

## **Privacy Concerns Must Be Addressed to Achieve the Full Potential of RFIDs**

Creative applications of radio frequency identification (RFID) devices hold possibilities for consumers, businesses, and government. They can reduce costs in inventory management, improve drug safety, help to lower error rates in hospitals, and track luggage and cargo at airports to increase homeland security.

There are many possible applications of RFID that do not pose major privacy concerns. But many applications do raise important privacy questions. For example, to the extent that RFID devices can be linked to personally identifiable information, RFIDs could compromise privacy. Even RFIDs that are not intrinsically linked to individuals could nevertheless in some circumstances be used to invade the privacy of an individual. In an era of widespread collection of data about individuals, RFID heightens concerns about the ability of businesses and government using these technologies to create deep, rich profiles about people and their travels, lifestyles, interests and activities.

Well-established principles of fair information practices provide a ready framework to address many of these issues. These principles should apply to the gathering of information using RFID, the handling of that information, and the broader question of consumer knowledge of and control over RFIDs contained in products they buy.

These principles represent a starting point, but determining how fair information practices can be applied in a practical, useful, and meaningful way will require work on the part of stakeholders. Technology developers and businesses often raise the issue of the cost of building privacy into new technology. CDT cautions that it is more effective and efficient to create a culture of privacy that incorporates sound technical protections for privacy and that establishes the key business and public policy decisions for respecting privacy in RFID use before RFID is deployed, rather than building in privacy after a scandal or controversy erupts publicly.

Federal, state and local governments have taken a leadership role in the deployment and use of RFID technology. Government use of RFID raises special concerns and requires special consideration. Government agencies closely involved in deployment of RFID devices must develop privacy guidance for agency use of RFID, as they have for electronic authentication technology. Congress should also explore whether current privacy laws, such as the Privacy Act, Computer Matching and Privacy Protection Act and Section 208 of the E-Government Act, adequately cover use of RFID by government agencies.

To address privacy concerns, CDT believes that it would not be appropriate to enact legislation specially regulating RFID, as to do so would risk the creation of technology mandates that are ill-suited to the future evolution of the technology. In the near term, a technology assessment could provide critical information that would help policymakers, technology developers and businesses find privacy solutions that encourage responsible innovation and use of the technology, and avoid unintended and unwanted consequences for privacy and RFID. CDT supports the development of technology-neutral baseline privacy legislation that would ensure that retail and marketing uses of not only RFID, but any information-collection technology in conjunction with personal information is bounded by fair information practices. Doing so would provide industry with guidance as they deploy new technologies, and consumers with assurances that their personal information is being collected in a manner respectful of privacy.

For more information contact Staff Counsel Paula Bruening at 202-637-9800 or [pbruening@cdt.org](mailto:pbruening@cdt.org).



1634 I Street, NW Suite 1100  
Washington, DC 20006  
202.637.9800  
fax 202.637.0968  
<http://www.cdt.org>