

Privacy in the Workplace

Case Studies on the Use of Radio Frequency Identification in Access Cards

RAND RESEARCH AREAS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND
HOMELAND SECURITY
TRANSPORTATION AND
INFRASTRUCTURE

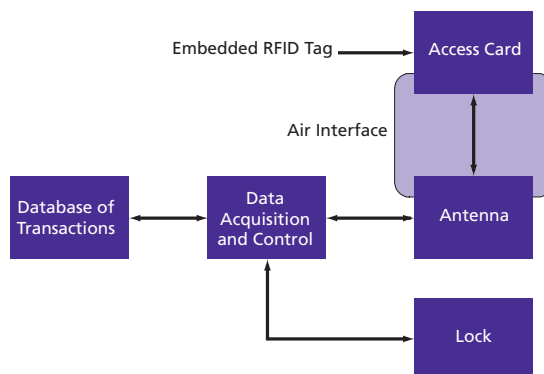
Proposed retail uses of Radio Frequency Identification (RFID) tags have generated privacy concerns, which, in turn, have spurred legislative proposals to limit their use in six states. Such concerns center around uses of RFID tags where an individual does not know that he or she has been associated with the tag or who may be reading the data gathered and for what purpose.

Although such “noncooperative” uses of RFID technology have yet to be deployed, let alone understood, cooperative uses of RFID are widespread in workplace access cards, credit cards, and toll tags. What can we learn from that experience that is applicable to the current debate?

RAND Corporation researchers sought to answer this question by undertaking a replicated case study of six private-sector companies with 1,500 employees or more to understand their policies for collecting, retaining, and using records obtained by sensing RFID-based access cards.

How Do RFID Access Control Cards Work?

The figure shows the typical elements of an RFID access control system. Each system comprises a number of antennas used to interrogate RFID tags embedded in access cards; electronics for data acquisition and control; a lock or some other physi-



Abstract

Companies use RFID workplace access cards to do more than just open doors (e.g., for enforcing rules governing workplace conduct). Explicit, written policies about how such cards are used generally do not exist, and employees are not told about whatever policies are being followed. Using such systems has modified the traditional balance of personal convenience, workplace safety and security, and individual privacy, leading to the loss of “practical obscurity.” Such systems also raise challenges for the meaning and implementation of fair information practices.

cal security feature under the control of the system; network integration of the distributed electronics; and a centralized database that records the details of the use of access cards. After scanning an access card, the system determines whether the individual is authorized to enter (or exit) and unlocks the barrier (if authorized to do so). A record of the transaction is (optionally) captured in the database.

Access Cards: More Than Just Opening Doors

While RFID access cards are primarily used to open doors, five of the six companies interviewed said the records collected were used in both a personally identifiable form (i.e., to understand the movements of an individual) and in aggregate form (i.e., to describe the behavior of many individuals without identifying any of them).

Personally identifiable uses included investigating allegations of work rule violations (e.g., misreporting time spent working) and, in one case, monitoring all former employees of an acquired company to ensure they adopted enterprise norms for work hours.

This product is part of the RAND Corporation research brief series. RAND research briefs present policy-oriented summaries of individual published, peer-reviewed documents or of a body of published work.

Corporate Headquarters
1776 Main Street
P.O. Box 2138
Santa Monica, California
90407-2138
TEL 310.393.0411
FAX 310.393.4818

© RAND 2005

Aggregates of records were used in logistics and cost analyses (e.g., refining building evacuation plans) and to generate required government reports (e.g., an air quality report characterizing the number of employees at the workplace).

Lack of Explicit Policies Raises Concerns

As shown in the table, only one of the companies interviewed has explicit, written policies governing the use of RFID in the workplace, and that one (D) provided them only to the security function in the organization, not the whole company.

Also, none of the companies has a limited data retention policy; they keep the records indefinitely. And although most companies do audit their system records, only one conducts an external audit. Moreover, none of the companies regarded the policy for access control system data retention and use to be a company-wide one that should be managed and overseen by a corporate officer. In all cases, the policymaker is either the security or facilities department.

Finally, in all cases, records were linked to other company databases (mostly to personnel records in human resources, HR), which is inevitable since individual employees are generally assigned uniquely identified cards. In one case (F), the company linked the database to medical records to allow first responders to scan an employee's badge to call up relevant medical records during an emergency. In two cases (C and F), the linkage is fully automated.

Company	Explicit Policies?	Data Control	Policymaker	Other Database Links
A	No	Stored indefinitely; no audits	Corporate security	Manually to HR
B	No	Stored indefinitely; self-audit	Corporate security	Manually to HR
C	No	Stored indefinitely; external audit	Corporate facilities/security	HR
D	Yes	Stored indefinitely; self-audit	Corporate security	Manually to HR
E	No	Stored indefinitely; no audits	Corporate security	Manually to HR
F	No	Stored indefinitely; self-audit	Facility operations	Medical records/HR

A and B = nonprofits; C and D = high-tech manufacturing; E and F = media services.

Policies Are Not Communicated to Employees

While the policies being followed raise some concerns, none of the companies communicates to their employees that data collected with access cards are used for more than simply controlling locks.

To the extent that we understand applicable workplace laws, monitoring and recording employees' use of access cards to enter and/or leave facilities seems to be well within the rights of private-sector companies. But nothing prevents them from making their policies known, and fair information practices codes would encourage them to do so. The RAND study suggests that policies about access control records are invisible to most employees but are otherwise similar to email or phone monitoring policies. Surveys suggest that most such systems have explicit policies and that those policies are communicated to employees.

Implications

Access cards clearly have benefits for both individuals and for security and public safety. They are certainly easier to use than a conventional key, particularly if individual areas or rooms within a facility remain locked and require separate keys.

However, the use of RFIDs in access control systems is an example of how technology has led to the loss of "practical obscurity." Prior to access control systems, anonymous movement in the workplace was nearly guaranteed. RFID tags and fine-grained access controls within a building make it possible to observe the movements of any employee all the time.

Moreover, the use of such systems has modified the traditional balance of personal convenience, workplace safety and security, and individual privacy. These case studies suggest that security and public safety trump personal privacy—that securing the workplace, investigating instances of theft or misconduct, accounting for employees after emergencies, and providing effective responses to medical problems are the priorities favored in designing and operating the systems. Employer policies also trump personal privacy: We found that the organizations studied used such collected data to enforce rules governing employee conduct (A, B, C, D, and F) and to monitor collective behavior (C).

In addition, while fair information practices argue that employees should be informed about uses of access control system records and should have the right to inspect and correct records about their activities, implementing such practices would be impractical for some situations, such as an employee's ability to correct an erroneous record. After the passage of time, could an employee reconstruct the details of daily movements to challenge an automated system? Based on these issues with RFID and given other emerging sensor technologies that enable the collection and analysis of fine-grained details about an individual's behavior, the authors see the need to rethink elements of fair information practices. ■

This research brief describes work done for RAND Infrastructure, Safety, and Environment and documented in *9 to 5: Do You Know If Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace* by Edward Balkovich, Tora K. Bikson, and Gordon Bitko, TR-197-RC (available at <http://www.rand.org/publications/TR/TR197/>), 2005, 36 pp., \$12, ISBN: 0-8330-3719-6. TR-197-RC is also available from RAND Distribution Services (phone: 310.451.7002; toll free 877.584.8642; or email: order@rand.org). The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.



INFRASTRUCTURE, SAFETY, AND ENVIRONMENT

CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND
HOMELAND SECURITY
TRANSPORTATION AND
INFRASTRUCTURE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

This product is part of the RAND Corporation research brief series. RAND research briefs present policy-oriented summaries of individual published, peer-reviewed documents or of a body of published work.

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

[Browse Books & Publications](#)

[Make a charitable contribution](#)

For More Information

Visit RAND at www.rand.org

Explore [RAND Infrastructure, Safety, and Environment](#)

View [document details](#)

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use.