Personal Privacy and Use of RFID Technology in Libraries

Vinod Chachra, CEO VTLS Inc.
Daniel McPherson, FASTRAC Project Manager, VTLS Inc.

October 31, 2003

1. Introduction

Most individuals reading this white paper on personal privacy will already be familiar with RFID Technology. However, for purposes of completeness, a brief description of RFID technology is provided with the permission of the author [1].

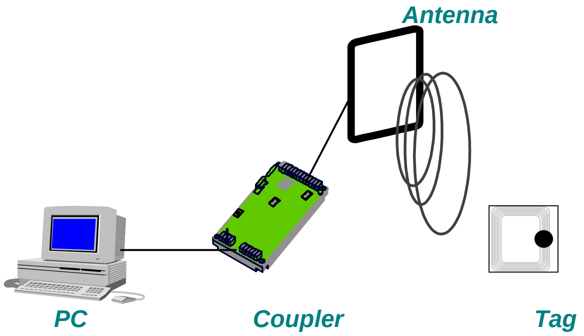
> *Radio Frequency Identification (RFID) is the technology that is slated to replace barcodes in library applications. It is a form of identification that is contact-less and does not require line of sight. The technology, though new to libraries, has been in use in other sectors for more than 20 years. The RFID tags are placed in books and generally covered with a property sticker. Antennas of different sizes, based on application, are used to read the tags and manage the various library functions.*
>
> *The RFID Solution is a revolutionary application of automatic identification and data capture (AIDC) technology. In a library environment, RFID technology resembles a traditional barcode system in that it provides a means of assigning an ID to an item and reading that ID to perform circulation transactions or to take inventory. But while RFID technology resembles a traditional barcode system in application, the VTLS RFID Solution is far superior in performance—plus it offers built-in security.*

How the VTLS RFID Solution Works

A standard RFID system consists of four main parts:

- ***RFID Tags** - Flexible, paper-thin smart labels that are applied directly to library items. Each RFID tag contains a tiny chip, which is both readable and writable and can store information to identify items in your collection. In library applications,it also stores a security bit and if needed, information to support sorting systems.*
- ***Antenna** - A conduit between RFID tags and the coupler. RFID antennas emit radio waves that activate RFID tags as they pass through the activation field. After a tag is activated, it can send information to or receive information from the coupler.*
- ***Coupler** - The link between RFID tags and the PC. The coupler can send information in two directions: It can read information from a tag and send it to the PC (read mode), or it can read information from the PC and send it to an RFID tag (write mode).*
- ***PC** - The link between the coupler and your library automation system. VTLS has developed software that runs on your PC to provide an interface between the RFID hardware and your library automation system.*

1. Tag enters RF field created by the antenna.
2. Antenna's RF signal activates the tag.
3. Coupler sends a modulated signal.
4. Tag demodulates the signal and returns its data to the reader.
5. Coupler sends data to the computer.
6. Computer transmits new data through the coupler to the tag.



2. RFID in retail Sales

RFID technology holds the promise of substantial improvements in retail store logistics. Large department stores like Wal-Mart in USA and Marks & Spencer in the United Kingdom have made aggressive plans for use of RFID in their management of product inventories and sales.

Katherine Albrecht, head of Consumers Against Supermarket Privacy Invasion and Numbering, (CASPIAN) has suggested a moratorium on the commercial use of RFID technology until legal guidelines are set [4]. CASPIAN and other privacy groups may continue to exert pressure on commercial companies as they attempt to improve supply-chain management. [2], [3] The impact of this movement is spilling over to libraries. Several libraries have already implemented RFID technology and others are giving it active consideration, increasing the importance of issues raised by CASPIAN.

3. RFID in Libraries

The most comprehensive application of RFID technology in libraries can be found in Singapore [3]. Libraries in Singapore, under the leadership of the National Library Board, aggressively implemented RFID technology in their libraries. A very large percentage of the public libraries in Singapore are already using RFID technology with remarkable results. Libraries in the United States and United Kingdom are also deploying RFID technology. [5], [6], [7] Examples of the use of RFID technology in USA can be found in both public and academic libraries. New Hanover County Public Library in North Carolina and City Library at Santa Clara California were among the very early implementers of this technology. Others like Sarasota County in Florida are sufficiently pleased with their pilot projects that they are expanding the program to cover all libraries. The economic case is clear – the use of RFID technology is accompanied with improvements in productivity, better levels of service to patrons, effectiveness of self-check stations and reduction in losses due to theft. "However, privacy advocates fear the technology's short-term productivity gain will result in long-term privacy losses [6]"

The Electronic Frontier Foundation (EFF), [11] a digital rights advocacy group, feels that "the time is right for an assessment" of RFID technology [4]. Greg Pottie, a member of EFF and an electrical engineering professor at UCLA, has called for limits on the use of RFID, and believes policy makers should evaluate the technology. For additional details on RFID technology for libraries, please refer to [8], [9].

The following points are important to understand about today's RFID technology in the library environment:

a. RFID tags in libraries are powerless.

RFID tags come in many varieties. The tags that are presently used in libraries are 13.56 MHz (Mega Hertz) tags with no embedded power source. The tags are literally "powerless". Without power the tags can do nothing; they are inert and inactive. The tags receive their power from an antenna (or reader). When a reader comes in close proximity (say within 2 to 18 inches) of a tag, then the tag is temporarily charged and becomes a very small radio and begins to transmit its data. There are no batteries in the tag to store any power. So when the antenna goes out of range, the tag once again becomes inert and inactive. Thus any exposure to privacy issues can only happen in the presence of an antenna which is within 18 inches of the tag. Clearly the concept that someone driving by your house with an antenna, or that a satellite passing overhead is going to energize these tags is ignoring the reality that it would have to be within 18 inches of the item. At that distance, it would probably just be easier to read the title on the cover, rather than scan the item for its ID number!

One might argue that future tags may have a power source associated with them. This has two problems. First, power requirements within the tag would increase the price and size of the tag substantially. Second, batteries are sure to run out, seriously limiting the useful life of the tag – defeating the whole purpose of it. Therefore we expect that even in the future the RFID tags in libraries will be "powerless", with very limited read ranges thus seriously limiting the damage they can do to privacy.

b. RFID tags in used libraries have a very short read range

The read/write range of RFID tags is very limited. The full tag value can be read at a range of 8 inches. (Note: Some tags can be read at a maximum distance of 18 inches). Additionally some tags have security bits. The security bit, which operates at a different frequency and is read in a slightly different manner, can only be read at a range of up to 18 inches. This is by design. During the checkin and checkout procedure it is necessary to write information on these tags. If the range were large then there would be increased risk of interference with other tags in the area. Certainly we do not wish to inadvertently checkout a room full of books to a single patron when our intent is to check out a single book or just a few books. The theft bit has a larger range of 18 inches to allow the securtiy gates to comply with ADA requirements. Security gates have two pedestals. Each pedestal has a range of 18 inches so that the two together can cover the required 36 inches.

In the retail industry there are some RFID tags which have a much larger read range – up to tens of feet. This is not the case with tags used in libraries. In libraries, therefore, it is clear that the use of tags with a limited range have little security risks particularly as the tags are "powerless".

This is one area where it will be desirable, in the future, to ensure that the read range of tags for library applications in not substantially increased over the present range of 8 to 18 inches.

c. Data stored on library RFID tags does not pose a privacy threat.

Data stored on library RFID tags is essentially the same as that represented by bar codes. Let us look at each item stored on the tag:

a. Item ID (identical to bar code information)
b. Security bit (equivalent to magnetizing a magnetic strip in a book)
c. Optionally - shelving location information is stored on the tag (used in conjunction with sorting machines.)

In order for the RFID system to work, only two attributes are required – Item ID (or bar code number) and security bit. (Some systems -like the 3M system- do not store the security bit [8]). Both these attributes are currently in use in libraries. The bar code and magnetic strip are direct equivalents to the data on the RFID. The only added privacy concern is that the item ID can be read without line-of-sight. However, in order to read the RFID tag, one would have to obtain the required RFID based reader and position it within inches of the tag. This would be very difficult to do undetected, and again the only data obtained would be the item ID; one would still need to gain access to the ILS to determine the title or other information of the tagged item. This severely limits the value of trying to invade a patron's privacy using RFID technology. Since one needs to be so close to the book (or other material) to read it using RFID technology, it would be far easier to gain access to the material and view it's title directly.

However, in the event that this risk is still greater than the library wishes to introduce, it is possible to encrypt the item ID on the RFID tag. The data written to the RFID tag then bears no relation to any ID in the ILS, and only the library's own RFID readers would have the algorithm to turn the encoded number into a meaningful value. Even though we feel that this additional security is not necessary at this point, it can be added at little or no cost to further enhance the security of the overall system.

Some systems use mechanical sorting devices. These devices require either the shelving location of the book on the RFID tag or an interface to look it up in the ILS. In any case, there is no patron data on the tag as it is not required; nor is it desirable to have it.

Additional services can be added in the future which may require that additional data be maintained on the RFID tag. For example, some libraries like to weed their collection or send it to off site storage based on the last use date. Whereas it is possible to look up this information from the ILS system it is faster to program it on the tag. Thus at checkin (discharge) one can place the last use date on the tag (and not the patron information) for use in weeding and other inventory management functions.

For future privacy protection, it is important that patron information NOT be added on the tag for any reason. This is an easy requirement to meet, as patron information does not help the workflow in any way. In fact it hinders it; the more information on the tag, the longer it takes to read it, and hence the slower the process.

Even though caution has to be exercised, the real danger does not lie in the use of the RFID tags in libraries but in the implementation of the Integrated Library System (ILS) itself.

4. Much greater patron privacy exposure in ILS system

The ILS poses a much greater risk to patron privacy, particularly with legislation such as the US Patriot Act in place in the United States. In the ILS it is necessary to establish a link between the book and the patron so that the library can tell who has the book checked out. In order to protect the privacy of the patron it is essential that the link be broken as soon as the book is checked-in (discharged). However, some libraries do not break the link immediately causing privacy related exposure for their patrons. Some of the reasons used for not breaking the link are as follows:

a. Link not broken to gather library statistics.

In order to gather usage statistics some libraries maintain a detailed circualation transaction log. This transaction log has the link between the book and the patron. If these logs are maintained for long periods of time then it poses a very serious privacy concern. A properly designed system should use item classes (instead of item ID) and patron classes (instead of patron ID) for statistical purposes. At the time of discharge, the patron ID should be replaced by the patron class, and the item ID by the item class. This way the link between the patron and item is broken but a log record shows the link between the patron class and item class, which can then be used for statistical purposes. As a further precaution, the library should insure that the minimum number of patrons and items is large enough to prevent the possible identification of the individual or item by simply knowing its class. We recommend a number greater than 15.

b. Link is not broken when the patron owes fines for the book.

If here is a fine associated with the book then the library may be required to maintain the link till the fine is paid. This is a legitimate use of the data and the library can only break the link when the fine is paid. The only solution to protect the patrons privacy is to have the patron pay the fine as quickly as possible. Patrons that are overly concerned about this issue may consider establishing a prepaid fine account so that when a fine occurs then it is immediately deducted from the patrons account and the link broken. However, if the patron wishes to audit the payments, the links are broken and so an audit will not be possible.

This matter is in the hands of the patron and the options are:

i) Do not have any overdue books so fines do not accrue
ii) Pay fines as quickly as possible so that the exposure is minimized
iii) Establish as prepaid account and give up the audit requirements so that the link can be broken immediately.

c. Link not broken to provide "value added" services to the patron.

There are certain services that the libraries are asked to provide that depend upon maintaining the link between the book and patron. Examples of these value added services are "reading lists" and "home bound" patrons.

In K-12 schools some "home room" teachers like to assign a "reading list" to students and expect the ILS to manage this reading list. In order for the system to know which books have been read and which remain to be read, the link between book and patron needs to be maintained. Supplying a book delivery service to "Home Bound" patrons require that a similar link be maintained.

Once again this matter is in the hands of the patrons – if they wish to have these additional services then their privacy has to be compromised for the duration that the service is active.

d. Links not broken to support "recovery" functions using backups and transaction logs.

It is typical in managing computer systems to take periodic backups of the system. Backups may be taken with some frequency like weekly or twice a week or each night. In case of computer failure, two sets of data are required – the most recent backup and a transaction log from the time of the last backup to the time when the computer failed. These transaction logs must maintain the links mentioned above otherwise it will be not be possible to recover the data.

Since this is purely an operational issue, it is important for the library to plan their operations is such a manner as to minimize the risk of exposure for their patrons. The frequency of backups must be matched against the possible threats to patron privacy.

All of these are valid reasons to maintain the link until such time as the library determines it can be safely removed. Most important is that the security of the systems upon which the ILS software is running be carefully maintained and monitored as this is truly the point at which someone could invade a patron's privacy. Most ILS vendors will make recommendations in this area and will perform an audit and make recommendations on how to better secure your system if asked.

5. How can we ensure that the future of RFID technology doesn't violate patron privacy?

As shown above, the current state of RFID technology does not warrant the concern being expressed about patron privacy being violated today. However, it is true that future advances in this technology will allow for irresponsible implementations if privacy concerns are not carefully considered. The most common concerns expressed regarding advances in RFID technology are:

a) Increased read ranges, allowing more remote reading of items
b) Increased memory allowing more information to be stored on the tag

Both are valid concerns. However, if the second concern is kept in check, then the first is not as relevant. As stated earlier, patron information does not belong on the RFID tag. Likewise, any information that identifies the book should be kept to a minimum and/or encrypted. Future RFID developments such as higher memory can be used to make encryption stronger, thus enhancing patron privacy. This way, even if future developments make longer range reading of tags a possibility, the information gained will be meaningless outside of the library's own system.

As with all new enabling technologies, libraries, vendors and standards bodies should view these concerns as an opportunity to create standards and guidelines for the future use of this technology. We, at VTLS, suggest that a formal standard be developed, perhaps by an organization such as NISO, to help libraries ensure that when they purchase RFID systems, that the technology store the minimum set of data to support the necessary workflow and no more. The minimum set could include the following:

d. Item ID
e. Security bit
f. Call number (or shelf location)
g. Alternate shelf location (if any)
h. Last activity date.

The standard should also likely address whether broadcast range should be specified and limited and if the information on the tag should be stored in some encrypted format.

6. Use Library Vendors for your RFID solutions

Perhaps the most important lesson of all is that no technology is completely safe and ultimately could be abused. RFID technology used in a reckless fashion can cause serious privacy concerns for users, in the same way that a recklessly implemented ILS could. One way to avoid this is to work with vendors who understand the technology and know its limitations, and also understand the unique privacy needs of libraries. This way, you can be sure that the systems you purchase will be created to enhance productivity and provide other benefits while keeping the risks to the minimum. A vendor who understands both RFID and libraries is best equipped to use the right technology in a library environment, and to use future developments in the technology to enhance, rather than compromise, patron privacy.

7. Conclusion

The RFID tags in libraries offer the possibility of great increases in productivity and hold a promise of better service for the patrons. The tags are "powerless", have a very small read range, store a minimum amount of data and carry no patron data on the tags. All these factors make privacy concerns almost non-existent at this time. However, it is possible that in the future the tags will have a larger range and more data will be stored on them. This is a direction that should be avoided. The library should always exercise the option to not store any data considered "risky" for its patrons. Through the creation of standards and implementation guidelines, this is possible.

The greater danger to patron privacy comes from an improperly designed or implemented ILS. It is therefore important to work with a vendor that understands patron privacy concerns and builds systems that will minimize the risk for the patrons.

References

1. Experiences in implementing RFID solutions in a multi-vendor environment
   VINOD CHACHRA (VTLS Inc., Blacksburg, USA), IFLA Conference, Berlin, August, 2003
   http://www.ifla.org/IV/ifla69/papers/132e-Chachra.pdf

2. Group Proposes RFID Privacy Law, June 18, 2003
   http://ww.rfidjournal.com/articleview/466

3. Raising an RFID Ruckus, Steve Ulfelder, October 7, 2003,
   http://www.newsfactor.com/perl/story/22439.html

4. Privacy activists call for rules on RFID, Alorie Gilbert, CNET News.com, August 19, 2003
   http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,39115785,00.htm

5. SF Library Wants to Track Books with Computer Chips Ron Harris, Associated Press, October 3, 2003 http://usatoday.com/tech/news/internetprivacy/2003-10-03-sf-library-rfid_x.htm

6. City Library Adopts Controversial RFID Chips, Matthew Artz, October 10, 2003
   http://www.berkeleydaily.org/article.cfm?issue=10-10-03&storyID=17547

7. And They Shall Know you By Your Books Timothy, October 5, 2003
   http://yro.slashdot.org/article.pl?sid=03/10/05/2029251&mode=thread&tid=126&tid=158&tid=188&tid=192&tid=99

8. Choosing Your RFID Solution, VTLS Inc., November, 1999
   http://vtls.com/Products/rfid/documents/choosing.pdf

9. VTLS Radio Frequency Identification Solution, VTLS Inc. November, 1999,
   http://vtls.com/Products/rfid/documents/tearsheet.pdf

10. RFID@Library - A Journey That Saves S$50m, CHAN PING WAH (National Library Board, Singapore), IFLA Conference, Berlin, August, 2003

11. Plan for Library Book Tagging Generates Privacy Concerns, October 2, 2003.
    www.eff.org/Privacy/Surveillance/ RFID/20031002_eff_pr.php