

Spychips Revisited

Spychips co-author Katherine Albrecht has written a lengthy rebuttal to RFID Journal's review of her book, but still has not made a credible case that RFID poses a significant threat to personal privacy.

By Mark Roberti

Nov. 21, 2005—After *RFID Journal* published a review of *Spychips: How Major Corporations and Government Plan to Track Your Every Move With RFID*, I received an e-mail from Katherine Albrecht, founder of Consumers Against Supermarket Invasion and Numbering (CASPIAN) and co-author of the book. She said that in the interest of fair journalistic practices, I should give her a chance to rebut my review on our site. I pointed out that journals that publish book reviews don't give authors the right of rebuttal, but I said I would be happy to publish one if it was factual and advanced the debate over radio frequency identification.

Albrecht did not take me up on the offer. However, she has published a rebuttal on her own *Spychips* Web site (see Dismantling the RFID Journal's Critique of Spychips).

I'm not going to waste your time by going through each point in Albrecht's rebuttal. At more than 7,000 words, it's twice the length of my admittedly long review. But I would like to address a key point raised in her article, which is that consumers will not have a choice about whether to accept RFID in the products they buy.

First, a little history. The authors uncovered a four-year-old patent filed by IBM for "Identification and Tracking of Persons with RFID-Tagged Items." The patent spells out a method for tying people to the tagged items they buy in exactly the way consumer advocates fear. You buy a shirt at XYZ store, you pay with a credit card, and the next time you wear that shirt to that store, the retailer interrogates the tag in the shirt, looks up who bought the shirt and identifies you personally.

Using this technology, profiles could be built up over time. It could be used to track your movements throughout the store, and to make personalized advertising pitches to you, based on your buying patterns. Worse, the patent goes on to say the technology could be used to track persons deemed potentially suspicious.

The authors of *Spychips* say this and several other patents filed by technology companies are the smoking gun proving the RFID industry has a "master plan" (one of the chapter titles) to track people and invade their privacy. The book presents no evidence that these applications have been built and are, or will soon be, used to invade consumers' privacy. (To put the IBM patent in perspective, it was filed a full two years before the privacy issue erupted when Benetton announced plans to tag clothes in its Sisley line.)

In her rebuttal, Albrecht says: "We didn't claim that Company X *will* track you with RFID. We simply point out that Company X is *thinking about* tracking you with RFID, and probably *wants* to. A good way to predict what a company is going to do is to examine what it says it wants to do."

This is quite a different tone than the book takes, but the point made in my review is that there is a far better way to predict what companies are going to do than to look at what they were thinking four years ago—and that is to consider how they *actually are behaving*. My review pointed out that the book presents no evidence

companies have used the tens of millions of RFID tags already carried by people today to infringe on their privacy. I also pointed out that companies such as Benetton, which had no intent to track people with RFID, backed off plans to embed tags in clothes when CASPIAN raised a ruckus in the press. (see Spychips Book Fails to Make Its Case).

Albrecht admits in her rebuttal that companies will back off as soon as their tagging plans become the subject of controversy. So my question, then, is this: why is RFID such a big threat to consumer privacy if companies will back off as soon as a few customers complain about its use in a particular way? Why should we worry about IBM's four-year-old patent if, even if it were ever implemented, the technology would most likely be dismantled as soon as it was discovered? The answer, according to Albrecht's rebuttal, is that RFID tags will be hidden and people won't know they're in their clothes, shoes, handbags and so on, which means they won't be able to make a choice. That strikes me as farfetched in the extreme.

The book spells out how RFID tags can be physically hidden in packaging, but never points out that anyone with an RFID reader can uncover a tag's presence. In order for companies to get away with a "master plan" to secretly embed tags in clothing and shoes and use them to track people, they would somehow have to prevent consumers, journalists and privacy advocates from ever getting their hands on an interrogator and simply reading the tags.

Even if that were possible—which it obviously is not—companies would also have to find a way to prevent the millions of people who make the tags, sew them into clothing, interrogate the tags as they move through the supply chain and collect and analyze the ill-gotten information from ever spilling the beans anonymously on a blog or e-mailing photographic evidence to a reporter (remember: they, too, are consumers vulnerable to being tracked). Given that even minor smart shelf tests where no data has been collected on customers have been exposed, its inconceivable how tagging on such an incredibly massive scale could ever remain secret.

The authors also point out that RFID interrogators can be hidden, without acknowledging that interrogators are actually much easier to detect than a hidden video camera since readers must emit energy to read a tag. At RFID Journal LIVE! 2005, ThingMagic, a leading provider of interrogator technology, gave out a handy little device that could detect the strength of a UHF signal. It cost about \$10 to manufacture. Any privacy advocates, enterprising journalists or concerned consumers would easily be able to get their hands on such a device and expose retailers surreptitiously gathering data on customers through RFID tags in their clothes or personal items.

Of course, it should not be up to consumers to be constantly vigilant about preventing RFID items from being put in the things they buy. Then again, I don't think they'll have to be. Recent history makes it clear that if a company were to try to sneak RFID tags into its products without telling customers, they would be exposed and suffer bad press. Other companies would then learn the lesson pretty quickly, not wanting to be the next one exposed. We've already seen companies such as Marks & Spencer (M&S) address the privacy issue to the satisfaction of its customers after learning from Benetton's mistakes. (While Benetton, in fairness, was not planning to use tags in clothes to track people, it also had no plan for addressing concerns about the potential invasion of privacy the tags presented.)

Albrecht says in her rebuttal, "It's hilarious how Mr. Roberti illogically uses the fact of our past successes preventing RFID abuse to somehow criticize us for alerting the public to further planned abuses." Sure, it might be hilarious if that's what I actually suggested...but, of course, it's not. First, I certainly do not agree that CASPIAN prevented any past abuse because there's no evidence Benetton ever planned to use tags in clothes to invade privacy. My point was that even when companies don't have any plans to invade privacy, they will bow to a small group of people who put pressure on them.

Furthermore, I don't criticize the authors for alerting the public to planned future abuses. I criticize them for

presenting this technology as such an inevitable threat to society that people should reject all its consumer applications—and for not telling them about the many potential benefits RFID offers consumers. They only give half of the story.

Albrecht says she wants consumers to decide whether RFID's use in consumer products is acceptable, but freely admits she doesn't provide information about RFID's many potential consumer benefits. It seems odd to me that someone would claim to be acting on behalf of consumers but would not give them the information they need to make an educated decision. Albrecht says it's not her job any more than it's Schick's job to tout Gillette razors (of course, we're talking about an issue of public policy, not products, so there's quite a big difference between the scenarios).

She claims *RFID Journal* and the RFID industry have been “issuing voluminous quantities of pro-RFID information.” However, the information *RFID Journal* and the RFID industry puts out is almost entirely about the *business benefits* of the technology. Some retailers have put information in their stores about the improved on-shelf availability RFID tags bring, but there has been no concerted effort yet to educate the public about RFID's many consumer benefits.

Nevertheless, I continue to believe that as RFID proliferates, consumers will eventually get good information, and consumers are smart enough to make intelligent decisions. I think most people will understand that they have nothing to fear from RFID because *they* have the power, not the companies. They can always choose not to shop at stores infringing on their privacy.

And while I don't believe companies will ever be able to sneak tags into products and track people without their consent, *RFID Journal* supports CASPIAN's call for mandatory labeling (see Full Disclosure). We will continue to do so, in fact, because consumers shouldn't have to buy a reader to know if a tag is in their product. We continue to urge companies to adhere to fair information practices, not just because it's the right thing to do, but because it's also good for business. And unlike CASPIAN, we won't resort to personal attacks on those who disagree with us.

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

PS: Katherine Albrecht took offense at the comment in my review that *Spychips* uses copious footnotes to give the book the “illusion” of being well researched. She challenged me “to cite a specific page number and footnote that undermines the credibility of our research.” OK.

Footnote 6 on page 44 cites a Chicago Sun-Times article to support a claim that Procter & Gamble (P&G) used RFID to spy on customers. However, while the article does insinuate P&G spied on people, it doesn't present a shred of evidence RFID technology was ever used to collect personal data on customers, or to infringe on their privacy (a webcam was used, but as the story says, it was pointed at the shelves, not the customers).

Here's another example. On page 66, the authors say Texas Instruments “is encouraging retailers to install doorway RFID readers for `keeping track of customers walking in the door.’” Note the present tense. But footnote 24 on the following page points out that TI has removed the page from its site (it actually did this three years ago). So it is factually incorrect to say TI *is encouraging* retailers to track people, based on the evidence presented in the book. And if the authors are intent on telling readers what companies are thinking, then the fact that TI removed this after privacy concerns were raised over Benetton's tagging plans, is certainly relevant.

In any case, my point was not that the footnotes undermine the research; it was that having a lot of footnotes doesn't make a book *well* researched—it just gives that appearance. *Spychips* often presents facts in such a way as to lead the reader to believe an RFID vendor or end user had the intent to spy on people, without presenting any evidence whatsoever to support that insinuation.

For instance, on page 42, the authors say, "...Benetton was planning to put spychips in its Sisley line of clothing..." The implication is that Benetton planned to spy on its customers—why else would you put "spychips" in clothes?—but the book never presents any evidence that Benetton planned to track customers. It never says anything, in fact, about how Benetton planned to use the tags. *RFID Journal*, on the other hand, interviewed Mauro Benetton, director of marketing for the Benetton Group, and was told the company planned to use the tags to track the clothes in the supply chain, and that it would happily remove the tags at checkout if that's what customers wanted (see [Benetton Explains RFID Privacy Flap](#)). Albrecht's readers, of course, are never given these facts.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved