

Spychips Book Fails to Make Its Case

The anti-RFID book by the leaders of CASPIAN doesn't provide any compelling evidence that the technology is a threat to privacy.

By Mark Roberti

Oct. 24, 2005—The new book *Spychips: How Major Corporations and Government Plan to Track Your Every Move With RFID* is meant to be both an exposé and a clarion call to the masses to stand up and oppose all uses of radio frequency identification. While it may reinforce the beliefs of those who think big business and big government are out to control their lives, the book fails to deliver on the publisher's claim that it will show "how this seemingly innocuous commercial maneuver will inevitably turn our society into a Big Brother nightmare." In fact, anyone drawing conclusions from the hard evidence presented in the book—as opposed to the theoretical propositions put forth by the authors—will conclude that RFID is *not* a threat to privacy.

This is a long opinion piece, because many of the authors' claims go to the heart of the privacy issue and, therefore, deserve to be examined in depth. For those of you who want to skip the details and just get the bottom line, here it is: The book does not include one single concrete example of someone whose privacy was invaded because of RFID. That's right. Not *one*. Even with the proliferation of RFID tags in access control cards, car keys and toll collection systems, the authors could not cite one instance where RFID tags tied to personally identifiable information was used to infringe on someone's privacy. (The authors do tell the story of a woman whose estranged husband subpoenaed her electronic toll records during a custody case to prove she was working late and not attending to their children, but the referenced article does not say whether the records were turned over.)

The book is written by Katherine Albrecht, founder of Consumers Against Supermarket Invasion and Numbering (CASPIAN), and Liz McIntyre, CASPIAN's communication director, two leading opponents of RFID. The authors rehash a lot of old, discredited material, such as the smart-shelf pilot Procter & Gamble (P&G) ran with Wal-Mart. I've already shown how no one's privacy was invaded in that pilot (see The Real Scandal). What is new is their reporting on RFID patents filed by P&G and other companies, including Accenture, IBM, Kimberly-Clark and NCR, which involve identifying people with RFID or attempting to understand consumer buying habits.

What these patents show is that many companies would like to use RFID to better understand their customers, or to identify them so they can serve them in a more personal way. That's hardly a revelation. Companies want to use almost any new technology to better understand their customers, so they can offer the things people want to buy and—sin of sins!—make more money. The authors assume that because companies *want* to use RFID to know more about you, they *can* and *will* know more about you. But they utterly fail to make this case.

There are three problems with the book. First, the authors either don't understand how RFID and related technologies work, or they simply hide the reality from in order to scare them. Second, the book almost always fails to draw conclusions from history or the real world. And third, when it does look at history, it completely misreads it. Let me take these one at a time on the following pages.

Misrepresenting the Technology

If you this book and don't know any better, you are led to think that all RFID tags will be read and associated with an individual and that information will immediately be uploaded to a giant database in the sky, accessible to anyone. "Once all the billions of items on the planet contain [RFID transponders], theoretically, the whereabouts of everything and everyone will be known at all times and accessible to anyone with access to the databases, authorized or otherwise."

Theoretically, lots of things are possible, but in the *real* world, companies don't share information about their customers with other companies. Do the authors really believe Philips will make data available on its customers so Sony can do a Google search and learn everything it needs to know to steal those customers away?

The authors also lead the to believe that every time an RFID tag is read, that automatically constitutes an invasion of your privacy, even if you are completely anonymous. For instance, the authors present a patent application filed by NCR in which a smart shelf could track when a customer picks up a can of corn and either puts it back on the shelf or puts it in their shopping cart. This tracking could be done completely anonymously and still be of tremendous benefit to manufacturers. For instance, a manufacturer could learn that of 1,000 anonymous people who picked up its product and put it down, 78 percent subsequently picked up a lower-cost alternative.

The authors find it outrageous that an RFID interrogator in a shopping cart could detect that a customer (who could be completely anonymous) put a high-end brand of pasta in their cart, and that the interrogator could then send a message to a computer screen mounted on the cart recommending a high-end brand of tomato sauce. This might annoy some customers, but it's no different from a salesperson in a clothing store suggesting you try on a pair of Prada shoes based on the fact that you have been looking at Armani suits.

Sometimes, the discussion of potential abuses is downright silly, because of the authors' failure to think through how RFID systems work. For instance, in a chapter on the potential uses of RFID by stalkers and perverts, the authors mention that one problem modern-day peeping Toms have is that when they install cameras in a female shower stall or under the desk of a female colleague, the cameras use a lot of energy and the batteries die quickly. They suggest RFID could be used to conserve battery power—that the camera would turn on only when an RFID tag in a garment worn by the stalking target was detected by an interrogator.

But there are a couple of problems with this RFID-enabled peeping Tom system. First, it assumes people will agree to wear garments with functioning RFID tags in them, which is by no means a given. More important, a battery in the RFID interrogator would run out just as fast as a battery in a camera because it would have to emit radio waves constantly to detect a tag entering its field.

Ignoring History

The authors are very good at providing footnotes, which are meant to give the book the credibility of a well-researched tome. But the authors often ignore historical facts. For instance, more than 100,000 patents are granted in the United States alone each year, and it's widely known that the vast majority of these never become products. Several years ago, *RFID Journal* wrote about a company using RFID to track shopping carts around stores to measure customer flow. I'm not aware if any retailer deployed it, or if the vendor that created it is even in business, but the authors present their patent information as though these ideas will certainly be implemented in a couple of years and consumers won't be able to do anything except passively submit to being tracked.

It's ironic that when the authors do present examples from history, they invariably show RFID will not be a threat to privacy. For instance, they explain that RFID could be used to identify you, track your purchase

history and then adjust prices based on your ability to pay. The authors then explain that Amazon.com tried personalized pricing and had to stop the practice when consumers objected. So on one hand, the authors claim powerful corporations are going to force this technology on you, then on the other present *solid evidence* that powerful companies will back off on attempts to personalize pricing the moment consumers object.

It's fair to say that almost the entire book is based on the premise that evil corporations will force customers to wear clothing and carry objects that contain functioning RFID transponders so that these transponders can identify and track customers. The problem is, at the same time, the authors themselves present *evidence* that this is unlikely to happen. They rightly point out, for instance, that when a technology company announced it would sell Benetton RFID tags that Benetton planned to use in its Sisley line of clothing, CASPIAN opposed the move and Benetton dropped the plans.

The authors also conveniently ignore the fact that Marks & Spencer (M&S), the one retailer currently tagging clothing items, is putting the RFID tag on the price tag so that it will be cut off before being worn. And since the tag only contains a random number, scanning someone's garbage would not provide any information about the person who bought the garment. M&S has handled the privacy issue well (see Precedents Set). At RFID Journal LIVE! Europe, James Stafford, the head of M&S's RFID efforts, said he couldn't swear his company would *never* use RFID at the point of sale, but that he could see no advantages to outfitting cash registers with RFID interrogators.

The authors present research findings done several years ago by the Auto-ID Center, which they say showed that 75 percent of the public opposed the idea of putting RFID tags in clothes. In other words, readers are asked to believe that the companies derided throughout the book for wanting to sell you more of what you want to buy will suddenly put RFID transponders in products, even though 75 percent of the population might stop buying their products as a result.

This, of course, doesn't make any sense whatsoever from a business—or common sense—standpoint. However, the authors' penchant for ignoring evidence pales when compared to their pattern of misreading history, which they then use to suggest RFID will lead to totalitarianism.

Misreading History

Toward the end, the book switches from discussing the use of RFID for marketing to more sinister abuses, such as stalking women (discussed above) and utilizing the technology to figure out whom to rob (seems to me that thieves have been doing just fine without RFID for many years now). Then, we come to the "Nightmare Scenario," in which governments take advantage of all the tags in clothing items to track and control people.

The authors could look at the world today and see that North Korea, the most technologically backward society on earth, is the most totalitarian, and that the most technologically advanced countries are the freest. They could also examine history and see that neither the Soviet Union, the People's Republic of China nor Nazi Germany used technology to control people. Such observations might lead them to conclude correctly that RFID will not inevitably lead to totalitarianism.

Alas, history is no guide for these authors: "When the low-tech world goes bad," they write, "as it did in Nazi Germany, it's a nightmare, but when the RFID world goes bad, the nightmare could permeate every aspect of its victims' lives, making camouflage and escape all but impossible. RFID could fulfill dictators' wildest evil dreams, providing near total omniscience and control over every aspect of society. When RFID goes bad, it will be unlike anything we've seen before."

Sounds pretty scary, especially the certitude that things will go bad in the future if we adopt RFID. Too bad their premise is based on shallow thinking.

The authors point out that during World War II, some Jews removed the Star of David they were forced to wear and disguised themselves as non-Jewish Germans to survive. With RFID, they claim, no such ruse would be possible to escape a dictator because Big Brother would use RFID tags in your clothes, and maybe even embedded in your body, to identify you and track you. So even though it's easy to destroy RFID tags, remove them from under the skin, detect and jam readers, destroy data with computer viruses and so on, the reader is led to believe that *no one* in the future would be able to figure out how to do such things.

Moreover, the authors fail to understand that totalitarianism is not about tracking people and never has been. It's all about intimidation and control of information, both internal and external. During World War II, Germans had no means of getting news of Hitler's atrocities to the outside world. Dictators—such as Stalin in the Soviet Union and Mao during the Chinese Cultural Revolution—have always depended on complete control of information and secrecy, by and large, from the outside world. With the Internet, satellite TV, cell phones and other ubiquitous forms of communication in advanced society, however, such secrecy is no longer possible. If dictators tried to take over a democratic country, opponents would have the means to respond in ways unlike anything dictators have seen before. In other words, technology will save us, not enslave us.

In fact, CASPIAN's success in raising awareness about RFID and getting big companies to back down from plans to tag clothes is evidence that information technologies can be used to spread the word about potential abuses of RFID and, on a small scale in this case, organize people to oppose something.

So now imagine a world where RFID is ubiquitous and people are forced to have functioning tags in their clothes. Retailers have deployed interrogators to gather data on their customers or better serve them (depending on how you view things). But a dictator overthrows a democratic government and decides to use RFID to track people and squelch opposition. How does he do that? Does he seize all the databases so he knows the ID tags in his political opponents' clothes? That would be damaging to the companies, so they might not be too supportive of this dictator, but what about all the people in those companies with the lock codes? They could publish those on the Internet, and people could change the numbers in the tags, rendering the databases useless. A very simple process, actually.

The authors claim a dictator could mandate that tags not be killed, so perhaps the dictator could mandate that tags not be rewritten. But the point they miss is that digital information is nearly impossible to control, no matter how powerful you are. You only have to look at how hackers are able to do so much damage to corporate networks despite the billions spent to stop them, or how music companies and movie studios are struggling—and largely losing the battle—to prevent the sharing of songs and movies over the Internet. The only way to control the flow of information would be to shut down the Internet. But if you did that, then RFID readers couldn't be used to track anyone. You'd wind up with just a bunch of boxes going 'beep' as a leader of the opposition walked by. What use would that be to anyone?

Still, the book *does* expose a threat to consumers, and it's not what you might think.

The Real Threat to Consumers

One great irony of this book is that the authors don't seem to understand that it is their desire to dictate the future—they want people to reject the use of RFID for all consumer applications—that represents a threat to consumers. Why? Because in their haste to destroy RFID technology, they also destroy the possibility that consumers could use RFID to get information about their government or companies that break the law.

Isn't it possible that two well-meaning authors could do more harm than good to the consumers they want to protect? Consider this Orwellian twist. Let's say two authors had decided in 1995 that the Internet represented a threat to privacy because it would enable governments and corporations to pry into our everyday lives and see what we read, what we buy, what our interests are. And let's say they succeeded in getting use of the

Internet banned. Albrecht and McIntyre, who spread the word about RFID via their Web site, would never have had an opportunity to mobilize opposition to RFID, which they believe is bad, because there would be no World Wide Web.

The fact is, the Internet has led to a world in which consumers get far more information about companies than companies get about consumers, and RFID is likely to empower people in a similar way, because they will get more data on the products they buy. Thus, they will have the power to choose to buy or not buy products with tags in them—a point the authors make over and over in the book. Apparently, though, they aren't convinced people will make intelligent choices, because in spite of consumers' ability to reject tagged products, they still call for a total ban of the technology—and they almost never mention all the potential consumer benefits of RFID. Moreover, when the authors do talk about some potential beneficial applications, they tend to suggest you'll be forced to accept a lot of negatives that go along with them.

Take the case of someone whose child is allergic to peanuts. The authors point out that NCR proposed a system where a tagged item, when placed in an RFID-enabled shopping cart, would be identified and its contents compared against the customer's profile in the retailer or manufacturer's database. If the customer has a child allergic to peanuts, the system would alert Mom or Dad to that fact through a computer screen mounted on the shopping cart, and the parent would know not to purchase that particular product.

The authors concede this "may be helpful to some people," but quickly add that you'd have to identify yourself in the store and let the manufacturer of the product track your every purchase to get this benefit. They fail to point out that this system would only work with the shopper's expressed consent, or that it could work equally well anonymously. Customers who don't want their profiles stored in a retailer's database will likely be able to buy an RFID-enabled PDA that stores their private profiles. The PDA could go out to an Internet site hosted by one of those evil companies that wants you to buy their product (while simultaneously providing this information free of charge and protecting your privacy), download the information anonymously and alert the owner of a potential problem.

The authors oppose using RFID wristbands in hospitals to identify patients, even though you would think people would want to be correctly identified when having an operation or other medical procedure. They point out that only about 5 percent of the estimated 98,000 deaths from medical errors are caused by misidentification of the patient (e.g., the doctor gives Mr. Smith drugs, thinking he is Mr. Jones, and Mr. Smith dies of an allergic reaction). That's 4,900 deaths a year in the United States that could be prevented by RFID. The authors describe this tragic and avoidable loss of life as "at most a minor problem," failing to point out that that's only a part of the benefit RFID could bring to patients. RFID could prevent other tragic deaths, such as the case earlier this year in the United States where a girl who was properly identified was still given the wrong heart.

How many of the 98,000 deaths a year are caused by giving the right patient the wrong drug? I don't know, but the authors switch from discussing "medical errors" to "preventable deaths" in hospitals, which are caused by bedsores and pulmonary embolisms and things that RFID—or money spent on other technology—probably can't help.

Despite the numerous shortcomings of this book, it does serve a useful purpose. It highlights the need to have an open discussion about both the potential benefits and potential abuses of RFID. It's only through such a discussion that we will arrive at the best applications of the technology and the best possible future. If only the authors hadn't slanted their arguments so heavily, they would have done more to educate people and advance the debate.

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

