

# One Problem, Many Solutions

There are many ways to prevent people from using RFID to infringe on people's privacy—and some products are hitting the market even before most consumer items have tags.

By Mark Roberti

June 26, 2006—If you listen to opponents of radio frequency identification, their arguments are built on two suppositions: First, they argue that big corporations have all the power, and that consumers won't be able to prevent companies from spying on them through RFID tags in the things they buy. Second, they suggest there is no way to prevent surreptitious reading, or skimming, of RFID tags; a corollary to this is that the technology will improve to the point where you can track anyone, anywhere.

Both of these suppositions are wrong.

The first supposition plays on people's sense of powerlessness, assuming the business community is a unified bloc that acts in concert, whereas in reality, businesses are in constant competition and operate quite separately of each other. Moreover, in a capitalist system, customers have all the power, because they can choose not to shop at a retailer infringing on their privacy.

There will always be companies willing to appeal to a competitor's disaffected customers. I've said in the past that it is the capitalist system itself that will protect consumers from potential abuses of RFID technology (see [Faith in the System](#) and [Faith in the System, Part II](#)).

The second supposition—skimming—will also be solved by the capitalist system. It might be true that some unscrupulous individuals will find a way to abuse RFID technology's capabilities, but it's always seemed patently obvious to me that others will see opportunities to profit by offering products that *protect* people's privacy.

My faith in the system is not misplaced. A number of companies and individuals are already introducing products that could help consumers protect themselves from the possibility that RFID will be used to invade their privacy. [IBM](#), for instance, has come up with a "clipped tag" that continues to operate after an item is purchased, but at a greatly reduced read range (see [IBM Proposes Privacy-Protecting Tag](#)).

[RSA Security](#), a leading provider of digital security products, has developed a "blocker tag" that will prevent RFID tags in the same reader field from being read. The tags are not yet in production, but RSA says they can protect privacy while providing consumers and businesses the benefits of RFID tags. A blocker tag would essentially confuse an interrogator, preventing it from reading any tags in its zone (see [RSA Security Designs RFID Blocker](#)).

Two students turned an ordinary point-and-shoot camera into a device that destroys RFID tags by overloading their circuits with a pulse of electromagnetic energy. The German privacy advocacy group [FoeBuD](#) plans to manufacture and sell the device—the RFID-Zapper—to concerned consumers (see [RFID-Zapper Shoots to Kill](#)).

In last week's column, ([A Moratorium on Stupidity](#)), I mentioned [Skim Black](#), a credit-card-sized piece of material that its manufacturer, Japan's [Orient Instrument Computer](#), says will block 99.99 percent of electromagnetic radiation. Skim Black can be placed in your wallet and will prevent a tag in an ID from being read.

The most attractive security solution to hit the market so far, in my view, comes from the Danish Company [RFIDsec](#). This solution gives control of a tag to the consumer, who would essentially have to give someone permission to read the tag for after-sales support, returns or other business applications (see [RFIDsec Unveils Privacy-Protected Tags](#)). Consumers would own a digital key allowing them access information on the tag, so they could use the tags in products they buy for their own benefit. I've said all along that as the technology matures, consumers will eventually have control over how tags in the products they buy are used, and this is exactly what the RFIDsec solution attempts to do.

Opponents of RFID will do their best to argue against each of these solutions—and, in truth, they might have some legitimate issues. One is that most put the burden on consumers to protect themselves. But the point is not that one or all of these is the right solution. It's that even with RFID still in its infancy—very few items consumers buy today have tags in them—products are being developed to address the privacy issue.

There will be many more products introduced to ensure consumer privacy as the technology matures. That's why I don't worry that the privacy issue will be a big impediment to adoption.

*Mark Roberti is the founder and editor of RFID Journal. If you would like to comment on this article, click on the link below.*

Copyright ©2005 RFID Journal, Inc. All Rights Reserved