Practical Tips for Implementing RFID Privacy Guidelines

Organizations have expressed a particular interest in receiving practical tips to complement their current consideration and use of Radio Frequency Identification (RFID) technology.

RFID technology is seen as a means to improve business process efficiency levels by, for example speeding up inventory checks and minimizing "leakage."

Organizations must balance the advantages of using RFID technology with the potential privacy intrusions such technology can pose.

Even if an RFID tag does not contain any personal information, personally identifiable information may be created if the tag data is linked to a particular individual.

The use of an RFID system (as with other technologies) in retail and commercial environments, is appropriate within limited, controlled and well-defined circumstances.

The following practical tips are intended to help organizations develop retail RFID projects that address privacy issues and preserve consumer trust and confidence.

These practical tips will also help organizations comply with privacy legislation and other best practices, such as the *IPC RFID Privacy Guidelines*.

1. Accountability

- Organizations should have an effective privacy policy in place which recognizes the unique issues presented by RFID technology.
- Organizations with the most direct and primary relationship with the consumer, usually retailers, bear the strongest responsibility to protect consumer privacy.
- Organizations are accountable to the individual consumer for all disclosures of personal information to partners, affiliates, and third parties.

2. Identifying Purposes

- Organizations should only collect, use or disclose RFID-linked personal information for purposes that a "reasonable person" would consider appropriate in the circumstances. A reasonable purpose excludes the following:
    - price discrimination;
    - tracking and profiling individuals without their informed, written consent.

<u>Notice</u>

- Organizations should notify consumers if products contain an RFID tag, through clear and conspicuous labelling on the product itself.
- Organizations should notify consumers of RFID readers on their premises, using

clearly written signage, prominently displayed at the perimeters.

- Signs at the perimeter should identify someone who can answer questions about the RFID system, and include their contact information.
- Consumers should always know when, where, and why an RFID tag is being read. Visual or audio indicators should be built into the operation of the RFID system for these purposes.

3. Consent

- Organizations should have a clear policy for obtaining consent to collect, use and disclose RFID-linked personal information, taking into consideration the nature, sensitivity and intended use of the products.
- Unless the consumer chooses otherwise, removal, destruction, or de-activation of RFID tags should be the default actions at the time of purchase for products that are worn or carried by the consumer, or which may reveal sensitive information (e.g., medications).

4. Limiting Collection

- Before introducing RFID tags linked to consumer information, organizations should first consider alternatives which achieve the same goal, without collecting any personal information. A Privacy Impact Assessment (PIA) is critical.
- Wherever possible, organizations should seek to limit collecting RFID-linked consumer information to the minimum necessary.

5. Limiting Use, Disclosure, and Retention

- Organizations should not use or disclose RFID-linked consumer information for any purpose to which the individual has not consented.
- Organizations should not disclose RFID-linked consumer information to third parties who may profile or perform surveillance on individuals.
- Organizations should delete all RFID-linked consumer information as early as possible.

6. Accuracy

- Organizations that use RFID-linked consumer information for the purpose of making decisions affecting individuals should ensure that the information is as accurate, complete, and up-to-date, as is necessary for that purpose.

7. Safeguards

- Organizations linking RFID tags to personal information should take appropriate measures, beginning with a thorough PIA, to ensure that:

  - RFID tags do not contain personal information
  - RFID tags are not read by unauthorized parties, either within or outside the organizations' premises; and
  - all linkages between RFID tags and consumer information are minimized and kept secure.

- Whenever RFID tags are in the possession of consumers, such as at the time of purchase, they should:
  - be able to choose to have RFID tags removed, destroyed or de-activated easily and without penalty or consequence; and
  - have the ability, upon return of a product, to ensure that their personal information is de-linked from the product item.

8. Openness

- Organizations should publish, in compliance with applicable laws, information on their policies respecting the collection, retention, and uses of RFID-linked consumer information.
- Organizations should make available to the public general information about the RFID technology in use and the meaning of all symbols and logos used.

9. Individual Access

- Consumers should have a right to know what personal information, if any, is stored inside their RFID tags, or else linked to them.
- Upon demand, organizations should provide the consumer with an account of all uses and disclosures of RFID-linked personal information.
- If RFID-linked information is incorrect or unnecessary, there should be a means by which to correct or amend it.

10. Challenging Compliance

- Organizations should inform consumers of their rights and available procedures to challenge that business' compliance with these privacy principles.
- Organizations may wish to ensure that the use and security of any RFID technology or system is subject to regular audits. For example, the audit could address the company's compliance with the operational policies and procedures.