



ELECTRONIC PRIVACY INFORMATION CENTER

Guidelines on Commercial Use of RFID Technology

(FINAL VERSION - July 9, 2004)

Introduction

The guidelines are proposed to guide the use of RFID technology in order to protect both private enterprise interests and consumer privacy interests. This means that these guidelines do not address protection of consumer privacy from any governmental action. Rather, they seek to protect consumer privacy from private enterprises. Further, these guidelines focus on use in the retail and manufacturing industry where retailers and manufacturers are beginning to implement item-level RFID tagging to facilitate supply chain efficiency, inventory control, and similar applications.

These guidelines primarily address commercial, private applications which may use RFID tags to draw conclusions about consumers without their knowledge or consent, or that might generate data which could be used for entirely different purposes at a later date.

These guidelines are divided into three parts. Part A addresses the duties of private enterprises that use RFID technology. It imposes minimum requirements on RFID users, recognizing the advantages that RFID technology can provide while at the same time addressing privacy concerns. Part B addresses practices in which the RFID Users should never engage, including tracking, snooping, and coercing consumers to accept live RFID tags or associate their personal data with an RFID application. Finally, Part C states the rights of consumers who are exposed to RFID technology and incorporates some of the Users' duties stated in Part A.

Definitions

"RFID" means Radio Frequency Identification, *i.e.*, technologies that use radio waves to automatically identify individual items.

"Tag" means a microchip that is attached to an antenna and is able to transmit identification information, *i.e.*, capable of receiving data from, or transmitting data to, a Reader.

"Reader" means a device, capable of reading data from a tag or transmitting data to a RFID tag.

"RFID Subject" or "Individual" means a consumer, customer, or any other such individual that comes in contact with a product that has attached to it, or contains, an RFID tag.

"RFID User" means an RFID operator, such as a store, warehouse, hospital, and the like, who employs RFID technology, including RFID readers and tags.

"Premises" means a store, a warehouse, a hospital, or any other such equivalent space that encompass the tags and the readers that communicate with RFID tags.

"Consent": means the freely given, specific and informed indication of a RFID subject's wish to have his/her personal information processed by the means of RFID technologies.

RFID Guidelines

A. What RFID Users Must Do:

1. NOTICE. Give notice to a RFID Subject of:

a. **Tag presence**, whether through labels, logos, or equivalent means, or through display, either at the place where a tagged item is stored, such as a shelf or counter, or at point of sale, such as a cash register. The notice shall be reasonably conspicuous to the individual and contain information that enables the individual to be reasonably aware of the nature of the RFID system and the data processing in place.

b. **Reader presence**, whether through labels, logos, or equivalent means, or through display, whenever tag readers are present. The notice shall be reasonably conspicuous to the individual and contain information that enables the individual to be reasonably aware of the nature of the RFID system and the data processing in place.

c. **Reading activity.** RFID Users must use a tone, light, or other readily observable and recognized signal whenever a tag reader is in the act of drawing information from an RFID tag anywhere on the sales floor.

2. REMOVAL. Attach tags to items in such a way as to allow for the easiest possible removal of tags.

3. ANONYMITY PRIORITY. Any RFID user -- before linking RFID tags to personal information -- should first consider alternatives which achieve the same goal without collecting personal information or profiling customers. If personal information must be collected and associated with tag data, the RFID user must satisfy the following five requirements:

a. **Consent.** Obtain written consent from an individual before any personally identifiable information of the individual, including name, address, telephone number, credit card number, and the like, is attached to, stored with, or otherwise associated with data collected via the RFID System.

b. **Purpose.** Before obtaining written consent, the RFID User must inform the RFID subject about the purpose of associating gathered data with personal information, and specify that purpose before such attaching, storing, or association.

c. **Use limitation.** Before obtaining written consent, the RFID User must inform individuals about the scope of use of gathered data, whether the use is limited to the person's own interests or whether the data will be disclosed to third parties. Keep data only as long as it is necessary for the purpose for which the data was associated with personal information.

d. **No third party disclosure.** Not disclose, directly or through an affiliate, to a nonaffiliated third party an individual's personally identifying information in association with RFID tag identification information.

e. **Data quality.** Keep gathered data accurate, complete and up-to-date, as is necessary for the purposes for which it is to be used.

4. SECURITY. Take reasonable measures to ensure that any data processed via an RFID system is transmitted and stored in a secure manner, and that access to the data is limited to those individuals needed to operate and maintain the RFID system.

5. OPENNESS. RFID Users must make readily available to individuals, through the Internet or other equivalent means, specific information about their policies and practices relating to its handling of personal information. Any personally identifiable information itself shall be provided upon written request of the individual in a secure manner.

6. ACCOUNTABILITY. Designate someone who is accountable for the RFID User's compliance with these guidelines.

B. What RFID Users Must NOT Do:

1. TRACK. Track the movement of RFID subjects at any time without their written consent to all tag reading events. RFID users shall not track individuals via tagged items on the premises or outside the premises where an RFID system is employed to obtain individual shopping habits or any other such information obtainable through tracking, even upon suspicion of such activities as fraud or shoplifting.

2. SNOOP. Record or store tag data from tags that do not belong to the RFID User for any reason except for the processing of returns or warranty service and upon the consumer's request. RFID users shall not collect RFID data from objects on, or carried by, an individual person for the purpose of generating a consumer profile, even if the profile is assigned anonymously.

3. COERCE. Coerce or force individuals to keep tags turned on after purchase for such benefits as warranty tracking, loss recovery, or compliance with smart appliances; and not require individuals to provide unnecessary personal information as a precondition of a transaction. RFID Users must allow individuals who so desire to enroll anonymously in any RFID data-gathering scheme.

C. RFID Subjects' rights:

1. ACCESS. RFID Subjects must have the right to access data containing personally identifiable information collected through an RFID system, and have the opportunity to make corrections to that information.

2. REMOVAL. RFID Subjects have the right to get tags removed from tagged items.

3. ACCOUNTABILITY. RFID Subjects have the right to challenge the compliance of persons employing RFID systems when practice contradicts the guidelines set forth above.