Implementing RFID Responsibly: Calling for a Technology Assessment

Testimony submitted to the Federal Trade Commission
RFID Workshop, Washington, D.C.
Radio Frequency Identification: Applications and Implications for Consumers

June 21, 2004

by Beth Givens, Director
Privacy Rights Clearinghouse
3100 – 5th Ave., Suite B, San Diego, CA 92103
This presentation: www.privacyrights.org/ar/FTC-RFIDTestimony.htm
Contact information:
> bgivens@privacyrights.org
> www.privacyrights.org

Thank you for the opportunity to participate in this workshop.

My presentation is in four parts. I will first summarize the characteristics of Radio Frequency Identification (RFID) that could threaten privacy and civil liberties. I will follow by critiquing some of the technology-based proposals for mitigating privacy threats. I will then say a few words about the role of consumer education. And I will close by calling for a comprehensive multi-disciplinary "technology assessment" of RFID.

RFID Characteristics that Threaten Privacy

Industry representatives have described the numerous benefits of RFID in today's workshop. But RFID is a classic information technology in that there is a potential downside as well. If the technology is implemented irresponsibly, we as a society could experience it not as a wonderful convenience with many social benefits, but as a tool for consumer profiling and tracking -- in other words, as one part of a larger surveillance infrastructure.

So the key question we face is how to shape the implementation of RFID to ensure its socially beneficial aspects and to prevent the negative ones.

RFID has several characteristics that, working together, could threaten privacy and civil liberties. These are:

- The bit-capacity of the Electronic Product Code (EPC) tags, sufficient to uniquely identify all objects around the globe.
- The fact that both tags and their readers can be installed invisibly, enabling tags to be read from a distance without the individual's knowledge or consent.

- And, the data bases that are developed to compile, store, and analyze the vast amounts of data gathered as the products containing RFID tags make their way from the factory to the point of sale, and perhaps beyond.

It's the "beyond" that is of concern to privacy and civil liberties advocates – where the item-level data on the tag can be combined with personally identifiable information -- either in data bases, or when read-write capabilities are more sophisticated and less expensive, on the tags themselves.

Put these qualities together, and there is the potential to create a comprehensive infrastructure for individual tracking and profiling.

Proposed Technology-Based Solutions

A variety of technology-based fixes have been proposed to mitigate the potential threats. One is to "kill" or permanently deactivate tags at point of sale. Another is to provide individuals with tag-blocking devices.

However appealing these so-called solutions appear upon first glance, they are not satisfying ones. Killing tags or blocking them does not address in-store tracking, for example. And some of the strategies for tag-killing are inconvenient and are likely to be used by only a small percent of shoppers. One proposal is the placement of kiosks in stores that shoppers can visit to deactivate tags after paying for goods at the point-of-sale. I question the effectiveness of this approach. How many supermarket shoppers with $100 of groceries in the cart and two young children in tow will stop by the kiosk to deactivate their tags? Probably few.

Further, merchants could offer incentives or disincentives to encourage their customers to not kill tags, for example, by making it more difficult to return or exchange items that do not have working tags. While some might think this is unlikely, we only have to look at the present-day situation around product returns to realize that it's not out of the picture.

Among the top-ten complaints we've received at the Privacy Rights Clearinghouse over our 12-year history are complaints about merchants who do not enable shoppers to return items *unless* they give name, address, phone number, and driver's license number – and that's when the customer *has* the receipt. We've received such complaints about all the top-name retailers, too numerous to list here. So such a scenario could well evolve for RFID tags as well.

Disadvantages that I see for blocker devices are that they, like killer-kiosks, add a burden to consumers. They fail to protect consumers when products are separated from the blocker tag. And like the kill-choice, they create two categories of consumers – those who take the time and energy to use the blocking device, versus the larger number of individuals for whom deactivation is inconvenient or meaningless.

Is Consumer Education the Answer?

Industry representatives are calling upon consumer education as an important way to mitigate consumer concerns and instruct individuals on the choices they have to protect their privacy. As a consumer educator, this recommendation strikes close to home.

I think it's important to differentiate between a true consumer education campaign and an industry-sponsored public relations campaign. Let me give you one example of the former:

In 1996 I participated in a comprehensive consumer education program for the implementation of Caller ID in California. The message of consumer choice revolved around the selection of complete phone number blocking versus selective blocking. The message was developed by a committee comprised of representatives of all stakeholders, including consumers, phone industry representatives, and regulatory agency officials (California Public Utilities Commission).

The message was ultimately conveyed via many media (radio, TV, and newspaper public service announcements) and in many languages. By the time Caller ID was launched, a survey showed that two-thirds of consumers were aware of their choices. The effort was guided by an academician who was a communications scholar. Her area of expertise was in the field of public information campaigns. [To read more about this consumer education campaign, see www.privacyrights.org/ar/callerid.htm]

In commencing with a consumer education initiative for RFID, I strongly recommend the development of strategies borrowed from such efforts as I've just described, rather than from the realm of public relations campaigns.

Proceeding with a Technology Assessment

Last November 2003, nearly 50 consumer, privacy, and civil liberties organizations developed and released a position statement on RFID. The effort was led by CASPIAN, and the Privacy Rights Clearinghouse, joined by EPIC, EFF, the ACLU, PrivacyActivism, Junkbusters, Meyda Online, and other consumer-oriented organizations from around the world. The statement can be found on several websites, including ours, and will be submitted as part of the written comments for today's workshop. [www.privacyrights.org/ar/RFIDposition.htm]

In it we called for the implementation of RFID to be guided by the Principles of Fair Information Practices, something to be discussed later today. We focused on the principles of openness (transparency), purpose specification, collection limitation, accountability, and security safeguards. [www.oecd.org]

The position statement also called for a comprehensive "technology assessment" to be conducted by an impartial body, akin to the assessments conducted by the now-defunct Office of Technology Assessment, a Congressional office from 1972 to 1995. [To learn

more about the OTA and its many technology assessments, visit the archives housed at the web site of Princeton University, www.princeton.edu/~ota.]

Even though industry is moving full-speed ahead with RFID, I continue to believe that such an assessment is vitally important for the responsible implementation of this technology.

Ideally, a technology assessment of RFID would consist of a multi-disciplinary analysis covering its expected benefits as well as its adverse impacts. The assessment would include impacts on labor and the economy, environmental and health implications, and of course threats to privacy and civil liberties. It would be overseen by an impartial body. Representatives of all stakeholders including consumers would be involved.

Here are examples of the kinds of questions that could be addressed by a technology assessment:

- Are there other technologies that can accomplish much the same things as RFID, but that are less intrusive? One alternative technology could be, for example, 2-D barcodes.
- What are some potential consequences of item-level tagging that could be of risk to individuals' privacy and civil liberties? Would law enforcement, for example, adopt surveillance strategies that take advantage of the unique RFID identifiers and their concomitant data base records?
- Can many of the benefits of RFID be accomplished without resorting to the placement of a *unique* identifier, called the Electronic Product Code (EPC), on each and every consumer product that is released into the marketplace? For example, one benefit of RFID that has been touted is to label toxic materials contained inside computer products, such as components containing lead or nickel-cadmium. This application of RFID could make it much easier to separate out such materials when they are headed for the landfill. Yet, such materials do not need the fully unique identifier, only a generic tag that emits the code for "lead" or for "nickel-cadmium." There may be many other ways to benefit from the RFID technology without embedding unique identifiers on each and every product, right down to each individual can of Coke, for example.

The overall goal of an RFID technology assessment would be to enable all concerned, from industry leaders to policymakers, to make informed decisions about the best ways in which to implement the technology – that being, to maximize the social and economic benefits and prevent or minimize the harmful ones.

One of the aspects of Congress's technology assessment process that I like best was that it came up with multiple policy scenarios, not just one. So stakeholders could, for example, consider a roll-out of the technology with high, moderate, or low amounts of government oversight – and consider the long-term ramifications for each approach.

In closing, I strongly recommend that the FTC -- or perhaps the National Academies of Science, an academic institution, or even a consortium of several impartial bodies

working together -- oversee a technology assessment for RFID. It's not too late, and several pieces are already underway separately among industry groups, academic institutions, and consumer groups.

With that in mind I close with a quote from U.S. Senator Patrick Leahy, who in March spoke out on RFID:

"We need clear communications about the goals, plans, and uses of the technology, so that we can think in advance about the best ways to encourage innovation, while conserving the public's right to privacy." [Beth Bacheldor, "Sen. Leahy Calls on Congress to Study RFID," *Information Week*, March 25, 2004, http://informationweek.securitypipeline.com/news/18402730]

I want to thank the Federal Trade Commission for convening this important forum and for enabling me to participate today.