

The Privacy Nightmare

Only an aggressive PR campaign and an enforceable code of ethics will get people to accept self-regulate of RFID tracking of consumer products.

Aug. 12, 2002 - My wife and I recently went to see *Minority Report*, Steven Spielberg's new film starring Tom Cruise. For those who haven't seen it, the movie takes place in Washington in 2054. John Anderton, the character played by Cruise, is on the run because three "precogs" have predicted he will commit murder. Washington has all but wiped out homicide by prosecuting crimes that the precogs say will be committed.

My reason for writing about the movie is a scene in which Cruise's character ducks into a shopping mall to escape his pursuers. In this futuristic world, retinal scans are used to identify people. Advertisements in the malls quickly scan people's eyes and then deliver customized messages. Cruise is bombarded with pitches, such as: "You're looking tired Mr. Anderton. You need a vacation."

The scene is meant to be a satirical commentary on where our advertising culture is going. For me, it drove home the level of cynicism that proponents of ubiquitous, low-cost RFID will have to overcome. I used to think that the public would accept self-regulation of RFID privacy policies. Lately, I've begun to wonder.

A couple of things have changed in ways that are going to make it tougher to convince the public that their privacy will be protected. In the U.S. at least, the mood has shifted from anti-government to anti-business. Distrust of companies is high. The failure of the Internet industry to adequately self-regulate on privacy has made privacy advocates believe that self-regulation is another way of saying no regulation.

And I think most people understand in their gut that putting chips in things is infinitely more invasive than the Internet. Just look at the opposition in many countries to a national ID card that stores information on a chip. And frankly, Stephen Spielberg's vision of the future is benign compared to some horror stories that scaremongers will dream up about RFID.

What can be done? Three things. First, and most obvious, the industry needs to come up with a sensible opt-in policy – that is, companies agree that they won't track consumers' purchases unless those consumers expressly agree to it through some kind of loyalty program. I know the Auto-ID Center has been working on the privacy issue and its leaders are aware of how important it is to get consumers to accept this technology. I expect they will come up with sound proposals along these lines sometime next year.

Second, I think the industry needs to begin a loosely coordinated PR campaign as soon as a set of proposals is drafted. In politics, you always try to define your opponent in the public's mind before he has a chance to define himself. The same principle applies here. The public needs to be convinced RFID is good before scaremongers convince them it is bad.

That can be done by getting stories in the media about how RFID can reduce crime. I would love to see the Auto-ID Center run a pilot with a police department to show hard evidence of how RFID could reduce theft and facilitate the recovery of pilfered items. Even if that isn't feasible, the U.K.'s "Chipping of Goods" initiative will produce results that companies can point to.

The U.S. government has already undertaken a few pilots to show how RFID can be used to secure containers coming into ports. The success of these pilots needs to be trumpeted in the press. In this week's feature, [RFID Sensors: From Battlefield Intelligence To Consumer Protection](#), we show how smart sensors might be used in the not-too-distant future to protect the public from everything from anthrax to e. coli in meat.

Ideally, such articles would begin appearing soon. That's because no one knows precisely when scaremongers will begin dreaming up crazy stories about the government tracking your every move. And there needs to be a steady drumbeat of stories to influence public opinion – example after example of how RFID can benefit consumers.

Even if a positive image of RFID is created, it may not be enough to overcome negative articles that appear later. The way to do that, in my view, is to make self-regulation enforceable. If the electronic product code is adopted, companies will need to license technology developed by the Auto-ID Center to use it. I propose that companies be required to agree to adhere to a privacy code as a condition of receiving the license. And if they do not adhere to the code, their license to use certain portions of the technology should be revoked temporarily.

I know that no administrative body wants to get into policing. But I believe it can be done fairly easily. The EPC licensing body could set up a small department to investigate complaints by consumers. When a company is found to have violated the code, it gets a warning. If it violates the code a second time, its ability to issue new EPC codes is revoked for, say, one month. Each additional infringement is punished with longer revocation periods.

It may be difficult to devise a system that punishes those who do not adhere to a privacy code without hurting the violator's business partners, but I think it can be done, both technologically and administratively. Such a policy will show everyone that companies are very serious about respecting the privacy of their customers. It won't stop the scaremongers, of course. But it can help to inoculate the public against the spread of fear.

Mark Roberti is the Editor of RFID Journal. If you would like to comment on this article or submit your own, send e-mail to mroberti@rfidjournal.com.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved