International Journal of Information Management 31 (2011) 244–251

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

The application of RFIDs in libraries: an assessment of technological, management and professional issues

Forbes Gibb[a,*], Clare Thornley[b], Stuart Ferguson[c], John Weckert[d]

[a] Department of Computer and Information Sciences, University of Strathclyde, 26 Richmond Street, Glasgow G1 1XH, United Kingdom
[b] School of Information and Library Studies, University College Dublin, Belfield, Dublin 4, Ireland
[c] Faculty of Arts and Design, University of Canberra, ACT 2601, Australia
[d] Centre for Applied Philosophy and Applied Ethics, Charles Sturt University, Wagga Wagga, New South Wales 2678, Australia

ARTICLE INFO

Article history:
Available online 13 August 2010

Keywords:
Ethics
Radio frequency identifiers
Library management
Processes

ABSTRACT

This paper starts by outlining the technologies involved in RFIDs and reviews the issues raised by their general application. It then identifies their potential application areas within the library sector based on a generic process view of library activities. Finally it highlights the issues that are raised by their application in libraries and provides an assessment of which of these issues are likely to raise ethical concerns for library professionals. The purpose is to provide an overview of the technology within the context of the library process and to highlight issues which may raise ethical concerns for the profession. A second paper will focus specifically on these concerns within the context of the professional obligations of the librarian.

1. Introduction

RFIDs are small chip-based devices which can store data which can be used to identify objects uniquely. Their origins can be traced back to radio frequency transponders which were attached to allied aircraft in WWII to identify friend from foe (Cavoukian, 2004). Identification is an essential component in the delivery of library and information services as it facilitates procurement, stock management, protection of intellectual property, location and retrieval of information objects and discrimination between editions and formats. Key to the application of identifiers are the existence of strings to identify information objects (e.g. an ISBN), standards for the production of strings (e.g. ISO standard 2108:2005 for ISBNs), and schemes for the implementation and monitoring of these standards (e.g. the International ISBN Agency). These identifiers should also incorporate the characteristics of uniqueness, resolution, interoperability and persistence (Paskin, 2008). That is, a string should be associated with one, and only one, object; it should be capable of generating associated information, such as price and publisher; it should be usable by multiple participants irrespective of platform; and should identify an object in perpetuity.

An object which contains or is tagged with a RFID can be detected, categorised and tracked as it moves from one location to another. It should be emphasised that, unless combined with other technologies, RFIDs only allow the presence of an object to be detected within an area rather than providing a specific location. However this still offers a considerable improvement over other existing identification technologies. The data storage capacity of RFIDs varies from a few bits to several kilobytes but library applications normally use tags with 256 bits, with 2048 bit tags also available. The data can be read from fixed or mobile devices at high speeds and without the need to have a line of sight between the object incorporating the RFID and the reading device. This makes RFIDs considerably more effective and versatile than conventional barcodes, although their cost is currently much higher. Barcode technologies are also improving, however, and systems such as Bokodes, which use small (<3 mm) LED based tags which can be read using mobile phones, may prove to be viable alternatives (Mohan et al., 2009).

RFIDS can be divided into two main types: passive and active. Passive RFIDs do not have their own power supply but convert energy from transmissions from a reading device into a signal which can be delivered across very short (up to 60 cm) or short ranges (up to 5 m). Passive RFIDs are the cheapest and smallest of the technologies. Data can be modified on certain types of tags and this can be restricted to only the security bit being changed when an item is lent. Active RFIDs are generally larger and more expensive but, as they have their own power supply, can transmit data over much longer ranges (typically up to 100 m). In general the data contained on an active RFID is re-writable, and hence the RFID itself is re-usable. Standards for RFIDs are evolving and embrace aspects such as tag structures, self service, wireless connections and

* Corresponding author. Tel.: +44 41 548 3704.
E-mail address: forbes.gibb@cis.strath.ac.uk (F. Gibb).

0268-4012/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ijinfomgt.2010.07.005

security settings. However, agreement has been reached by major suppliers to support ISO 28560-2 for tag content and structure.

RFIDs are widely expected to bring significant benefits to enterprises, ranging from retailers to legal firms and health services, as they have the potential to minimise the physical handling of goods and reduce or eliminate errors throughout the supply chain. Kelly and Ericson (2005) highlight the efficiencies that may be gained in the following areas: inventory control, manufacturing processes, retailing, transportation, logistics, security and recalls. Interestingly these are all activities which may be encountered in the library sector and are addressed below in Section 2. However Kelly and Erikcon, and others, also raise many concerns about the legal, privacy and ethical issues that might arise from the widespread use of these technologies. For instance, Kelly and Ericson speculate on whether a RFID enabled article of clothing could be used to incriminate a citizen if it placed them at the scene of a crime.

These concerns are echoed in a joint report from the European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC) and the Bureau Européen des Unions de Consommateurs (BEUC) which challenges the claim made by the European Commission that RFIDS have great potential to improve the life of European citizens (ANEC and BEUC, 2007). While recognising that many RFID applications are neutral with respect to the consumer the authors express concerns that some applications could have adverse effects. As a consequence they recommend that no funding should be approved into research aimed at tracking citizens, and that a European committee dealing with ethics should be formed. The main areas of concern raised in the report include:

- privacy (tracking, profiling and discrimination);
- security (identity theft);
- health (EMF emissions);
- freedom of choice;
- competition;
- environmental protection.

RFIDs can enhance the ability to track and trace citizens particularly if they are combined with location-based technologies such as the global positioning system (GPS). Aspects highlighted in the report in the context of tracking include: control of children's behaviour by parents, monitoring of pupils in schools, and the impact of RFID implants. The use of RFIDs to monitor attendance of pupils has already occurred in California where it met with fierce resistance from parents who claimed the technology had been introduced without consultation (Zetter, 2005). Although the school maintained that RFID enabled badges would help reduce truancy and provide early warning of missing children there were concerns that their use was linked to attendance based funding rather than to an enhanced educational environment.

With respect to profiling, concerns are expressed about how aggregations of increasingly detailed data could lead to the identification and characterisation of an individual without their consent. The potential of programmable RFIDs being augmented with consumer data is also identified raising issues regarding consumer rights to know and to choose. It is recommended that consumers should be informed about the use and location of tags and readers in any premises that they enter and pictograms should be used to indicate that objects are tagged. Consumers should also have the right to opt into RFID data capture for profiling (rather than opting out) and should have the right to require that RFIDs are either destroyed, removed or deactivated at the point of sale. Furthermore, consumers should not be discriminated against should they request de-activation, etc., of a RFID, or refuse to opt in to RFID schemes.

With respect to security the authors note that e-passports have already been hacked and that information has been copied from the embedded RFIDs. They therefore recommend that security and privacy concerns should be addressed in the design phase of future RFIDs and that liability for damages should be introduced should security be breached and personal data exposed. With respect to health concerns are expressed about the lack of research into the effects of extremely low frequency (ELF) and electromagnetic field (EMF) exposures in technology and risk assessments. There are also concerns about potential lock-in to components and consumables (though these should be addressable in part through more open standards) and the implications this has for competition. With respect to the environment the high levels of heavy metals, adhesives and silicon are highlighted, as are disposal and re-cycling of RFIDs.

Specialist RFIDs have also been developed for use in living tissue (implantable RFIDs) and are being used for pet passports and for labelling patients. In these applications the RFID is contained in a hermetically sealed glass tube which is covered by a plastic which bonds to tissue to stop it moving around the host. The United States Food and Drug Administration approved the first RFID for implanting in humans (VeriChip) in 2004. The chip is used to identify a patient and to provide a link to the patient's medical records in a database which allows doctors to provide more rapid and effective treatment, reduce the risk of adverse drug effects, identify patients who are unable to communicate, and ensure authentication for medical procedures. Foster and Jaeger (2007) consider the implications of implantable RFIDs including potential and actual application areas such as identification tag replacements for soldiers, customer management in night clubs, employee tagging and tagging of immigrant workers.

The issues that are raised by implants, explicitly or implicitly, are:

- coercive applications (e.g. to monitor immigrants);
- funding (i.e. who pays for implantable RFIDs);
- bodily integrity (i.e. modifying a body);
- invisibility of devices and readers (i.e. others might be able to read the chip without the individual's knowledge);
- security (i.e. is data encrypted or open?);
- ownership (e.g. does a device belong to a patient or hospital and, by implication, an employer or employee? who owns the data on the chip? what happens to the data or chip if an employee leaves?);
- scale (i.e. chips will store larger and larger amounts of data);
- data integration (i.e. the use of a common piece of data to link to multiple databases related to an individual).

Sade (2007) also comments on implantable RFIDs as a response to the American Medical Association (AMA) Resolution 6 (A-06) which called for a study into the medical and ethical implications of RFIDs in humans. Under this resolution only passive RFIDs are currently approved for use in humans and no personal information should be stored on the chip. The issues raised by Sade are:

- physical risks to patients (e.g. migration of devices within tissue);
- interactions with pharmaceuticals, an area which is as yet untested;
- interference with other medical equipment, which may adversely affect patient care;
- privacy (i.e. there is an obligation on the profession to protect patient confidentiality);
- security of data, an area which is as yet relatively untested;
- the need for informed consent, including how data will be used.

Although implants are not of immediate relevance to librarians, the intimate association of a RFID with an individual does raise sim-

ilar issues in terms of employer–employee and supplier–customer relationships (discussed below).

Cavoukian (2004) raises concerns over the use of RFIDs in general but many of these concerns are relevant to the application of RFIDs in library and information services. Firstly the use of RFID technologies in currency (and many libraries sell local publications, discarded stock, etc.) removes the anonymity currently offered by cash. Secondly smart shelves, which could be used to control access to rare materials, can be used to monitor customer behaviour. Thirdly, patrons should have the right to informational self-determination. That is, they should be given the choice of when and how to provide information about themselves in order to retain their autonomy. While patrons must accept that they need to provide some information in order to underwrite a transaction they should be aware of what is being provided in order to judge that it is reasonable for the purpose.

Tags may also be embedded in products without the consumer's knowledge and there is therefore an obligation on the service provider to communicate the existence and role of tags when a customer signs up for services. In this context Schuman (2005) highlights the filing of patents by several large corporations, which explicitly exploit the ability to read RFIDs, and hence track consumers, beyond the point of sale. For practical purposes tags will not be removable from books on loan and it is unlikely to be economic to de-active and re-activate them when a book is returned. Tags can also be read from a distance and customers must therefore be advised that the tags will still be live when a book is taken outside the library and that there is the potential for the data to be read by suitably configured equipment. Clashes between tags and systems in other agencies must also be considered to avoid wrongful accusations of product theft.

Finally, law enforcement agencies have increasing powers to gain access to underlying systems and the data that these hold about citizens. RFIDs have the potential to change the relationship between information content and library user in terms of how easy it is to find data based on this relationship and the ease with which possible conclusions could be drawn. An accession number on its own is neutral but long-term storage of that data in association with a reader number could be used to develop a profile of that reader's interests. A transaction number could be used to provide the temporary link between the accession number and a reader and this could be deleted once a loan has been concluded. Library managers should therefore consider whether they should separate, as far as is possible, the data they hold about an item of stock from the data they hold about a reader of that item of stock. In this context NISO (2008) have recommended which data elements should be mandatory and which should be optional.

Such concerns should be addressable, at least in part, through the application of three key privacy principles:

- Notice and consent: users have the right to know that a product contains a RFID and that readers are being used, either overtly at an issue desk, or covertly to improve security. They should also participate in a RFID application voluntarily through consent, though non-consent may mean that access to services is not permitted if that consent is not given. Van't Hof and Cornelissen (2006) refer to this as identity management where an individual defines what may be known or not known about that individual.
- Choice: the right to have the RFID tag in a purchased product deactivated. Privacy enhancing technologies (PETs) have been proposed which deactivate RFIDs based on stored user preferences. However it could be argued that these also represent the storage of more personal data and that all RFIDs should be deactivated automatically unless a consumer specifies otherwise. Although this will not be possible for items that have been borrowed, any item that becomes the property of the customer should have its RFID deactivated, where requested.
- Control: the right to have personal identity information kept separate from information about that object. There may be a need to use a transaction number to link the two on a temporary basis but that does not need to be held once a loan has been concluded.

Gruber (2005) discusses the implications of RFID applications for the privacy of the employee rather than the consumer. Smartcards are already used extensively to control access to and within buildings and hence the entry time, exit time and point of entry of an employee can be recorded. However, RFIDs take this a step further by introducing the possibility of monitoring the location of employees in real time and hence removing a significant element of privacy. While there may be benefits in terms of increased auditability, accountability and productivity, reduced theft, fewer security breaches, and improved employee safety (e.g. evacuation of buildings based on precise knowledge of who is where), these may be outweighed by the disadvantages. For instance, identity theft and cloning of employee data may be possible if the RFIDs are still active outside the place of employment. The loss of anonymity in movement may stifle innovation as employees may have fewer serendipitous encounters with other employees. Finally the integration of RFID data with other surveillance technologies may instill a sense of fear in the workforce, which may reduce co-operation with, and loyalty to, the employer.

This section has reviewed the characteristics of RFIDs in general and has also considered some of the broad implications of their application. The next section looks at their use in libraries.

2. The impact of RFIDs in libraries

In the library context RFIDs are being marketed as providing a number of benefits which will lead to greater operational efficiency and improvement in service quality. Engels (2006) identified the following expected or actual benefits from a survey of 27 public and academic libraries:

- Patron self-checking, which should reduce the levels of staff required for issue desks.
- Increased patron satisfaction as a consequence of less queuing.
- Improved stock security, as non-issued items will be more readily detected.
- Tracking of misfiled items of stock, as the presence or absence of an item in an area will be more readily achieved.
- Improved inventory management, as stock-checking can be achieved more rapidly and comprehensively.
- Reductions in staff injuries (e.g. repetitive strain injury), as there will be less physical handling of books.
- Reductions in lines at circulation desks as self-checking will divert some book issues and the remaining issues can be booked out more rapidly.
- Release of staff from circulation desks to undertake more professional activities.

To these we may add:

- Automated sorting of returned books to speed up the return of stock to shelves.
- Improved safety of employees as they can be more readily located in emergencies.
- Enhanced patron privacy through self-service.
- Improved location and removal of editions with (e.g. dangerous) errors.
- Improved management of consumables and retail stock.

- Greater auditability of the usage of photocopying in order to comply with copyright legislation.
- Improved identification of shortages in deliveries as whole consignments can be scanned and matched to orders immediately on arrival.
- Prevention of the lending of adult material to minors.
- Ability to scan boxed material (e.g. archives) without opening the boxes.

A report from the San Francisco Public Library Technology and Privacy Advisory Committee (2005) is interesting in that it demonstrates a proactive approach by policy makers towards determining the ethical, and other, issues related to the adoption of RFIDs. In order to address issues which are raised by new technologies in general San Francisco applies a Precautionary Principle to decision-making in the absence of full scientific certainty which incorporates anticipatory action, the right to know, assessment of alternatives, full cost accounting and a participatory decision process. The key benefits anticipated by LTPAC with respect to the implementation of RFIDs were:

- Reduced time spent on circulation tasks.
- Increased patron privacy (as self check-out could be supported).
- Improved shelf collection management.
- Reduction in tedious aspects of some tasks for staff.
- Improved materials management.
- Reduced incidence of theft.
- Expanded security through use of more flexible RFID gates.
- Reduced rate of repetitive strain injuries (RSI).

However studies have also identified a number of disadvantages associated with the application of RFIDs in libraries. Garofoli and Podger (2007) highlight public concerns regarding the San Francisco Public Library's proposal to tag its book stock in order to deter theft, track materials and check out books faster. The concerns expressed by the public primarily revolved around the potential for inferences to be made about life-style, sexual orientation, politics, etc., based on their reading habits.

San Francisco LTPAC also identified a number of potential disadvantages. There were particular concerns that RFIDs might contravene the American Library Association's (ALA) Library Bill of Rights (based on First Amendment rights) which states that "the right to privacy is the right to open enquiry without having the subject of one's interest examined or scrutinized by others." The interpretation given is that "regardless of technology used, everyone who collects or accesses personally identifiable information in any format has a legal and ethical obligation to protect confidentiality." The ALA adopted a resolution regarding RFIDs and privacy in 2005.

There were ancillary concerns that the means to monitor the reading habits of an individual may compromise free speech as free speech depends on a right to read with relative anonymity. Related legislation in the United States is the Video Privacy Protection Act which requires a court order before rental records can be released. California law also protects the privacy of circulation records, except: those related to fines (presumably for audit purpose); access for library administrative purposes; written authorisation from a borrower; instruction by the supreme court. Libraries should therefore only store a unique identifier on a RFID, rather than full bibliographic data which could inform other individuals with a compatible reading device about the reading habits of the borrower. Unlike retailers the book is lent, rather than sold, and the RFID needs to be kept live as it is never the borrower's property. There are however concerns that this could compromise privacy as a motivated individual could obtain information about a borrower's movements.

Health concerns focus on the effects of electromagnetic frequencies which have attracted attention with respect to other technologies (mobile phones, electricity lines, etc.). Health issues can be broken down into thermal effects (i.e. as in a microwave oven) and non-thermal effects (e.g. cancer inducing rays). Neither of these is seen as an issue based on current research, though it is acknowledged that more is needed.

3. A process view of RFID issues

Processes represent one of the key capabilities of an enterprise and are crucial to the delivery of value, which may be economic, social or informational in nature, to the customer. A process view of an enterprise is an essential step towards the effective design and implementation of information systems and services. It also provides a context within which governance issues, such as ethical policies, can be analysed and understood. While a functional structure is necessary to define reporting lines and to organise physical assets, it does not provide a picture of how various elements of an enterprise must co-operate in order to provide a service and achieve customer satisfaction. There is an obligation on managers and operational staff to ensure that each process is conducted in an efficient, effective and consistent manner and that this happens within an agreed set of organisational norms and policies. This will involve the use of business rules to guide decisions and sign-off points during the execution of the process. The librarian therefore has an important role to play as an agent in linking the customer to appropriate information resources. There is also an important role for library managers to ensure that the processes, and by implication their outputs, are informed by and conform to an ethical framework.

The general characteristics of any process (Gibb, Buchanan, & Shah, 2006) are that it:

- has customers (external or internal);
- crosses organisational and functional boundaries (external or internal);
- has inputs and outputs from many parts of the enterprise;
- is highly information and IT dependent.

The key processes of a library and information service are depicted in Fig. 1 using the following typology:

- transaction processes;
- production processes;
- governance processes;
- interaction processes;
- facilitation processes.

Each specific process can be analysed in terms of the issues that have been identified above and others derived from a more detailed analysis of the implications for ethical behaviour and, in particular, privacy. Some of these issues are neutral with respect to RFIDs, others have an immediate link. In the tables below a **Yes** indicates that there is an issue that must be addressed with respect to RFIDs; a **Neutral** indicates that there is not a specific issue with respect to RFIDs, though the issue will still need to be considered within wider library policy.

3.1. Transaction processes

Transaction processes are concerned with servicing external customers, e.g. fulfilling orders, handling queries, etc., and involve direct engagement with customers. Transaction processes should make the enterprise distinctive and/or characterise the sector in

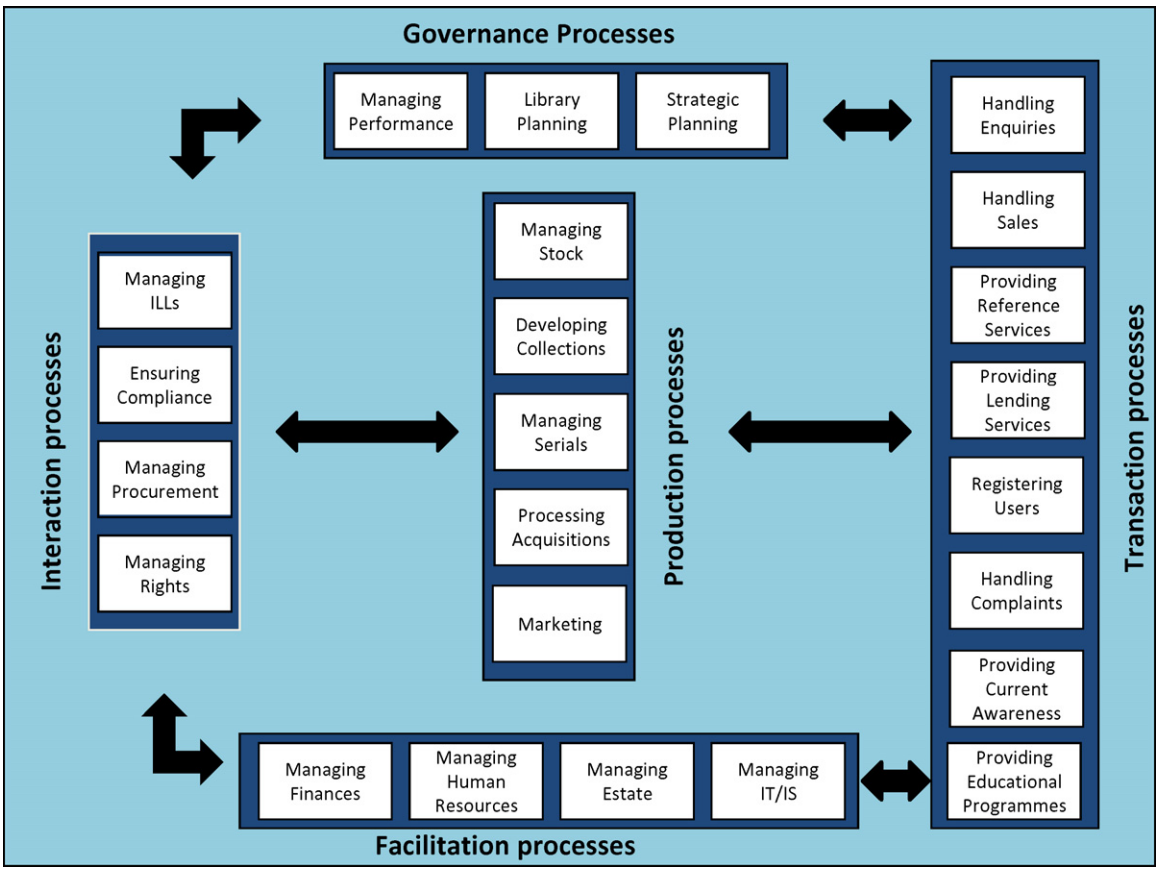

Fig. 1. Process map for library and information services.

which it operates, and are also customer-sensitive: they are visible to the customer, and customer demands and satisfaction are key drivers for configuring and improving these processes. Table 1 summarises the issues related to ethics and privacy with respect to these processes and indicates the immediate relevance to RFID implementations. Issues which have been identified as being relevant to RFID implementations have been numbered; these numbers are used as shorthand references in the analysis section (Fig. 2).

Likelihood \ Impact	Low	High
High	7	25, 26	4
	24	12, 23, 27	3, 21, 22 30, 31, 33
Low	2, 6, 10 11, 16, 17, 18, 37	13, 19, 21 34, 35	1, 5, 8 9, 14, 15, 20, 28, 29, 32, 36

Fig. 2. Ethical risk matrix (numbers refer to issues identified in Tables 1–5).

3.2. Production processes

Production processes encompass essential behind the scenes activities which feed into transaction processes, and involve the design, creation and management of both physical and informational products and resources. Table 2 summarises the issues related to ethics and privacy with respect to these processes and indicates the immediate relevance to RFID implementations.

3.3. Governance processes

Governance processes provide the direction, oversight and context within which other processes take place and are concerned with planning, organising and overseeing the enterprise. These processes are market-sensitive: they are concerned with strategic direction and developing an enterprise that is responsive to external change and which has the competencies necessary to deliver its vision. The key drivers are competitive positioning, regulatory regimes and the availability and development of intellectual capital. Table 3 summarises the issues related to ethics and privacy with respect to these processes and indicates the immediate relevance to RFID implementations.

3.4. Interaction processes

Interaction processes cross the boundaries between enterprises and link partners in a supply chain, including funding and sponsoring agencies, and co-operating and collaborative partners. These processes are supply-sensitive: they are concerned with facilitating the exchange of resources between partners to guarantee the delivery of a product or service to the end-customer. The key drivers are reliability and sustainability of business relationships, the avail-

Table 1
Transaction process issues.

Process	Issue	Relevance to RFID implementations?
Registering users	Collection of personal details recorded through registration	Yes – 1
	Possible incorporation of user information with smartcards which could be read beyond library operations	Yes – 2
	Exclusion of readers on the basis of external information (e.g. paedophiles denied access to children's libraries).	Neutral
	Incorrect information held about a user.	Yes – 3
Providing lending services	Profiling of user reading habits and behaviour based on lending records.	Yes – 4
	Infringement of the right of a user to anonymity with respect to freedom of thought and speech.	Yes – 5
	Chains of borrowing could be established and hence implicit links between borrowers.	Yes – 6
	Materials could be tagged on the basis of content which could be suppressed or access controlled.	Yes – 7
	Access to services might be impossible by default if a user is unwilling to comply with RFID technology.	Yes – 8
	Obligations to the state and law enforcement agencies with respect to the release of data.	Yes – 9
	Incorrect information might be held about an item (reader could be associated with a title which is incorrect).	Yes – 10
	Modification of tags by users.	Yes – 11
	Removal or deliberate damage to tags by users.	Yes – 12
	Suppression of tag capability by users.	Yes – 13
Providing reference services	Recording of enquiries on sensitive topics.	Neutral
	Obligations to the state and law enforcement agencies with respect to the release of data.	Yes –14
	Correctness of information held about an enquiry.	Neutral
	Profiling of user reading habits and behaviour based on use of open access web services.	Neutral
	Profiling of user reading habits and behaviour based on tracking of usage of non-lending material.	Yes – 15
Providing current awareness services	Profiling of user reading habits and behaviour based on records of user preferences and information needs.	Neutral
	Obligations to the state and law enforcement agencies with respect to the release of data.	Neutral
Handling enquiries	Recording of enquiries on sensitive topics.	Neutral
	Obligations to the state and law enforcement agencies with respect to the release of data.	Neutral
	Incorrect information may be recorded about an enquiry.	Neutral
Handling sales	Profiling of users based on transaction records.	Yes – 16
	Potential to track users outside of library through active RFIDs.	Yes – 17
	Employee information might be advertised on receipts.	Neutral
Handling complaints	Discouraging complaints by recording of customer objections to pervasive technologies such as RFID.	Yes – 18
	Discouraging complaints by recording of customer complaints regarding stock and service provision.	Neutral
Providing educational programmes	Imbalance of access and provision for groups with special requirements.	Neutral

Table 2
Production process issues.

Process	Issue	Relevance to RFID implementations?
Developing collections	Censorship and social engineering through collection management.	Neutral
Processing acquisitions	Inadequate de-accessioning procedures for items removed from stock which can be identified in perpetuity.	Yes – 19
Managing stock	Profiling of user reading habits and behaviour based on records from smart shelves (what they refer to rather than just what they borrow).	Yes – 20
Managing serials	Profiling of user reading habits and behaviour based on usage of individual volumes and issues (and in an e-library, individual articles) which provides greater detail with respect to consultation and subject matter (serials are often just referred to and copied, rather than borrowed).	Yes – 21

ability of technologies to support information interchange, and the reduction of transaction costs. Table 4 summarises the issues related to ethics and privacy with respect to these processes and indicates the immediate relevance to RFID implementations.

3.5. Facilitation processes

Facilitation processes are concerned with servicing internal customers and transaction and production processes through the provision of infrastructural activities, e.g. managing finances, purchasing, etc. Facilitation processes are common to many enterprises and therefore provide little, if any, distinctiveness. These processes are resource-sensitive: the key driver is efficiency as they do not, in themselves, generate value. These processes are candidates for outsourcing, as third parties, such as book distributors, may be able to achieve lower operating costs through economies of scale. Table 5 summarises the issues related to ethics and privacy with respect to these processes and indicates the immediate relevance to RFID implementations.

Table 3
Governance process issues.

Process	Issue	Relevance to RFID implementations?
Strategic planning	Policies which do not incorporate principles of notice and consent, choice and control.	Yes – 22
	A lack of application of, and education in, professional ethics and standards.	Yes – 23
Library planning	Inadequate planning of the location of readers for stock management and security.	Yes – 24
Managing performance	Service level agreements or specifications which do not make the ethical aspects of RFIDs explicit.	Yes – 25
	Service level indicators related to ethical conduct are not monitored and measured as rigorously as other indicators.	Yes – 26
Marketing	Ineffective promotion and statement regarding role, etc., of library services which incorporate RFIDs.	Yes – 27

Table 4
Interaction process issues.

Process	Issue	Relevance to RFID implementations?
Ensuring compliance	Inadequate compliance with DPA requirements.	Yes – 28
	Inability to identify, contain and address any breaches of DPA.	Yes – 29
	Inability to demonstrate that professional ethics and standards are defined, implemented and audited.	Yes – 30
Managing procurement	Requests for particular books could be linked through user records.	Neutral
Managing inter-library loans	Recording of requests on sensitive topics.	Neutral
	Amending tags on items from lending partners.	Neutral
Managing rights	Inability to audit loans of materials.	Neutral
	Inadequate policing of fair use copying.	

Table 5
Facilitation process issues.

Process	Issue	Relevance to RFID implementations?
Managing human resources	Employees may be unaware that they are being monitored in terms of where they are, how long they are there, and what they do.	Yes – 31
	Tagged employee cards that control access to restricted areas could place them in danger.	Yes – 32
Managing IT/IS	The exposure or alteration of personal information as a consequence of inadequate security measures.	Yes – 33
	The corruption or loss of data as a consequence of inadequate back-up mechanisms.	Yes – 34
	Denial of access to services as a consequence of inaccurate data.	Yes – 35
Managing estate	Inappropriate location of RFID readers (i.e. would it be appropriate to place them in rest rooms?).	Yes – 36
Managing finances	Access to tills and petty cash may be linked to individual employees as part of log-on procedures.	Yes – 37

4. Conclusions

What then should be the priorities for librarians and library managers? In risk management events are often assessed in terms of the likelihood of the event occurring and the associated business impact, leading to the calculation of a risk score (Gibb & Buchanan, 2006). However computing scores in the context of ethics seems inappropriate and therefore a qualitative approach has been adopted to assess the issues identified in the tables above, where they are judged to be relevant to the application of RFID technologies. A matrix analysis has been used in which the criteria of likelihood and impact and have been employed to position the issues relative to each other. Likelihood has been interpreted as a measure of how likely an issue is to convert from a possibility to an event with which a librarian will have to deal, while impact has been interpreted as the seriousness of the outcome of the event to any of the stakeholders involved. As context will vary from enterprise to enterprise, and jurisdiction to jurisdiction, the assessments should be taken as indicative and are based on the opinions of the authors and informal discussions with practitioners.

Based on this analysis the following issues are highlighted as being of particular importance as they can be characterised in terms of strong combinations of likelihood and impact:

Profiling of user reading habits and behaviour based on lending records.
Incorrect information held about a user.
Profiling of user reading habits and behaviour based on usage of individual journal volumes.
Policies which do not incorporate principles of notice and consent, choice and control.
Inability to demonstrate that professional ethics and standards are defined, implemented and audited.
Employees may be unaware that they are being monitored in terms of where they are, how long they are there, and what they do.
The exposure or alteration of personal information as a consequence of inadequate security measures.
Service level agreements or specifications which do not make the ethical aspects of RFIDs explicit.
Service level indicators related to ethical conduct are not monitored and measured as rigorously as other indicators.

A second group of issues can also be identified which should not be ignored as, while they are judged to be unlikely to occur, the

impact in ethical, financial and reputational terms may be high.

Potential exposure of personal details recorded through registration.
Infringement of the right of a user to anonymity with respect to freedom of thought and speech.
Access to services might be impossible by default if a user is unwilling to comply with RFID technology.
Obligations to the state and law enforcement agencies with respect to the release of data.
Profiling of user reading habits and behaviour based on tracking of usage of non-lending material.
Profiling of user reading habits and behaviour based on what they refer to rather than just what they borrow.
Inadequate compliance with DPA requirements.
Inability to identify, contain and address any breaches of DPA.
Tagged employee cards that control access to restricted areas could place them in danger.
Inappropriate location of RFID readers.

RFIDS have the potential to deliver gains in efficiency and effectiveness which, particularly in a climate of financial cutbacks and re-prioritisation of services, can be helpful to any library manager. However they also, like many new technologies, introduce new management challenges. From an ethical perspective librarians can be considered to have a duty of care to their customers in terms of protecting their interests, as far as is practicable, and a duty of confidentiality in particular with respect to the data that is held about those customers concerning their transactions with the library. Many of the issues raised by RFIDs may be seen as merely extensions of existing challenges: we already record data about customers; we have already had requests for such data from security services; we already assume that some customers will not conform to library regulations and need to secure the library against any breaches. However, we should accept that RFIDs have the potential to be more invasive, intrusive and pervasive, while being less visible, and that they also offer greater detail and granularity of data. Other issues may be seen as somewhat hypothetical or rather unlikely: RFIDs can be tracked outside the library but the distances over which they operate are very short and it would probably be simpler to look over a customer's shoulder to ascertain their reading habits; reader profiles might be built up from transaction data but this could be avoided by separating user and information object data and by only maintaining a link between the two during the period of the loan, as recommended in the American Library Association's RFID guidelines (2006). Finally we have to recognise that the library manager has prime responsibility for what occurs inside the library and that it is difficult to control or predict what will happen once the customer has left the building: information objects, employees and customers are mobile and therefore move between jurisdictions.

Nevertheless it will be essential for the library manager to extend and enhance training and education of users and employees to ensure that there is a shared understanding of the role of RFIDs and a commitment to ensuring that that role is focused on delivering customer benefits, i.e. that the trade-offs are weighted heavily towards customers and their needs. Minimal coercion may have to be accepted (i.e. that a service may not be able to operate universally at an economically acceptable level unless the technology is adopted) but that decision should not be taken lightly. The customer needs to be fully informed about such decisions and must expect greater flexibility in service provision and be assured of the protection of personal data in return. The operational imperatives ("does this work?") should not be allowed to over-ride the ethical ones ("does this work appropriately?") as the library profession has long maintained a noble tradition of freedom of thought and freedom of access.

References

American Library Association. (2006). *RFID in libraries: Privacy and confidentiality guidelines*. Available from http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=130851 Accessed 01.3.2010

ANEC and BEUC. (2007). Consumer's scenarios for a RFID policy. *Joint ANEC/BEUC comments on the communication on radio frequency identification (RFID) in Europe: Steps towards a policy framework* (x/31/2007-03/07/07; ICT-2007-G-059).

Cavoukian, A. (2004). *Tag, you're it! privacy implications of radio frequency identification (RFID) technology*. Ontario: Information and Privacy Commissioner.

Engels, E. (2006). *RFID implementation in California libraries: Costs and benefits*. Sacramento: California Library Association. Available from http://www.cla-net.org/included/docs/IT3.pdf Accessed 01.03.2010

Foster, K. R., & Jaeger, J. (March 2007). RFID inside: The murky ethics of implanted chips. *IEEE Spectrum*, 24–29.

Garofoli, J., & Podger, P. J. (2007, October 6). Ethics of library tag plan doubted. *San Francisco Chronicle*.

Gibb, F., & Buchanan, S. (2006). A framework for business continuity. *International Journal of Information Management*, *26*(2), 128–141.

Gibb, F., Buchanan, S., & Shah, S. (2006). An integrated approach to process and service management. *International Journal of Information Management*, *26*(1), 44–58.

Gruber, J. (2005). *RFID and workplace privacy*. Princeton: National Workrights Institute. Available from http://www.workrights.org/issue_electronic/RFIDWorkplacePrivacy.html Accessed 01.03.2010

Kelly, E. P., & Ericson, G. S. (2005). RFID tags: Commercial applications v. privacy rights. *Industrial Management and Data Systems*, *105*(6), 703–713.

Mohan, A., Woo, G., Hiura, S., et al. (2009). Bokode: Imperceptible visual tags for camera basd interaction from a distance. *ACM Transactions on Graphics*, *28*(3), 1–8.

NISO RFID Working group. (2008). *RFID in US libraries*. Baltimore: NISO. (NISO-RP-6-2008) Available from http://www.niso.org/publications/rp/RP-6-2008.pdf Accessed 01.03.2010

Paskin, N. (2008). *Digital object identification (DOI) system*. Oxford: Tertius Ltd. Available from http://www.doi.org/overview/080625DOI-ELIS-Paskin.pdf Accessed 01.03.2010

Sade, R. M. (2007). *Radio frequency ID devices in humans*. Chicago: American Medical Association. (CEJA Report 5-A-07).

San Francisco Public Library Technology and Privacy Advisory Committee. (2005). *Radio frequency identification and the San Francisco public library*. San Francisco: LTPAC.

Schuman, E. (2005). The ultimate privacy argument against RFID. *CIO Insight*, 21st October. Available from http://www.cioinsight.com/c/a/Past-Opinions/The-Ultimate-Privacy-Argument-Against-RFID/ Accessed 01.03.2010

Van't Hof, C., & Cornelissen, J. (2006). *RFID and identity management in everyday life*. Hague: European Technology Assessment Group. Available from http://www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf Accessed 01.03.2010

Zetter, K. (2005). *School RFID plan gets an F. Wired.* , 10th February. Available from http://www.wired.com/politics/security/news/2005/02/66554 Accessed 01.03.2010

Forbes Gibb is Professor of Information Science in the Department of Computer Science at Strathclyde University.

Clare Thornley is a lecturer at the School of Information and Library Studies, University College Dublin and has an academic background in Information Retrieval (IR) and Philosophy. Principal research interests are the use of philosophy of language in information science, and information ethics.

Stuart Ferguson is an Assistant Professor in Information Studies, Faculty of Arts and Design, University of Canberra. Principal research interests are application of knowledge management frameworks in organisations, and information ethics.

John Weckert is Professor of Computer Ethics, School of Humanities and Social Sciences, Charles Sturt University, and a Professorial Fellow at the Centre for Applied Philosophy and Public Ethics (CAPPE).