (see Irresponsible Reporting on RFID), there are legitimate reasons to raise privacy concerns. But to solve any and all privacy issues so that governments, businesspeople and consumers can benefit from RFID technology, we need to have an ongoing intelligent discussion.

My advice to providers of RFID hardware, software and

services—and to companies using the technology now—is to raise these issues every chance you get. Raise them every time you are interviewed by the press, and whenever you speak at an event. These myths are not easily dispelled. We need to keep repeating the facts until people understand them.

Mark Roberti is the founder and editor of RFID Journal. *If you would like to comment on this article, click on the link below. To read more of Mark's opinions, visit the RFID Journal Blog or the Editor's Note archive.*