Comment #: 45

Microsoft

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 .... 4~~3~~

1.1 How Privacy Threats Arise in RFID Use .... 8~~7~~

2 THE MICROSOFT PERSPECTIVE ON RFID PRIVACY .... 14~~13~~

2.1 Unauthorized Access to RFID and Associated Information .... 14~~13~~

2.2 Authorized Use of Personally Identifiable Information (PII) .... 15~~14~~

2.3 Conclusion .... 16~~15~~

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.

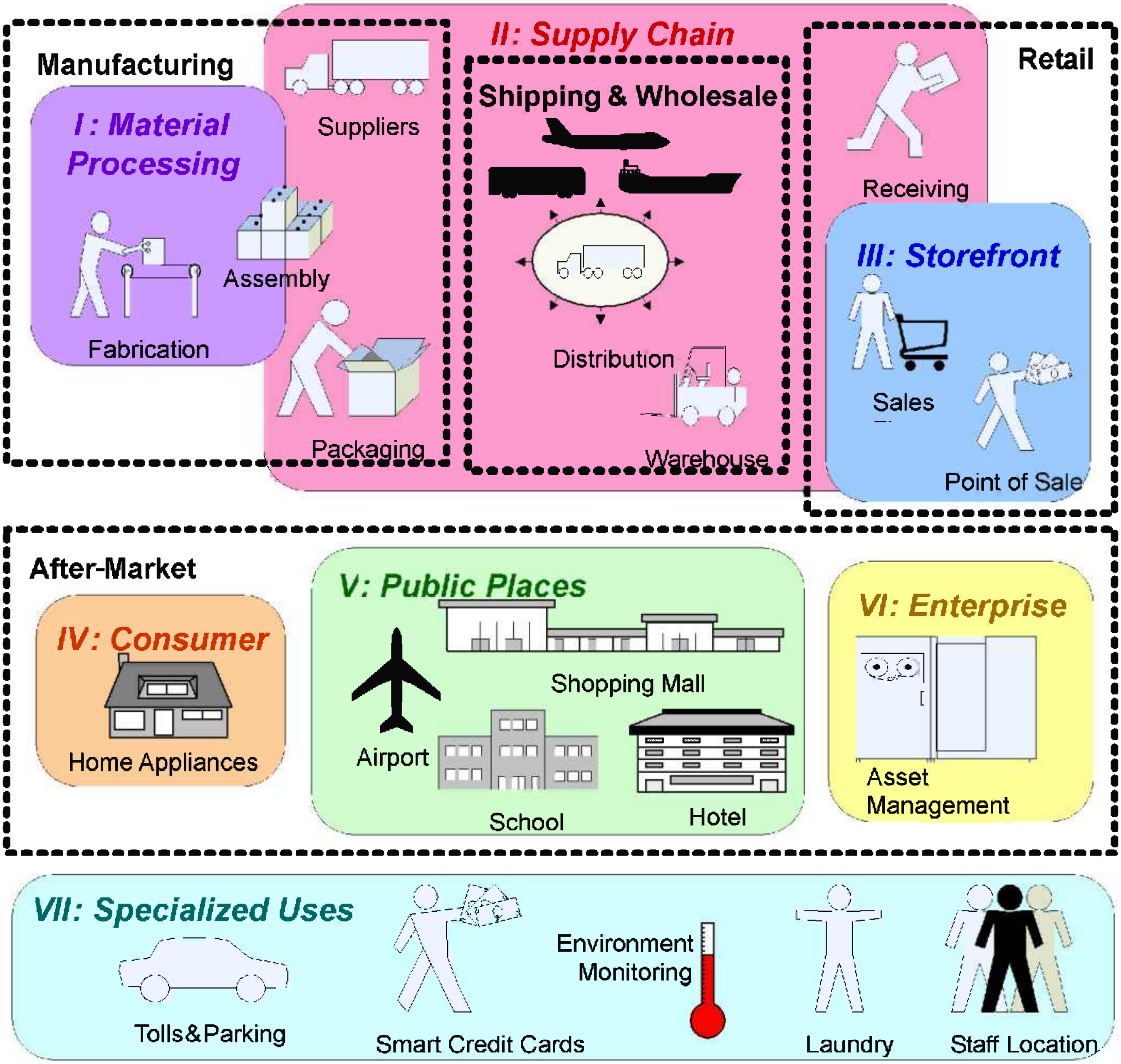

Figure 1. *Settings for RFID Use*

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 consumer scenarios. This requires interoperable RFID tags, such as those under development through the EPCglobal Inc. standards body.

III. For use in the storefront, tags must be applied at the level of individual items rather than shipping units such as crates. These would be passive, interoperable tags. Adoption in the storefront will be slower than adoption for the supply chain, because many more readers and tags will be needed. Item-level tagging is beginning to appear for high-value goods and for large items (which are also considered "cases" for shipping purposes).

IV. Consumer scenarios are "after-market", meaning that they would be based on item-level tags applied by the manufacturer, and which remain present and active on the goods after the point of sale or acquisition. Such scenarios include smart medicine cabinets and smart kitchens; but these have been primarily research scenarios. At present, there are few consumer scenarios being developed outside of research projects.

V. Scenarios in public places would presumably use the same tags as consumer scenarios, but would involve RFID readers in public venues. Few such scenarios have been proposed, however those that are typically seem to be government mandated programs.

VI. Within enterprises, asset management and other scenarios can be extremely valuable. To date, such RFID installations have been based on privately issued tags bearing private number codes. However, in the future, if interoperable item-level tags are applied during manufacture, those tags might be used for asset management within enterprises. Health-care facilities may be among the early adopters of RFID for asset management.

VII. Specialized uses are typically within-enterprise or single-data-holder, and represent the traditional uses of RFID.

The key privacy-related issues that can be noted through this figure are:

- Privacy threats are primarily embodied by tags that are interoperable across enterprises, meaning that many different enterprises may be able to access data about the same tags, and the data may be held by many operators. This arises in settings II, III, IV, V, and possibly VI.

- Privacy threats in RFID generally concern its association with information about individuals, which can only occur with item-level tagging. This will arise only to the extent that setting III becomes viable, or for high-value or large goods that are also shipping units.

- Information about purchases that is contained within the retail establishment is generally considered a legitimate record; the privacy concerns thus arise when tagged goods are carried by individuals from the storefront into settings IV and V.

- If tags are deactivated at the point of sale, then private RFID information is not carried from the storefront to the after-market settings. Thus, the privacy threat is substantially limited to the case that tags are not deactivated at the point of sale. Assuming deactivation is available, the motivation for not choosing it might be from the consumer's desire to use tags in settings IV and V, however, such scenarios appear to be distant. Another motivation might be compliance with requirements such as return or warranty policies, item function, or recycling regulations. There are no such compliance requirements at this time.

- Even if all the above conditions were met – interoperable tags, applied at item level, carried out of the storefront, for use in after-market settings – the privacy threat is minimal inside of one's home (setting IV). It arises only if there are involuntary leaks of data by appliances, or snooping by guests in the home (invited or uninvited); we do not expect these to be common scenarios. (Scares about snooping from outside the home are not supported by the technological realities.)

Thus, it is the carrying of tags into public places that gives rise to the key privacy concerns (setting V).

- From this, we conclude that the privacy threats are very real, but they concern scenarios that are far from the present round of development of the technology, which is aimed primarily at setting II, the global supply chain.

1.1 How Privacy Threats Arise in RFID Use

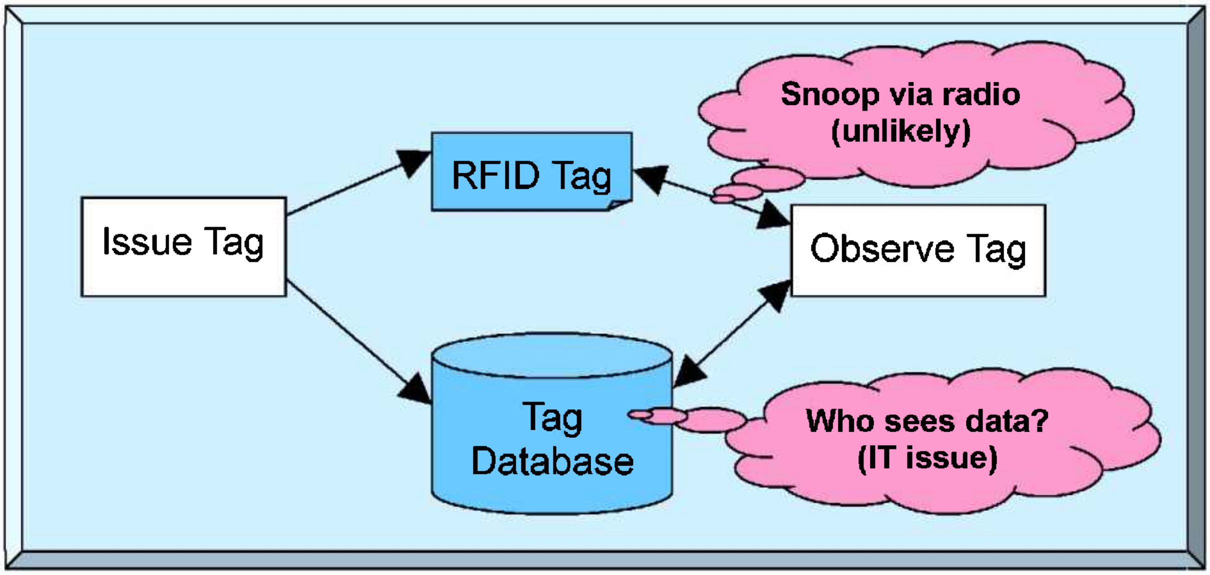

Figure 2. *Within-Enterprise Use of RFID*

In Figure 2, the use of RFID is shown within a single enterprise. When the tag is issued (i.e., assigned a unique ID number), a corresponding entry is written into a private database. Later, when the tag is observed, the ID number can be used to retrieve associated data from the database. There are two opportunities for data leakage:

- A snooper with a radio could observe the tag in unauthorized times or places. However, this is unlikely since the presumption in this figure is that the tag used is restricted to a single enterprise. Any snooper would have to be on (or very near) the premises.

- Someone could break into the tag database, or the data could be used inappropriately. These are real concerns, but they arise in all IT situations and are not unique to RFID. In the within-enterprise scenario, these IT concerns are not exacerbated by the fact that RFID is being used.

> *Example: Fabrikam, Inc. manufactures hats. In its factory, each hat is placed in an RFID tagged tote bin used to track the hat's progress through the factory. As each hat is placed in a bin, the hat's description is recorded in an internal database along with the bin's tag ID number. There is no external use of the RFID tags, and they are not interoperable with other businesses or consumers.*
>
> *The danger of radio snooping is minimal, as someone would have to enter the premises of the factory. The database is of minimal value to the outside, and is protected by standard IT security measures.*

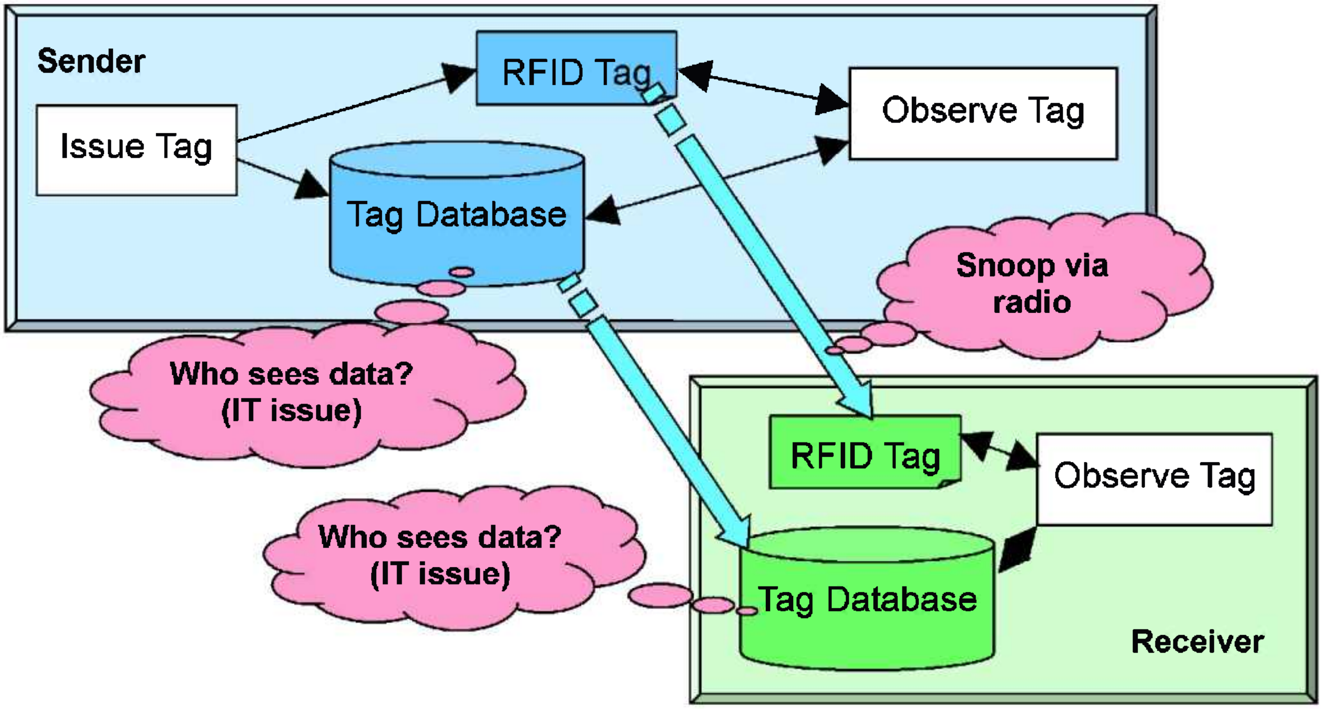

Figure 3. *RFID Use Between Trading Partners*

Figure 3 shows the use of RFID between trading partners. This scenario adds the physical transport of the tagged goods, along with the transfer of information from one database (sender) to another (receiver). The danger of radio snooping within either enterprise is omitted for the reason given above; and the transfer of data over the network is likewise considered not to be an RFID-specific threat. The primary privacy threats are:

- Radio snooping while goods are in transit. Since the databases are assumed to be secure in this scenario, such snooping of tag IDs would have little value.

- Leakage of data from the source or destination database. As described above, the issues here are well-known IT issues and are not specific to RFID.

Example: Fabrikam, Inc. manufactures hats. In its factory, each hat is placed in an RFID tagged case for shipping to retailers. As each hat is placed in a case, the hat's description is recorded in an internal database along with the case's tag ID number. When Fabrikam, Inc. ships cases of hats to Northwind Traders, a retail store chain, the database entries describing the cases' contents are also transmitted. Northwind Traders will remove the hats from the cases prior to putting them out for purchase in the storefront.

Snooping via radio is a possibility, since the tagged cases will be in transit on public streets, but the information is of minimal value. The database is also of minimal value, and is protected by both Fabrikam and Northwind Traders using standard IT security measures.

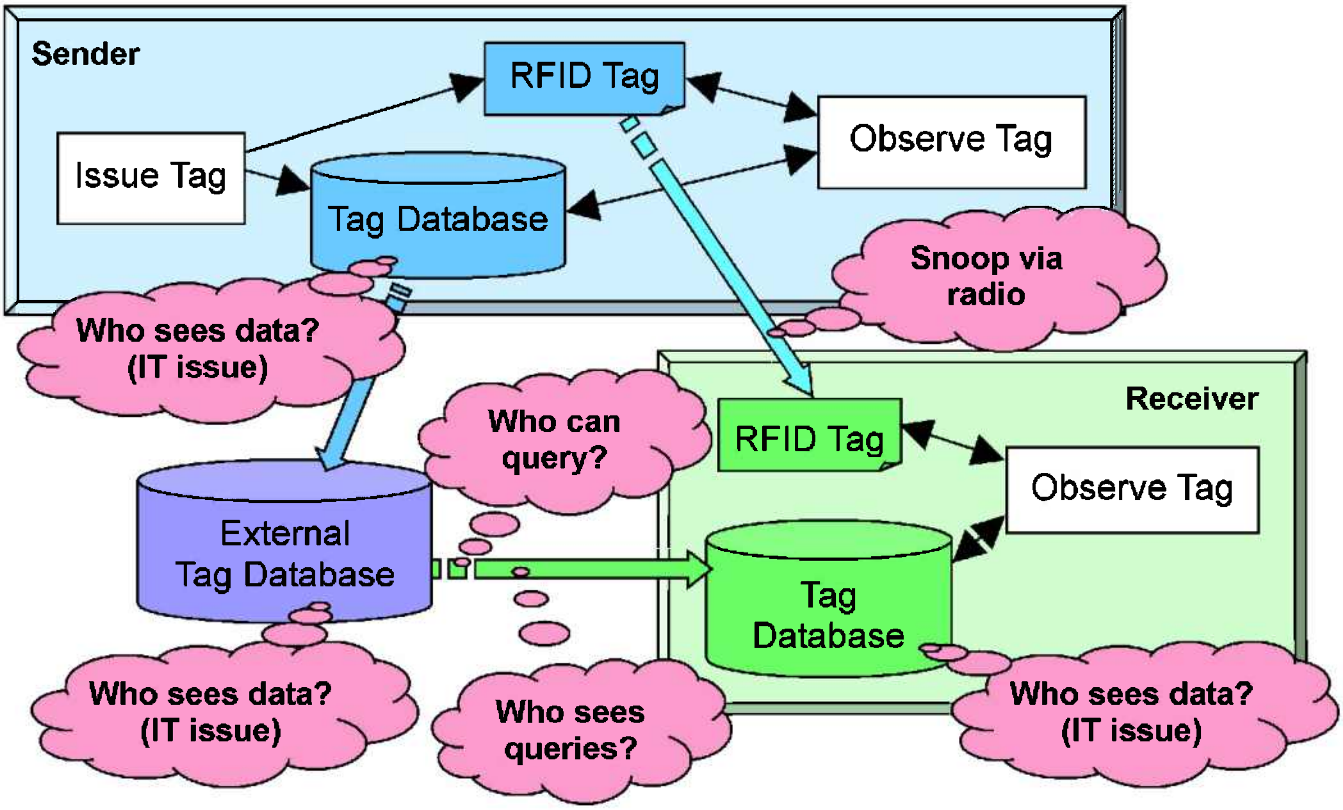

Figure 4. *RFID Use in Anonymous Interoperation*

Figure 4 also shows the use of RFID between trading partners, but in this scenario an external, third-party database is used to store data related to the tagged goods. Most of the privacy issues are the same as the Trading Partner scenario; the new issues pertain to this external database (as before, generic IT issues are omitted):

- Who is allowed to query this database? Presumably all trading partners who handle these tagged items will be authorized. What other parties are authorized to fetch information?
- Who can monitor the queries to this database? Monitoring the queries can also reveal information, even when the returned data is encrypted or otherwise hidden.

Example: As above, Fabrikam manufactures hats which are sold by Northwind Traders. However, Fabrikam now uses RFID tags that are interoperable with all their retail distributors, not just Northwind Traders. The database information is copied to a third-party network site, operated by A. Datum Corporation, from which Northwind Traders and other retailers can retrieve it. Northwind Traders will remove the hats from the cases prior to putting them out for purchase in the storefront.

The tag data and database information are of minimal value, as above. However, there are additional opportunities for information dissemination, intentional or not, due to the storage of the database at A. Datum Corporation, and its Internet-accessible web service. A. Datum Corporation must take standard security measures, including authentication and authorization, in protecting both the data content, and the queries and responses that it communicates with others.

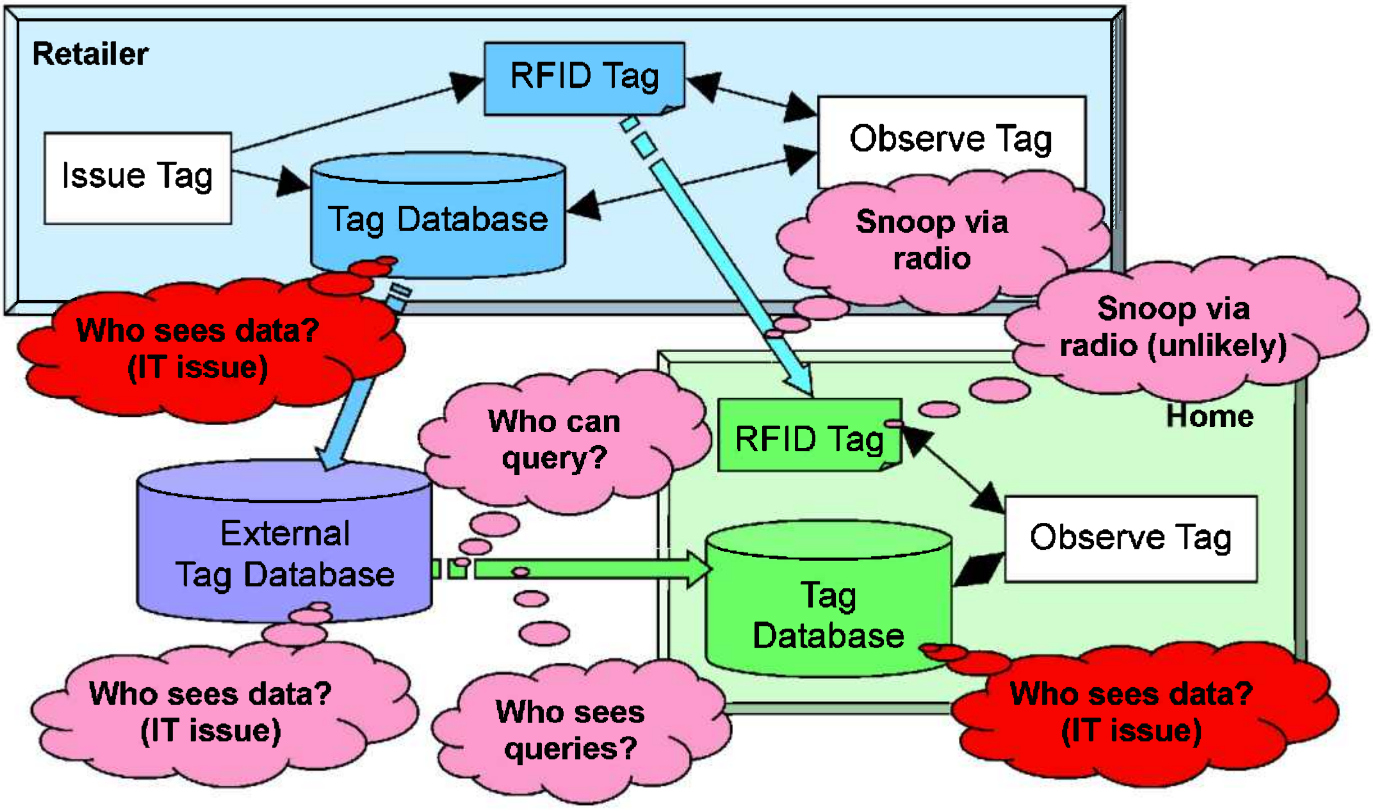

Figure 5. *Private RFID Use in an After-Market Consumer Scenario*

Figure 5 shows the first consumer-use scenario (setting IV in Figure 1). Here, the source enterprise is the retailer, and the receiver is the consumer's home. The privacy threats are the same as for Figure 4, with one addition:

- Radio snooping of items in the home. This is considered an unlikely threat due to the low radio power levels of returned signal from passive RFID tags. Signals are readable at a distance of a few feet in ideal circumstances, and there would be little or no signal to be read through the walls of the home. One can imagine snooping by a skillful guest or through extraordinary means. This risk could be mitigated through the use of passwords and data encryption if such standards were included in future generations of tags. Note that the availability and use of an external database is required for such after-market scenarios, since the consumer is presumably not a "trading partner" of the store with electronic database synchronization. Thus, the store must post the data into a customer-accessible data store.

Two threats that were present in the previous scenario are elevated; they are highlighted here:

- The database of the vendor is more valuable if it contains ID numbers of RFID tags along with associated PII (personally identifiable information) about the purchaser. There may be an incentive for the vendor to accumulate and possibly use or sell this information.

- The database inside the home could be exposed to the Internet by design or by accident. Since individual consumers would be administering such databases, there will be many people lacking the skill, information, or resources to properly ensure the security of their home inventory data.

Example. Northwind Traders requires that all its suppliers tag individual items for sale, including the hats it receives from Fabrikam, Inc. These suppliers, including Fabrikam, record the item descriptions in A. Datum Corporation's data warehouse. Northwind Traders sells these hats, with tags still attached.

Helen is a customer who buys a hat at Northwind Traders and puts it into her RFID-enabled "smart closet" in her house that can give her an inventory list of what's inside. The smart closet reads the tags of all items using a reader built into the closet; it then sends a query to A. Datum Corporation's web service to retrieve the description of each item. These descriptions can then be listed or queried by Helen or by other authorized people in her house via the Internet.

The added privacy risks include exposure of Northwind Trader's database, radio snooping in or around Helen's house, and exposure of her smart closet inventory database. Radio snooping of (passive RFID) tags from anywhere outside the closet itself would be difficult due to the RFID attenuation of the closet walls; outside the house, the difficulty would be much greater due to additional walls and distance from the tags. The database of the smart closet might be shared with other appliances in the home, but probably will not be exposed outside the home to the Internet. If it is exposed, Helen would need to use appropriate security measures or risk its interception.

Helen might not be too sensitive about others learning her choice in hats. But, she might be more concerned if they could learn what she is reading, or what medicines she purchases.

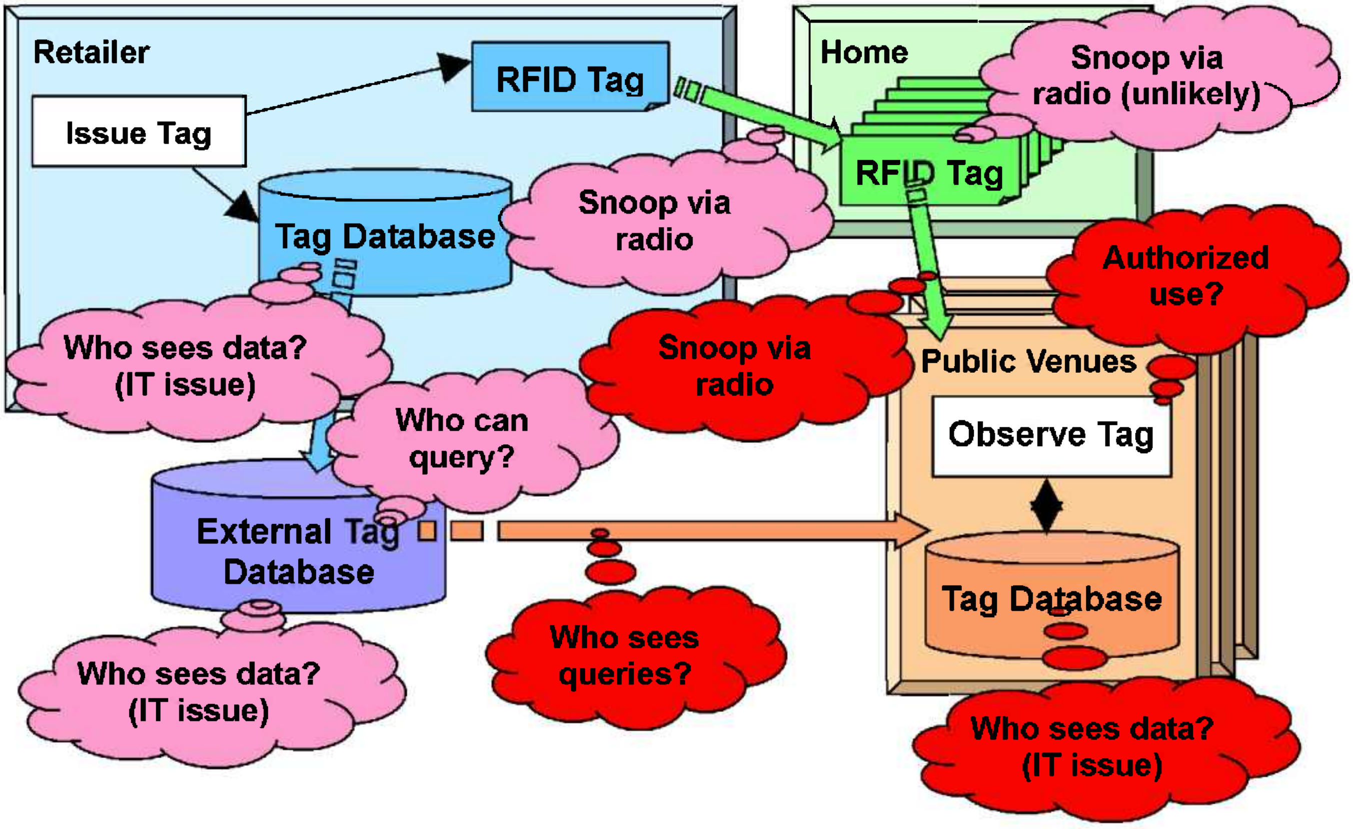

Figure 6. *After-Market RFID Use in a Public Venue*

Finally, in Figure 6, we see the key privacy threats emerge when RFID tags are applied to individual items (blue), remain active in the consumer's possession (green) after the point of sale, and are then carried by the consumer into public venues (orange). This is shown as setting V in Figure 1. The new or exacerbated dangers are shown here in red:

- Since the tagged goods are being carried by the consumer into public places, there is a more tangible threat of unauthorized snooping by radio. Such radios could be carried by individuals or sited in fixed locations within enterprises or public venues. In practice, the radio physics would make such snooping awkward, for example it would require a close-contact swipe by a small antenna, or the use of a larger (several-inch square) antenna at a distance of a few feet. So, this threat is small, but the possibility exists.

- When an RFID reader is in use in a public place, the "notice" principle, discussed below, requires that its presence be announced. Even if an RFID reader's presence is announced, there may be a concern over the use to which the collected data is put, as well as concern over the interpretation of the announcement.

- The usual concerns about IT security of the venue's database apply, but they are exacerbated because now there may be many venues observing the tags' presence. Thus, there are many data holders, and they may have varying levels of skill and compliance with data privacy and security practices.

- Since queries may be made of the external database from many venues, the record of these queries becomes revealing about the consumer's activities. Thus, the danger posed by snooping on the queries, or other inappropriate use of the query history, is exacerbated.

Example. Helen purchases a tagged hat at Northwind Traders, and she wears it when she goes shopping. Each venue that she enters, such as Fourth Coffee, Blue Yonder Mall, and the Southridge Video in Blue Yonder Mall, could operate RFID readers that read her hat's tag. Fourth Coffee doesn't bother to read RFID tags, but Southridge Video is concerned about theft and has tag readers at its doors; and the Blue Yonder Mall records the entries and exits of customers at its various stores. This data is sold to some of the stores, such as Tailspin Toys, which combine it with their own sales records for targeted marketing. Tailspin Toys, lacking the sophistication to do the analysis, actually ships the data to Trey Research to generate reports and mailing lists.

Since Helen is wearing her hat in public, there is a possibility of the hat being scanned by other people using covert RFID readers to read the tags of passers-by. This is technologically awkward, but not inconceivable. Helen expects the anti-theft RFID use by Southridge Video, but she would be surprised to learn that it registers her hat. She is also unaware of the recording of her hat's movements acquired and sold by Blue Yonder Mall. If her personal information is linked to the hat then her movements may be inferred, otherwise it is merely the hat's location/information that is being tracked.

Tailspin Toys is sometimes concerned that its staff may not be following all the security procedures carefully when exchanging data with Trey Research. All of these data handlers query the service at A. Datum Corporation for details about the hat and its history; Helen has little or no awareness of this data trail or the history of its use. All of these records, of course, could be subject to discovery during a legal proceeding.

Against the background of these threats, Microsoft offers the following recommendations concerning RFID privacy.

2 The Microsoft Perspective on RFID Privacy

The primary scenario in which RFID poses risks for consumer privacy will arise when a person has an **item** that has been **acquired**, with an RFID tag that remains active for **after-market scenarios**, especially when this item is carried into a **public venue**. The clear privacy threats emerge under these conditions:

- The tag must be on an **item** that a consumer would acquire, rather than on a shipping unit.

- At the point of **acquisition** the RFID tag ID can be associated with other personal information.

- If a tag is deactivated at the point of acquisition, it no longer exposes personal information. But, if there are **after-market scenarios** for RFID use, a customer might be motivated not to deactivate the tag at the point of acquisition.

- The threats are greatest when the item is carried into a **public venue** in which its tag may be exposed to RFID readers operated by other parties.

The exposure of private information can be due to snooping (unauthorized) or legitimate use (authorized).

2.1 Unauthorized Access to RFID and Associated Information

Unauthorized access to information in computers is generally prevented by security measures built into those systems. The new threats from RFID arise from the proliferation of such data, and from the possibility of snooping via radio.

- The security issues arising from the proliferation of data can best be addressed by continuation of current efforts to develop stronger protection technologies, to educate system operators, and to provide them with new tools that are easier to use and more effective.

- Radio snooping must be prevented by a combination of three features:

  - **Authorization** of readers to tags, for example requiring a password from the reader before a tag will communicate with it.

  - **Authentication** of tags to readers for anti-counterfeiting, for example using an algorithm or unique “signature” feature of a tag.

  - **Encryption** of data transmitted between a tag and a reader.

  Authorization, authentication, and encryption for RFID should all be developed and applied on a routine basis to ensure trustworthiness of RFID radio communications.

One source of concern to privacy advocates and to the general public has been the absence of these features from the current proposals for interoperable RFID tags. It is our view the technology currently under development should include some or all of these features and or the ability for tags to be deactivated. If a tag is deactivated at the point of sale, the key potential threat to security is eliminated, but the tag becomes unavailable for after-market use. The development of security measures for authorization, authentication, and encryption could allow after-market use while also preserving privacy.

2.2 Authorized Use of Personally Identifiable Information (PII)

Microsoft believes in trusted relationships, including the safeguarding of personal information. We have a single principle that guides our policies around consumer privacy and data protection: "***Microsoft customers will be empowered to control the collection, use and distribution of their personal information***." Microsoft's approach to putting consumers in control of data about them is based on the widely-accepted concept of Fair Information Practices, which form the basis of a number of privacy laws and industry guidelines, such as the European Data Protection Directive. Our policies are intended to provide a set of standards that apply to all personally identifiable information, irrespective of the technology in use.

Based on those policies, Microsoft presents these recommendations for policies to protect privacy in the context of RFID:

Notice

Conspicuous notification must be posted and the governing privacy statement must be available near the readers and tags when RFID tags are in use. Items or packaging tagged using RFID tags must be so labeled. The privacy statement must include information on the purposes for which tags and readers are being used.

Choice and Consent

Consumers must be provided with the choice to remove or deactivate tags on purchased items without impairing the primary use of the item or impacting the conditions of purchase (e.g., warranty, returns).

Onward Transfer (Transfers to Third Parties)

Consumers must be notified if personal data associated with RFID tags is being transferred to third parties and be given the opportunity to consent to any secondary use. Data transfers of personal data must include appropriate security measures.

Access

Reasonable access must be provided for customers to their personal data associated with RFID tags to correct or amend such data.

Security

Appropriate security measures must be in place to help protect personal information from unauthorized access, use or disclosure.

Data Integrity and Data Quality

Reasonable steps must be taken to ensure personal data associated with RFID tags is relevant and reliable for its intended use.

Enforcement and Remedy

Consumers must have a mechanism for dispute resolution with the RFID data collector.

The above principles are widely understood to be applied to private information such as Personally Identifiable Information. There are additional scenarios which may require additional analysis:

- A person buys a hat with an RFID tag. Later, the hat's movements are tracked through a shopping mall. Even if there is no association with the person's PII, the person may feel that this tracking is intrusive, especially if the value of the data is high enough that a data holder chooses to sell the data.

- A government mandate requires that all automobiles be fitted with RFID for various administrative purposes. In this case, the government has provided no consumer choice. In general, there can be other compelling public or private interests that must be reconciled with the protection of individual privacy, and governments may decide, through the political process, that such interests take precedence over privacy.

- Different jurisdictions have differing privacy laws concerning what information is protected and what protections are required.

In all of these cases, Microsoft believes that the principle of customer empowerment can provide guidance to public and private establishments as they implement RFID, to ensure that the technology can be put to good use while protecting individual privacy.

2.3 Conclusion

Microsoft believes that the responsible development and deployment of RFID technology can address the privacy concerns with the use of RFID. Continued development of radio security technology for RFID is also a necessary step in the technology's evolution. Application of the Fair Information Practices and other existing laws and regulations around the world provides a sound basis for addressing the privacy of individuals who use or come in contact with RFID. Applying accepted IT controls over the data collected, developing new security tools for non-professionals, and following the well established guidelines and principles for enterprises using the technology will all contribute to responsible development and deployment of RFID in the supply chain and beyond.