CHAPTER ONE

Introduction

New information technologies have created unprecedented opportunities to collect, store, and transfer information. Technology can be applied to make our lives both easier and safer, but it can also diminish our privacy and civil liberties. Effective decisionmaking about relationships among personal convenience, public safety, security, and privacy requires many kinds of knowledge. Together with Carnegie Mellon University, we outlined an empirical approach to generating such knowledge (Balkovich et al., 2004).

As a starting point, RAND examined a commonly used information technology—Radio Frequency Identification (RFID) tags in access cards. Access cards are often used in the workplace to control entry to facilities. Data describing a card's use by an individual employee can be collected by an access control system and analyzed. This common deployment of RFID technology should require policies to balance the concerns of personal convenience, security, and privacy when access cards are used. This report examines such contemporary workplace policies.

RFID technology is on a path that promises to make it a pervasive technology (Covert, 2004). There are high-profile private- and public-sector commitments to its use in tagging and tracking objects (Feder, 2003; Henry, 2003). These commitments are based on the perceived benefits of the technology. Those benefits include improvements in logistics, supply chain management, and retail sales (*RFID Journal,* 2002a, 2002b; "About EPCGlobal Inc.," 2003). They also include security applications such as that of the Mexican federal judiciary (Weissert, 2004) and proposed improvements to patient management in hospitals (Schwartz, 2004).

These perceived benefits must be balanced against concerns about privacy. Proposed retail uses of RFID tags have generated some of the greatest concerns (see, e.g., Albrecht, 2002, 2003). Such concerns about potential abuses of the technology have, in turn, spurred legislative proposals to limit its use in California, Missouri, Utah, Massachusetts, Maryland, and Virginia[1] as well as calls for a national policy discussion (Leahy, 2004). This privacy debate is primarily about a use of RFID technology—retail sales—that is yet to be deployed, let alone understood.

Although RFID technology is far from being as pervasive as retail sales might eventually make it, it is already in widespread use in workplace access cards. We hope to inform the debate about future uses by studying the policies and behaviors in existing uses. In this re-

[1] A summary of proposed state legislation can be found in "2004 RFID Legislation," 2004.

port, we examine these policies from the perspective of organizations using RFID-based systems to control access to their facilities.

To be sure, differences exist between RFID in tags for objects and RFID in access cards. The use of RFID in access cards, credit cards (e.g., Exxon Mobil Oil Corporation, 2003), and toll tags (e.g., New Jersey Department of Transportation, 2004) are all "cooperative" uses of RFID technology. That is, individuals agree to enroll in programs that offer the personal convenience of using RFID and presumably choose when to do so. Similarly, access cards are often a condition of employment as well as an individual convenience, and employees typically know when they are using them. In contrast, objects with RFID tags that come into the possession of retail customers expose those individuals to "uncooperative" reading of the tag, i.e., the tag carried by an individual may be read without that individual knowingly participating in the exchange. (Of course, such uncooperative reading of RFID tags is also possible with access cards, credit card proxies, or toll tags.)

Despite these significant differences, what might be learned from studying access cards? As with other uses of RFID, access cards offer clear benefits to persons and institutions. An access card is arguably more convenient to use than a key and, from an organizational perspective, offers a more cost-effective way to implement physical security. However, these benefits come with a price: Using the device changes an individual's degree of privacy.

In our results we discuss how policy is formulated and explore how sensor data about access card use, linked to individuals, are handled. Explicit or de facto data-handling policies will need to be formulated for all applications that can link sensor data to individuals. Experience with access cards can inform how such policies should be created because access card systems have already grappled with procedures that govern the retention and use of personally identifiable data.

We conducted case studies of six private-sector organizations and their policies for the collection and use of personally identifiable information obtained from access cards. These access cards rely on RFID technology to make them simple and easy to use. RFID tags are usually embedded in small plastic objects that can be attached to key rings, or in a card similar to a credit card. In the latter case, photographs or text can be printed on the card to provide visible information about its bearer. An access card is typically issued to and used by a single individual—like a key—to gain entry to physical facilities (such as a building or a room within a building).

Cards with embedded RFID tags are a simple, easily understood illustration of competing concerns and how such concerns are balanced:

- *The access card provides personal convenience*. It is easier and simpler to carry and use than a physical key—it must merely be waved near a reader.
- *The access card provides security*. Typically, a door lock is controlled by the system reading the access card. The card authorizes access to a controlled location for its bearer, allowing finer-resolution entry controls and making it difficult for those without authorization to enter.
- *The access card reveals otherwise private information about an individual.* It enables the collection of data about each use of the card that can be assembled into a picture of its user's behavior. Unlike a physical key, the access card has a unique identifier that is typically associated with only one person and provides a way for the access control system to observe the behavior of individuals as the cards are used.

Since RFID-based access card technology has been in workplace environments for some time, it provides an opportunity to study policies governing the retention and use of the personally identifiable information it generates. Our approach is a replicated case study to address the following broad questions:

1. Are there common principles underlying private sector privacy policies for data generated by RFID-based access control systems?
2. Are these policies communicated to the employees who use access cards?

We begin our discussion with an overview of privacy in the workplace. We follow that with an explanation of the methodology used. We then present a summary of answers to the research questions provided by our respondents. We close with an analysis and discussion of our findings.