

Policy Group Spearheads RFID Best Practices

The Center for Democracy and Technology announced guidelines for the responsible use of the technology and the data collection it enables.

By Mary Catherine O'Connor

May 2, 2006—The Center for Democracy and Technology (CDT), a nonprofit public-interest group based in Washington D.C., announced yesterday at RFID Journal LIVE! a set of best practices to protect consumers' personal information collected by companies using RFID technology. The group created these best practices as a guideline for the responsible use of the technology and the data collection it enables.

To determine the best practices, the CDT created a working group comprised of representatives from software and hardware vendors that sell RFID technology and organizations that use the technology, as well as industry and consumer-rights advocacy groups. Among the organizations represented were The American Library Association, Cisco Systems, Eli Lilly and Co., IBM, Microsoft, the National Consumers League, Procter & Gamble (P&G), VeriSign and Visa USA.

At least two of the working group's members declined to endorse the report describing the best-practices document. The consumer-privacy organization Electronic Frontier Foundation (EFF) felt the document failed to make the guidelines strict enough to mandate how personal information should be used. The National Retail Federation (NRF) also did not endorse the document.

The working group spent a year developing the best-practices document, available on the CDT Web site. In acknowledging the refusal of some members to endorse it, however, Paula Bruening, staff counsel for the CDT, explained that the group considered the report an interim document only. "RFID is a technology that is evolving quickly," she said. "We're seeing new applications all the time. This [best-practices report] is a living document, something we'll come back to after it's been in the marketplace and we've gotten some feedback on it."

Elliot Maxwell, an RFID consultant and fellow with the communications program at The Johns Hopkins University, also worked on the report. Maxwell noted that, "RFID is like the Internet, in that it is limited only by the imagination of people who deploy it." Consumers should have an increased ability to control information about themselves, he said, but one should also recognize that the technology has the power to increase efficiencies and provide benefits.

The primary goal of the best practices recommendations is to provide guidance on how personal identifiable information should be collected, what choices the consumers should have in providing this information and how the companies should use the data.

To develop this document, the group examined current laws and policies surrounding the responsible use of personally identifiable information, how RFID technology works and where breeches in the security of personal identification could happen in RFID deployments. "We looked at where the technology raises privacy concerns, and where it does not," said Bruening.

In developing suggestions on the steps companies can take toward protecting personal privacy in RFID deployments and where personal information is collected, she said, the group emphasized the use of consumer notification. It also advocated the consumers' ability to choose what data is collected and how that data may or may not be used.

Furthermore, the working group identified three guiding principles to address concerns surrounding the security of personal information linked to RFID technology. One principle says RFID technology is a neutral element—that is, the technology does not threaten privacy, but can be one of a number of vehicles through which personal information can be exploited and used irresponsibly. Another principle is that privacy protections and data security should be primary design elements in RFID deployments, not afterthoughts. Finally, companies should be transparent about their RFID use, so that consumers know about it—and how their personal information could be stored or used—before taking part in any transaction that leverages the technology.

"The guidelines are drawn from fair-information practices, well-established principles for responsible information management," said Bruening.

EPCglobal, an industry group working to commercialize electronic product code standards and technology, last year released its own privacy guidelines for consumer products carrying RFID tags. Maxwell noted, however, that an important distinction between these guidelines, available on the [EPCglobal Web site](#), and the CDT guidelines is that the latter are based on a much broader view of RFID technology than just a means of identifying consumer products with EPCs. "This document goes beyond those applications and includes things such as applications for financial services, or using tags to authenticate goods or services," he said.

Both the EPCglobal and CDT privacy statements and guidelines make clear, Maxwell noted, that the applications for RFID technology are continuing to evolve, and that these guidelines must keep evolving, as well.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved