
Radio Frequency Identification (RFID) Privacy: The Microsoft Perspective

Submitted to the Federal Trade Commission

as a follow-on to the Workshop on RFID: Applications and Implications for Consumers, June 21, 2004

AUTHORS:

Kim Hargraves, Senior Privacy Strategist
Steven Shafer, Senior Researcher

ABSTRACT:

Radio Frequency Identification (RFID) tags are poised to dramatically increase their presence in business and consumer applications. While the technology is 50 years old, recent advances and standardization activities have opened new opportunities for RFID to improve commerce and everyday life.

Some of these same advances create a new potential for infringements of consumer privacy. The responsible development and deployment of RFID technology can enable its many benefits while mitigating or eliminating these difficulties.

Trustworthy Computing is a major commitment of Microsoft Corporation. Trustworthiness demands not only that technology providers create hardware and software that embody integrity and provide fundamental security, reliability and privacy protections, but that all of these elements be demonstrated to the public conclusively. In this whitepaper, Microsoft describes the key privacy issues around RFID use, and presents recommendations to address these issues.

AVAILABILITY:

<http://www.microsoft.com/twc>

MORE INFORMATION:

Please send feedback and comments to privhelp@microsoft.com

Contents

1	PRIVACY ISSUES IN RFID TECHNOLOGY.....	<u>43</u>
1.1	How Privacy Threats Arise in RFID Use.....	<u>87</u>
2	THE MICROSOFT PERSPECTIVE ON RFID PRIVACY	<u>1413</u>
2.1	Unauthorized Access to RFID and Associated Information.....	<u>1413</u>
2.2	Authorized Use of Personally Identifiable Information (PII).....	<u>1514</u>
2.3	Conclusion	<u>1615</u>

1 Privacy Issues in RFID Technology

RFID tags are small mobile computers that communicate over specialized protocols with RFID readers. RFID technology has been in use for 50 years, in such applications as laundry tags, toll-road payment systems, door and building access control, theft prevention, pre-authorized payment systems, and tracking work-in-progress in manufacturing. These applications typically have taken place within a single enterprise or through a single data holder, raising little concern about privacy issues. However, recent developments are changing this situation.

The key developments that are raising the risk to privacy protection are:

- *Unobtrusiveness* – RFID is being developed to replace or augment bar codes in many scenarios. It offers the advantages of being able to operate without clear line of sight, and without the need to isolate each individual label and scan it physically by nearly touching it. These conveniences also mean that neither tags nor readers need to be visible to an observer; tags may be scanned without the need to physically present them to a scanning device one at a time; and there may be no human operator of the scanner to signal its presence. Thus, RFID tags and readers, and their operation, may not have any visible indications to an observer.
- *Uniqueness of ID* – There are many private series of bar codes, but the one system in most common use across enterprises is the UPC (Universal Product Code) and its counterparts across the world. UPC codes designate the manufacturer or source of a labeled object as well as the type of object to which it is attached. The counterpart for RFID, now under development under the name EPC (Electronic Product Code), includes the same information and also includes a unique serial number for each tag. Thus, while a UPC bar code designates a type or model of object, an EPC RFID tag designates a specific object. This raises the possibility that individual objects might be tracked over time through the accumulated record of their sightings by RFID readers.
- *Interoperability* – In the past, essentially all RFID applications have been carried out by a single enterprise. That enterprise controlled all readers and their operation, and held all the data. In most deployments, the readers were situated entirely on the premises of that enterprise. However, the new standards emerging for RFID emphasize the ability for the same tag to be read usefully by many enterprises. The model is that any enterprise can read a tag and query some repositories for information about that tag and its history. While there may be standard protections applied to the repositories, the universal access to their portals elevates the risk of data leakage to a new degree.
- *Proliferation* – The above developments, combined with cost-reducing technologies, are fueling a massive movement around the world to improve the efficiency of goods distribution (the supply chain) through the application of RFID. This is a very commendable goal, whose success is a goal of Microsoft as well as many other industries and agencies. However, the proliferation of RFID tags will also mean that the risks associated with the developments outlined above will increase. And, where risks exist, vigorous attention to their mitigation is necessary.

A detailed analysis of the scenarios of RFID use shows that these developments are not likely to result in privacy breaches in the mainstream use of RFID currently under development, i.e. in the supply chain. The scenarios that would result in the leakage of individual private information are still hypothetical and require numerous developments in the marketplace and in consumer lifestyle. The potential is there, but society-wide privacy breaches through RFID are not imminent at this time.

There are some technological considerations that also limit any current risk to privacy. One factor is that the passive tags slated for widespread adoption have a broadcast range limited by unlicensed radio

power regulations and by physics to roughly 10 feet in practice (the reader signal may be received from farther away, perhaps 90 feet, but the tag response is a fraction of that power). Active tags used in transportation and manufacturing may have a broadcast range of 300 feet, but these are much more expensive and are not slated for labeling individual consumer items. At the other extreme, contactless SmartCards and related RFID tags may become common for consumers, but they have a communication range around 8 inches. Another mitigating factor could be the inclusion of security measures on RFID tags and readers. The new generation of passive tags being developed for mass deployment do not currently have password protections planned to be built in.

In this article, Microsoft illustrates how privacy threats can arise from RFID, and enumerates the key threats in various settings. In general, the key threat to consumer privacy arises from a combination of **circumstances that will occur at an indeterminate point in the future, not in the near term.** However, it is appropriate to consider those future circumstances and to develop practices and policies that will engage the benefits of RFID while helping to ensure that privacy is protected. Microsoft therefore presents recommendations for responsible use of RFID in this article as well.

Microsoft's primary role in the RFID community is to provide software tools for the developers of RFID hardware components and software systems. Many of Microsoft's existing products are already prominently in use in the RFID community, and new products are under development that are specifically related to RFID. In addition, Microsoft products may be tagged with RFID in the course of manufacturing and distribution. Through all of these activities, Microsoft's respect for its customers will govern our creation and use of RFID technology. We are committed to following the same principles and practices we are recommending to the broader RFID community.

The many settings for RFID use are illustrated in Figure 1.

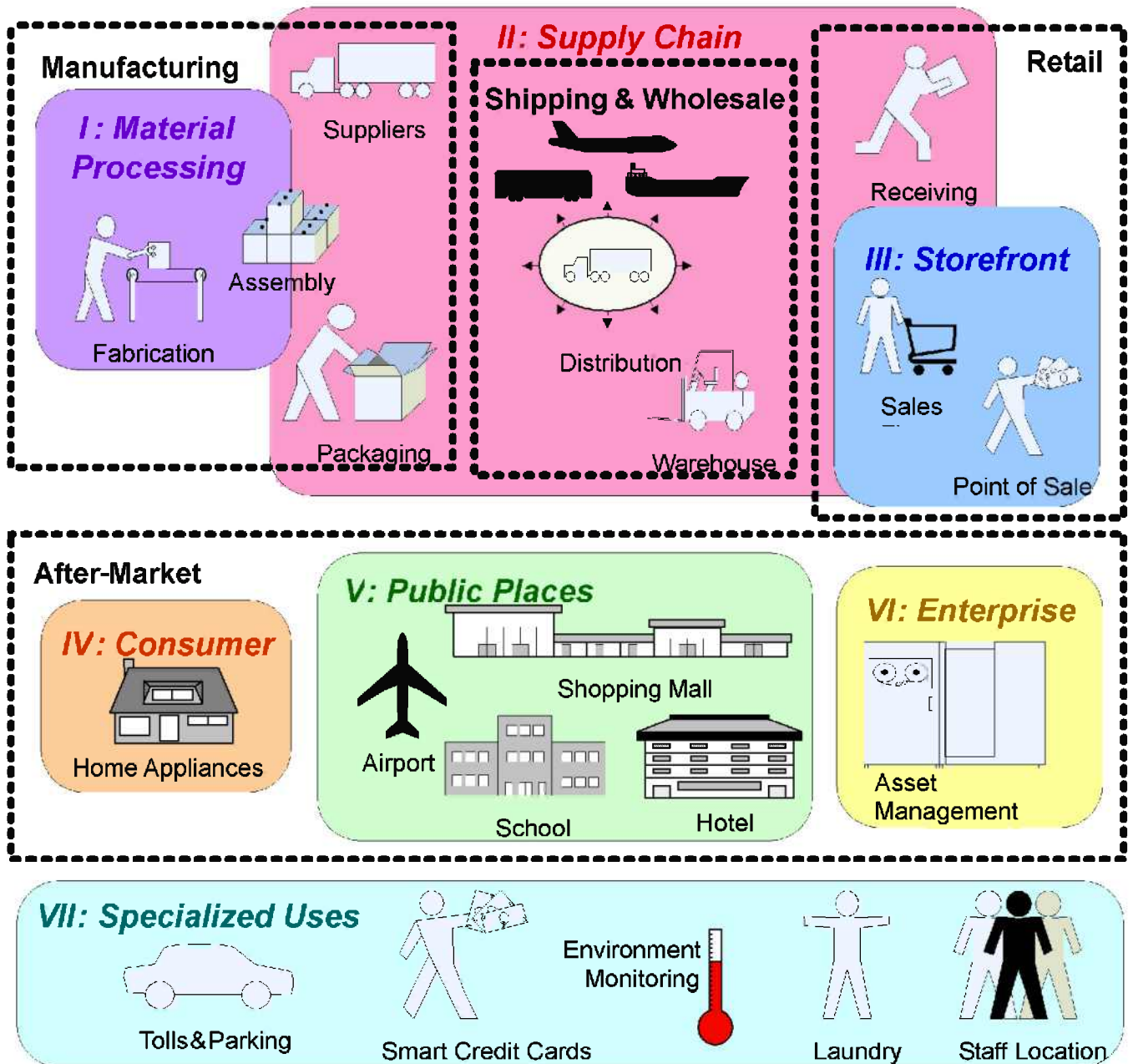


Figure 1. Settings for RFID Use

In this figure are shown several settings for RFID use:

- I. Manufacturing material processing has been and continues to be an arena of RFID use.
- II. The global supply chain, from manufacturing to shipping to distribution to the retail backroom, is poised for explosive growth in the use of RFID. For shipping (conveyances and containers), active tags are typically used to provide long reading range. For packing (pallets, cases, and totes), typically passive tags will be used. Currently, active tags are not planned for use in

