Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)

June 2006

Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)

Introduction

This document is intended to serve as privacy "best practices" guidance for organizations when designing and operating Radio-Frequency Identification (RFID) information technologies and systems.

The Information and Privacy Commissioner of Ontario (IPC) has a mandate to educate the public and address privacy questions raised by new information technologies, with a view to encouraging effective solutions. Accordingly, the IPC has developed these Guidelines in partnership with industry and other stakeholders. The Guidelines are not intended to supersede any applicable privacy law or regulation.

We recognize that RFID tags are becoming more prevalent in our everyday lives, and offer many benefits and conveniences, from security access cards to ignition immobilizers to highway toll systems and other electronic pass systems.

RFID tags deployed in the supply chain process pose little threat to privacy – they are not linked to any individual but rather, placed on crates, pallets and cases to track products. They act as a unique identifier that uses Radio Frequency Identification for the automatic identification of products in the supply chain. These tags contain standard information pertaining to the products and do not include any personal information.

In order to allow RFID technology to realize its potential for consumers, retailers and suppliers, it is vital that we address privacy concerns prompted by the current state of the technology, while establishing principles for dealing with its evolution and implementation. Accordingly, we encourage organizations to observe and adopt the Guidelines contained in this document whenever deploying RFID technology with consumer-facing implications.

The use of RFID tags in the supply chain management process is not the problem. The problem arises with their use at the consumer item-level. RFID tags, when linked to personally identifiable information, present the prospect of privacy-invasive practices relating to the tracking and surveillance of one's activities. The goal of these Guidelines is to alleviate the privacy-related concerns associated with such data linkages, while increasing the openness and transparency associated with RFID systems. The use of these Guidelines will ultimately facilitate the preservation of trusted business relationships with existing customers, and perhaps assist in attracting new ones.

Scope

These RFID Privacy Guidelines apply to any organization that operates an information system involving the use of RFID technology on consumer products involving or potentially linking to, personally identifiable information.

"Organization" refers broadly to associations, businesses, charitable organizations, clubs, government bodies, institutions, and professional practices. In most instances, these Guidelines will be especially relevant to retailers.

"Information system" refers to any combination of RFID tags, readers, databases and networks that serve to collect, transmit, process and store RFID and RFID-linked information.

"Personal information" refers to any recorded information about an identifiable individual. In addition to one's name, contact and biographical information, this could include information about individual preferences, transactional history, record of activities or travels, or any information derived from the above, such as a profile or score, and information about others that may be appended to an individual's file, such as about family, friends, colleagues, etc. In the context of item-level RFID tags, the linkage of any personally identifiable information with an RFID tag would render the linked data as personal information.

These Guidelines are based upon the 10 principles of the 1996 Canadian Standards Association (CSA) Privacy Code, which were formulated by a wide range of stakeholders, including business, industry and consumer groups. The principles of the CSA Privacy Code now serve as the basis for Canadian privacy laws and regulations across Canada. They are observed by Canadian organizations in their day-to-day policies and practices, and are widely recognized as being one of the strongest and clearest expressions of privacy "fair information practices."

The Guidelines and their application are informed by the following three overarching principles:

1) *Focus on RFID Information Systems, Not Technologies:* The problem does not lie with RFID technologies themselves; it is the way in which they are deployed that raise privacy concerns. For this reason, we prefer to speak broadly of RFID *information systems*. These Guidelines should be applied to RFID information systems as a whole, understood in their broader contexts, rather than to any single technology component or function.

2) *Privacy and Security Must Be Built in from the Outset – at the Design Stage:* Just as privacy concerns must be identified in a broad and systemic manner, so too must technological *solutions* be addressed systemically. A thorough privacy impact assessment is critical. Users of RFID technologies and information systems should address the privacy and security issues early in the design stages, with a particular emphasis on data minimization. This means that wherever possible, efforts should be made to minimize the identifiability, observability and linkability of RFID tags with personal information and other associated data.

3) *Maximal Individual Participation and Consent:* Use of RFID information systems should be open and transparent, and offer individuals as much opportunity as possible to participate and make informed decisions.

This document provides voluntary, consensus-based guidance that recognizes the great variety of uses and applications for RFID technologies and information systems. Because of this heterogeneity, a degree of flexibility in its interpretation and application may be necessary.

We encourage organizations to adopt and to adapt these Guidelines for use in their own policies, procedures and applications, according to their own specific circumstances and needs.

RFID Privacy Guidelines

1 Accountability

An organization is responsible for personal information under its control and should designate a person who will be accountable for the organization's compliance with the following principles, and the necessary training of all employees. Organizations should use contractual and other means to provide a comparable level of protection if the information is disclosed to third parties.

Organizations that typically have the most direct contact and primary relationship with the individual should bear the strongest responsibility for ensuring privacy and security, regardless of where the RFID-tagged items originate or end up in the product life cycle.

2 Identifying Purposes

Organizations should clearly identify and communicate to the individual the purposes for collecting, linking to, or allowing linkage to personal information, in a timely and effective manner. Those purposes should be specific and limited, and the organizations and persons collecting personal information should be able to explain them to the individual.

3 Consent

Organizations must seek individual consent prior to collecting, using, or disclosing personal information linked to an RFID tag. To be valid, consent must be based upon an informed understanding of the existence, type, locations, purposes and actions of the RFID technologies and information used by the organization. Individual privacy choices should be exercised in a timely, easy and effective way, without any coercion. Consumers should be able to remove, disable or deactivate item-level RFID tags, without penalty.

Automatic deactivation of RFID tags, at the point of sale, with the capability to re-activate, should be the ultimate goal. Consumers should be able to choose to re-activate them at a later date, re-purpose them, or otherwise exercise control over the manner in which the tags behave and interact with RFID readers.

4 Limiting Collection

Organizations should not collect or link an RFID tag to personally identifiable information indiscriminately or covertly, or through deception or misleading purposes. The information collected should be limited to the minimum needed to fulfil the stated purposes, with emphasis on minimizing the identifiability of any personal data linked to the tag, minimizing observability of RFID tags by unauthorized readers or persons, and minimizing the linkability of collected data to any personally identifiable information.

5 Limiting Use, Disclosure and Retention

Organizations must obtain additional individual consent to use, disclose or link to personal information for any new purposes. Personal information should only be retained to fulfil the stated purposes, and then securely destroyed. Retailers should incorporate the data minimization principles outlined above, into and throughout their RFID information systems.

6 Accuracy

Organizations should keep personal and related RFID-linked information as accurate, complete, and up-to-date as is needed for the stated purposes, especially when used to make decisions affecting the individual.

7 Safeguards

Organizations should protect personal information linked to RFID tags, appropriate to its sensitivity, against loss or theft, and against unauthorized interception, access, disclosure, copying, use, modification, or linkage. Organizations should make their employees aware of the importance of maintaining the confidentiality of personal information through appropriate training. Although physical, organizational and technological measures may all be necessary, technological safeguards should be given special emphasis.

8 Openness

Organizations should make readily available to individuals specific information about their policies and practices relating to the operation of RFID technologies and information systems, and to the management of personal information. This information should be made available in a form that is understandable to the individual.

9 Individual Access

Organizations should, upon request, inform the individual of the existence, use, linkage and disclosure of his or her personal information, provide reasonable access to that information, and the ability to challenge its accuracy and completeness, and have it amended as appropriate.

10 Challenging Compliance

Organizations should have procedures in place to allow an individual to file a complaint concerning compliance with any of the above principles, with the designated person accountable for the organization's compliance.