How do libraries manage the ethical and privacy issues of RFID implementation? A qualitative investigation into the decision-making processes of ten libraries

Authors

Stuart Ferguson
(Faculty of Arts and Design,) University of Canberra, Australia

Clare Thornley
(School of Information and Library Studies,) University College Dublin, Ireland

Forbes Gibb
(Department of Computer and Information Sciences,) University of Strathclyde, UK

Corresponding author:
Stuart Ferguson, Faculty of Arts and Design, University of Canberra, ACT 2601, Australia.
Email: stuart.ferguson@canberra.edu.au

Abstract

This paper explores how library managers go about implementing RFID (radio frequency identification) technology and particularly how associated privacy issues have been managed. The research methodology consisted of a literature review, theme identification, interview scheduling, interviews and interview analysis. The sample was ten libraries or library networks and eighteen participants. Findings covered the main drivers of RFID development, perceived benefits, tag data, data security, levels of ethical concern, public consultation, potential impact of technological developments on ethical issues, and managers' sources of ethical decision-making. Analysis of potential ethical issues was not found to be a central part of the process of implementing RFID technology in the libraries. The study sees RFID implementation as an informative example of current practice in the implementation of new technologies in libraries and suggests that we look at management structures and decision making processes to clarify where responsibility for ethical considerations should lie.

Keywords

RFID; Radio Frequency Identification Technologies; Ethics; Library Technology; Privacy

Introduction

This paper explores how librarians and library managers implement RFID (radio frequency identification) technology, with particular reference to how ethical issues have been managed and whether ethical issues such as the right to privacy have been considered by those responsible. The study builds on earlier work on privacy aspects of RFID implementation in libraries (Gibb et al., 2011; Thornley et al., 2011) and seeks to discover how library and systems managers implement a new technology such as RFID; whether they were conscious of any ethical issues; what frameworks, ethical or otherwise, informed their decision making; and, if they did encounter ethical issues, how they addressed them. While the focus stays on potential ethical issues associated with the use of RFIDs in libraries, the study may have broader implications for the implementation of many new technologies.

The role of technology in raising new ethical issues, in particular the invasion of privacy, has been widely discussed in the academic literature and public awareness is reflected in increased scrutiny of major companies. For instance Google has encountered widespread concerns following its implementation of a new privacy policy (Arthur, 2012) and revelations that it has scanned personal computers, tracked iPhones (Angwin & Valentino-Devries, 2012), scanned wireless connections when collecting data for street view (Ionescu, 2010), and used pictures of house numbers as security checks (Hall, 2012). Similar challenges have been encountered with Facebook, which has alienated some users through changes to its security settings (Rogers, 2012) and the uploading of information from people's phones (van Grove, 2012), which has also been an issue for Apple.

RFID technology presents particular issues because it consists of small, often non-visible, chip-based devices (RFID tags) that can store data, which can be used to identify objects uniquely, and can be 'read' from a distance by an appropriate device. This latter characteristic, which allows digitally stored data to be read outside line of sight, has many benefits but it also raises potential privacy concerns because an RFID tag could be read by someone with an unauthorised RFID reader without the knowledge of the possessor of the tagged object.

While recognising that RFIDs have great potential to improve the life of citizens, a report from two European consumer bodies highlighted six main areas of concern with RFIDs, including privacy and the potential for tracking, profiling and discrimination (ANEC & BEUC, 2007). Tracking involves following consumers' movements through detection of an RFID tag in their possession, while profiling is the compilation of a composite picture of consumers from a variety of sources. Public awareness of potential privacy breaches has been raised by well-publicised cases involving companies such as Benetton, Gillette, Prada and Proctor & Gamble (Cadoo & Cadoo, 2004; Cavoukian, 2004; Lockton & Rosenberg, 2005). Such breaches can have significant financial, reputational and legal implications as consumers highlight their concerns through social media sites and government bodies appear more willing to take action. The Article 29 Working Party (an EU body tasked with advising on data protection) has highlighted the need to assess the implications of RFID implementation, suggesting that consent might be required from individuals (European Commission, 2011).

RFIDs raise two main privacy concerns in the library environment, both relating to the increased risk of surveillance, through the greater capacity to track items, and through the potential for 'hot-listing'. Hot-listing refers to the compilation of a list of 'hot' or dangerous publications (such as books on jihad or bomb-making) and checking who has borrowed or otherwise used these items. The latter goes beyond what many citizens may find acceptable and raises ethical issues about the right to privacy for library users. The circumstance under which this privacy may be invaded could exist, for example in the case of a serious security threat, but the process of ascertaining and judging these circumstances is complex. We argue that librarians need to maintain a critical engagement in the ethical issues raised by these processes rather than just concerning themselves with staying within the legal framework. The right to privacy is not absolute and the state and legal system have the major role in making judgements on this matter, but librarians also, as experts in information and its use, have a role to play in both policy and practice formation. It is one thing for security forces to have suspicions about an individual and to seek a court order, for instance, to examine their library records, but another to perform random checks on individuals based on their use of reading material that has been flagged as ‘dangerous’. The potential to track items refers to using RFIDs to identify the location and movement of books and, by implication, library users who are currently reading them.

Unlike the retail sector there are, as yet, no reports of privacy breaches in the library sector, but there has been publicity about privacy issues, most famously in the case of the San Francisco Public Library's RFID implementation (Garofoli & Podger, 2007), which raised public concerns around the potential for inferences to be made about readers' life-styles, sexual orientation, politics and so on, based on data held about their reading habits. This could lead to prosecution under local data protection legislation, fines and possible loss of donations from patrons. In reputational terms such a breach threatens the trust that libraries generally enjoy in the wider community (Coombs, 2004, p.495) and the values for which librarians and their professional associations stand. Indeed, privacy concerns over RFID implementation were sufficient to prompt the American Library Association to produce a set of guidelines (ALA, 2006), which, if followed, cut – but do not eliminate – the potential for privacy breaches significantly.

However, advocates of the technology claim that such concerns are exaggerated, primarily for technical reasons. It is noted that the great majority of libraries use HF (high frequency), 13.36 MHz tags, which have a maximum read distance of around one metre (sufficient to make their use as security tags feasible). These are 'passive' tags, with no power source of their own (in contrast to the more expensive 'active' tags used in retail applications) and reliant on a signal from the reader to send any data. As a consequence, advocates argue that the risk of tracking is not serious (Butters, 2007; Chacra & McPherson, 2003; cited in Palmer, 2009). To all extents and purposes RFID technology would appear to be confined for the present to tracking item use within the library and not once it has left the building.

Second, advocates argue that the data stored on RFIDs is generally restricted to unique identifiers and status codes, which means that, even if someone with an unauthorised reader could get close enough to read a tag, they would need to hack into the Library Management System (LMS) in order to identify the item (Palmer, 2009, p.55). Indeed if, for example, the security forces really wanted to spy on library borrowing habits (and readers should make their own judgement about how likely that is) then they could hack straight into the LMS and, as Palmer states (2009, p.55), 'it might reasonably be argued that the involvement of RFIDs is, to a large extent, incidental', though it should be noted that hotlisting does not require hacking into the LMS (see below).

Arguments based on the technical limitations of the current RFID technologies used in libraries, however, are not entirely convincing because technologies change. Surreptitious surveillance using RFIDs may be difficult – although not impossible – but such surveillance would become easier should the tag read distances be increased. At present this is unlikely but it is worth noting that read distances depend not only on the tags, but also on the readers, and that improvements in reader technology could conceivably increase read distances (Palmer 2009, p.54). Moreover, one needs to factor in changes in the market. There has been some interest in Ultra High Frequency (UHF) RFIDs, which would provide greater read ranges (Butters, 2008), and the ease with which they can be accessed has been demonstrated by researchers (Zanetti, Sachs & Capkun, 2011). One needs to ask whether library managers who have implemented RFIDs are likely to re-evaluate the benefits and ethical risks, if offered the new 'improved' tags at a competitive price. In addition, the potential to collect aggregate data from multiple RFIDs in the possession of an individual still exists, as does the possibility of storing more than just a unique identifier, which implies that libraries must be explicit about what data they store and consider what the consequences might be.

Indeed, one of the premises of this study is that, when considering new technologies from an ethical perspective, one needs to anticipate the ethical issues and not ground one's judgement in current technological limitations. Palmer notes that consumer bodies such as Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) and Electronic Frontier Foundation (EFF) have been concerned about RFIDs in libraries but significantly less with current possibilities 'and more with what might be feasible in the future as the technology develops' (Palmer, 2009, p.54).

It is also assumed that ethical issues are a matter of professional concern in the library sector, as evidenced, for instance, in the International Federation of Library Associations and Institutions' *Code of Ethics*, which states 'The relationship between the library and the user is one of confidentiality and librarians and other information workers will take appropriate measures to ensure that user data is not shared beyond the original transaction' (IFLA, 2012, p.3). Privacy is an ethical issue, not simply a legal one, and requires librarians who seek to behave professionally to make every reasonable effort to ensure that new technologies do not have potential to harm their clients, with whom they enjoy a position of trust.

This paper seeks to throw light on the management of the privacy issues posed by RFIDs in libraries partly by means of a literature review and partly through a research project that investigated several cases of RFID implementation. The project sought to establish how library and systems managers went about the implementation, whether they noted any privacy issues and, if so, how they addressed the matter. It is intended that the findings and discussion will provide a clarification of ethical issues associated with RFID technology, strategies for the management of these issues, and some measure of the impact of technological changes on both ethical and management issues. They may also have implications for professional associations in terms of providing information on the relevance of their current ethical guidelines. It is also hoped that the issues raised can feed into the process of implementing any new technology in the library context since they demonstrate the awareness and decision-making of librarians when dealing with potential concerns.

Literature review

Privacy concerns over RFID technology in the library sector have been fuelled by those raised in other sectors, especially retail (Garofoli & Podger, 2003). According to Palmer (2009, p.53), it was early adoption of RFIDs in retail that alerted CASPIAN, for instance, to potential issues in libraries. Palmer suggests (2009, pp.5-7) that much of the concern about the potential to enable privacy invasions stems from a tendency to lump a variety of RFID technologies together, arguing that RFIDs would be better thought of as a range of technologies, employing active or passive tags and a number of different frequencies – the main ones being Low Frequency, High Frequency (the frequency most commonly used in library applications), Ultra High Frequency (with a read range for active tags of up to 100 metres) and Microwave – with each technology performing quite differently (see also Butters, 2008, p.120). It would follow that well-publicised privacy breaches in the retail sector should not necessarily cause concern in the library world.

The case of San Francisco Public Library, noted earlier, is the most cited example in the library sector. San Francisco established a Library Technology and Privacy Advisory Committee (LTPAC) prior to RFID implementation, with a view to determining ethical and other issues. This represents the application of a 'Precautionary Principle' to the adoption of new technologies, one that, in the absence of full scientific certainty, incorporates anticipatory action, the right to know, assessment of alternatives, full cost accounting, and a participatory decision process (San Francisco Public Library Technology and Privacy Advisory Committee, 2005).

The LTPAC identified a number of potential disadvantages, including the concern 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' (ALA, 2002) – again, a principle that lies at the heart of the values librarians espouse.

Privacy concerns in the library sector led the ALA to produce a set of best practice guidelines, including use of the most secure means available to protect the data on RFID tags, limitation of the data stored on a tag to a unique item identifier, notification of the public about a library's use of RFID technology, and the training of library staff on privacy issues (ALA, 2006). The US standards body, the National Information Standards Organization (NISO), took privacy seriously enough to recommend that libraries use passive HF tags and that the read range for library applications should not be substantially increased (NISO, 2007, p.viii). It is worth noting, however, that the 2012 version of the NISO document mentions library implementations of ultra-high frequency (UHF) tags in Singapore, Australia and Hong Kong, projects in mainland China and interest from two US libraries (2012, p.50).

A US survey of two subgroups of librarians, public librarians and 'technology-oriented' librarians (Strickland & Hunt, 2005) suggests some privacy concerns in the sector. Although the findings are limited by the fact that the survey was not specifically about library applications, they did identify that there was no substantive understanding of the technology amongst either group surveyed, and that there was a greater concern for privacy than for security, overwhelming support for some form of federal regulation of the use of RFIDs and wariness of industry self-regulation (Strickland & Hunt 2005, pp. 228-231).

It may be significant that most of the literature expressing concern over privacy issues and RFIDs has come from the US. Palmer (2009, p.135) sees 'remarkably little concern' in Europe, while a Standards Australia working party (2006) also refers to a consensus view in the Working Party that the level of concern in Australia was relatively low', suggesting that this may reflect 'a lack of real awareness on the part of library sector' (Standards Australia Working Party, 2006, p.2)

Part of this may be the socio-political context. NISO (2007 p.37) refers to the tangled situation in the US and sees one of the factors as the USA Patriot Act, which significantly reduced both the perception and the reality of personal privacy with respect to what it calls government 'snooping'. Molnar and Wagner (2004, p.213) point out that 'Hotlisting is not a theoretical attack' and 'recall FBI warnings regarding almanacs as an indicator of terrorist activity' (they cite an FBI memo from 2002). Preer (2008, pp.196-197) refers to the FBI targeting academic libraries, looking for a generic suspect, and points out (2008, p.201) that the USA Patriot Act explicitly mentions library records. Indeed, Muir (2007 p.99) cites a 2005 case in which an organisation in Connecticut received a USA Patriot Act request from the FBI to hand over library patron records.

As noted already, proponents of RFIDs in libraries typically cite two important technical barriers to 'snooping', namely, the short read distances of the passive tags typically used in the library environment and the lack of customer information on the tags (Mehrjerdi, 2011 p.41). Issues of tracking and privacy were raised in two of the questions to a 2010 Webinar, 'The Power and Pitfalls of RFID Webinar' and received the standard response that the read distances are very short and that only barcode numbers are encoded on tags and that these do not appear in the catalogue.

The other common argument from proponents is that, while there are slight risks, the benefits are substantial. Such benefits, for example reduced costs and increased efficiency, have been well covered in the literature (Engels, 2006; Gibb et al., 2011) and do not need to be repeated here. However, the 2012 NISO recommendations include protection of 'the personal privacy of individuals while supporting the functions that allow users to reap the benefits of this technology' (2012, p.v). This is an interesting ethical dimension for librarians: should increased convenience and reduced cost be seen as sufficient benefit to take some privacy risks? RFIDs, may, for example, allow opening hours to increase or prevent library closure for small libraries.

It is also worth noting the counter-claim that RFIDs can actually enhance client privacy since 'using self-checkout means that no judgmental decisions by a staff member or clerical staff will be encountered, and no further explanation of what one is reading or why one is reading it will be necessary' (Zimerman, 2011, p.149). Coyle points out, however, that simply ‘adding self-check machines’, thereby cutting or even eliminating circulation staff, without providing extra services , risks being 'seen by users as a mere shifting of the burden of checkout from the library to the users themselves', with RFID technology becoming the 'ATM of the library world' (Coyle 2005, p.488).

From a technical perspective, there is concern that a determined user would be able to intercept RFID signals (Ayre 2004; Molnar & Wagner 2004; Archer 2007; Muir 2007; Cai et al., 2009). In one of the most cited papers, Molnar and Wagner (2004) argue that there is no guarantee of client privacy, even if libraries limit tag data to a barcode number and barcode numbers are not publicly available on the bibliographic database. Barcode numbers are static identifiers therefore hotlisting is feasible because any agency wanting to compile and use a hotlist would need only to visit the library in order to read the tags on hotlisted items, a point Molnar and Wagner demonstrated experimentally (2004). Molnar and Wagner's (2004) solution is Random Transaction IDs on Rewritable Tags but there is no sign that this is supported in any library RFID systems. In proposing a new RFID authentication protocol, Moessner and Khan (2012, pp.273-274) emphasise the relative ease with which a 'malicious party' can find a way around existing protocols; second, the need to embed an authentication protocol within the existing EPC global infrastructure, if costs are to be kept sufficiently low; and, third, the fact that several of the existing approaches to RFID authentication 'cannot be embedded with the EPC global standards'.

It is also worth noting that if one's ethical concerns extend to *potential* for privacy breaches then librarians need to be aware of the implications of buying books that have already been tagged earlier in the books' lifecycles. NISO recommendations include promotion of procedures that allow RFID tags to be used throughout the lifecycle of a book by publishers, printers, distributors, vendors, libraries, inter-library loan borrowers and second-hand bookshops (2012, p.v). Ayre (2012, p.17) supports such a development, pointing to the benefits in terms of improved library processes such as item processing, inter-library loans and acquisitions.

In the event of such cooperation, there is no guarantee that the book industry would opt for the kind of identifier preferred by the library sector. Blansit (2010, p.351) contrasts the ethics of librarians, which leads them to develop a system in which 'the target tag provides an identity number which by itself is meaningless', with those of booksellers, who 'may wish to encode a tag with an ISBN number'. The Standards Australia Working Party (2006) noted a divide between the needs of the library sector and those of the publishing industry in the context of the Working Party's privacy discussions, and Palmer (2009, p.54) points out that the International Standard Book Number (ISBN), already present in books with the '978' prefix, was proposed by booksellers as the basis for an EPCglobal number, which could therefore be decoded.

On the other technical barrier to potential privacy breaches, namely, the relatively short read range of the passive library HF tags, Muir (2007, p.100) points out that RFID readers are relatively inexpensive and could be upgraded to operate at longer distances. Molnar and Wagner (2004, p.214) warn that read distances are limited primarily by regulation on reader power and antenna size and that 'we should be prepared for illegal readers that might have a read range several times larger.' Archer argues (2007, p.22) that although current RFID technology requires close proximity 'one never know what advances will be made or when', adding that ‘if “they” can snoop, they will'. Another concern is around the transmission of data from RFID tag readers to LMS and the fact that wireless transmissions can be intercepted (Molnar & Wagner, 2004; Archer 2007).

Moreover, if one is to consider the potential for ethical abuse of the technology, one needs to factor in the fact that libraries may not always continue to use passive HF tags; there has already been some interest in UHF tags, which would provide a significantly longer read range. Butters, a strong proponent of RFIDs, acknowledges 'that suppliers might switch to UHF systems because it suits *their* business rather than it being the best technology for the library application' (Butters, 2008, p.131). He notes that RFID technologies 'are still evolving and are driven by markets and industries that dwarf libraries in terms of their current size' (2008, p.133).

The review of the literature shows much discussion on the relative risks to privacy of RFID technology. Tracking does not emerge as a significant risk, compared to the risk posed by the active RFID tags common in retail and other sectors, but hotlisting is seen as a potential issue and raises ethical concerns for librarians. There are few, if any, references to the guidelines from professional library associations and little discussion of management strategies that can be put in place to ensure libraries' long-standing respect for client confidentiality. This lack of discussion within the library sector can be contrasted to health, for example, where the ethical implications of new technology are often discussed. Sarhan (2009), for instance, discusses in depth the ethical considerations concerning the introduction of tele-medicine for nursing practice.

The library sector has a long tradition of respecting client privacy and guidelines, such as those developed by the professional library associations, that can minimise the chances of privacy breaches and the resulting ethical issues. However, such guidelines can only minimise the risks, not eliminate them. It is argued that the inevitability of these residual risks should not be used an excuse to ignore them, and that libraries still need to demonstrate that they have assessed the risk and acted accordingly.

There is little, however, in the literature on the actual management of RFID implementation, let alone management of the ethical issues relating to RFID implementation in libraries. In summary, there is a gap in terms of research into how RFIDs are implemented and in particular what part ethical considerations play. This study is designed, at least in part, to address this gap and to emphasise that libraries need to show that they have exercised due care in considering the ethical implications surrounding the implementation of new technology. In order to achieve this, we need a better understanding of how these decisions are currently made so that practice can be improved.

Research design

The next phase of this series of investigations into RFIDs and potential privacy issues was conceived as a pilot project to gather in-depth information on how libraries/library networks have undertaken RFID implementation and how, if applicable, project managers and/or those implementing RFIDs managed ethical issues. The aim of this project, therefore, was to undertake a set of interviews that would illuminate local practice, with a view to complementing the earlier, theoretical studies of ethical issues (Gibb et al., 2011; Thornley et al., 2011). The methodology adopted is shown in figure 1.

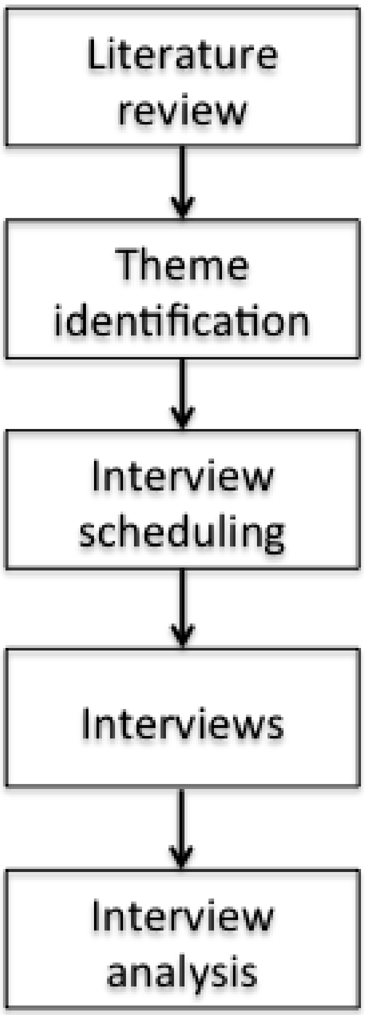

Figure 1. Research methodology

The literature review was used to identify the key themes that would be explored during interviews with practitioners who had adopted RFID technologies. The key themes were:

1. What were the drivers behind RFID implementation?
2. What benefits have you experienced from RFID implementation?
3. What data is held on the tags used in your library?
4. Did the adoption of RFIDs require any changes to how the security of data is ensured?
5. What privacy or ethical issues were identified, if any?
6. What consultation was there pre-implementation and post-implementation?
7. What technological changes do you anticipate?
8. What other issues are there, including advice on best practice, or on lessons learned, for other libraries?

The investigators used semi-structured interviews to gather the research data in which key people within the library/library network were asked to tell the story of how they planned and implemented RFIDs, either individually or, where possible, as part of a focus group. Focus groups were considered preferable, since people with different perspectives will generate richer reflection through their interaction. Where there was a need to elicit additional information, the investigators followed up with supplementary questions, such as whether those who took part in the implementation process saw potential ethical issues in the RFID applications implemented; if so, how they managed these issues; and whether they referred to any ethical frameworks such as professional codes of ethics. Other conversational prompts included rationale for implementation, interviewee understanding of the technology, staff and client concerns (if any), security and data protection issues, and lessons learned. With the agreement of participants, discussions were digitally recorded and subsequently transcribed.

Interviews were conducted in the Republic of Ireland, Australia and Britain. There was a total of eighteen individual participants and ten libraries: six libraries or networks from the public library sector, three academic libraries and one special library. The researchers scanned the sector to establish which libraries had implemented RFIDs and selected libraries to approach based on relative proximity for one of the research group (i.e., convenience sampling was utilised). The relatively large percentage of public libraries may be coincidental since the research sample is small but, based on the RFID literature, it may reflect the benefits RFIDs are seen to afford the transaction-orientated library services of the public library sector.

In an interpretive approach to the analysis of the collected data, thematic analysis was used to reveal the findings. Thematic analysis involves identifying, analysing and reporting patterns within data. A theme represents some level of patterned meaning within the data (Braun & Clarke, 2006). Analysis was largely top-down in that sets of anticipated themes were established prior to the interviews and these were matched to responses. However, iterative coding was also employed in which the core meaning of responses was established reductively by generalising from the language used by a respondent to a normalised set of terms across responses (Mostyn, 1985).

Findings

Drivers

Participants were asked about the rationale for RFID implementation so there was a strong sense of what drove it. The main drivers that were reported were: the need for efficiencies and the perceived need to release staff for client orientated services. The main efficiency improvement sought was that afforded by self-check. One public library had been refurbished and was going to increase substantially in size, but with the same staff establishment, and hence needed some kind of self-service to replace 'traditional issuing at the desk'. In most cases, it was difficult to disentangle the drive for efficiencies from the drive to make best use of staff and develop client-focused services; they are strongly interrelated in the sense that the efficiencies afforded by RFID technology allow library managers to redeploy staff to provide more and better user-facing services.

Efficiencies were generally described in terms of the enhancement of client services, or the maintenance of levels of service as libraries become busier. As one public library participant put it, there had been very little increase in staff hours over the previous two decades 'so we've just had to get smarter at what we do.' It is worth noting, however, that one public library interviewee commented about *another* public library authority: 'the main reason that they introduced RFIDs was actually around efficiency gains but also with a view to downsizing staff', not the kind of remark one reads in the professional literature, which focuses on the positive aspects of RFID implementation.

Benefits/outcomes

Benefits and outcomes were little different from what has already been reported in the literature and are not discussed here in any detail. Potential benefits listed in Gibb et al. (2011, pp.246-247) were mapped against participant responses but only two of the potential benefits demonstrated high incidence in the responses: ‘Patron self-check - less staff at issue desks’ and ‘Release of staff to more professional activities’. Given the drivers of RFID implementation, reported above, these findings were not surprising.

It is, however, worth commenting briefly on the impact of RFIDs on the relationship, as interviewees saw it, between themselves and their clients, particularly in view of the suggestion that RFIDs can enhance client privacy through the increased opportunity for self-check (Zimerman, 2011) and the alternative view that simply 'adding self-check machines' without providing extra services risks RFID technologies becoming the 'ATM of the library world' (2005, p.448).

Some participants saw reluctance on the part of the public to use self-check, with one interviewee suggesting that some clients are afraid they will lose the personal contact, and that the challenge is to persuade clients that there is greater opportunity for staff to spend time with them, as staff move away from the issue desk. Others reported that some customers found self-service less intimidating and that they enjoyed the comprehensive service that was provided (issues, reservations and returns). Another emphasised that RFIDs enable staff to spend more time with customers and that interactions are 'more meaningful', because, with traditional check-out there's little eye contact. One public library had emphasised to users that staff numbers were not being reduced as a consequence of RFIDs but, that as staff numbers had already been reduced through previous budget cuts, the technology provided an opportunity to release staff to engage with customers. It might be more accurate to say that the cultural barrier to self-check take-up can depend on the relationship between staff and clients, with one participant from a public library network pointing out that the network cannot tell branches how to operate. While interactions at an issue desk may be relatively superficial, it could be that interaction with staff for mundane things such as book issue gives the public an opportunity to engage, whereas it can be off-putting for people to approach a staff member with a complex query.

Data stored on tag

The ALA Guidelines recommend that only a unique, numerical identifier be stored on a tag and this matched practice amongst all but one of the libraries, according to participants. There was some confusion, however, about what kind of data was stored. One public library participant thought the whole catalogue record was stored on the tag but another participant from the same library was clear that it was only the item number on the tag. Another public library participant was unsure what was stored on the tag but settled for ISBN, which would be easier to trace to a bibliographic work (and obviously would not be item specific). Another public library interviewee indicated that tags initially contained the title and a barcode number but that currently only the barcode number was stored. One of the academic library participants thought that the complete bibliographic record was stored on the tag but an interviewee from the same institution said that only the accession number was stored.

The only libraries that reported storing more than a unique identifier were a public library and an academic library. The public library stored basic information such as title, author and branch location for all material bought since RFID implementation. During the retrospective conversion, tags contained only a barcode number but this was a pragmatic decision that aimed at streamlining the process. The feeling was that the basic information stored 'was not ethically sensitive information because ... it's publically available anyhow.' They did ask their supplier what data would be on the tags and were satisfied there would be no personal data, which 'was pretty much [their] concern.' The academic library also stored an institutional code to facilitate borrowing rights between students from other academic libraries and to reduce the number of books setting off security systems in other libraries.

When the issue of what data to store on RFID tags came up, most respondents felt that storing borrower information would ring alarm bells as far as privacy issues were concerned, but it is worth noting that one public library interviewee, responding to a question about future applications of RFIDs, said he/she 'would like a RFID borrower card so books would issue/discharge as they [borrowers] walk through.'

Data security

The issue of data security did not come up much in interviews. Two public library participants referred to bibliographic and loans data being stored behind Council/organisational firewalls. One participant said that it would be possible to hack into a Library Management System but that LMS are not as 'hackable' as they used to be. Another mentioned having a protected network that meets Government requirements and that some of the RFID solutions considered were deemed unsuitable because they failed to meet IT security regulations. A third public library participant was unsure how data were secured. A fourth public library highlighted their need to conform with the wider security needs of their parent local authority, whose IT systems had been outsourced and which imposed a security policy on users. In this environment the LMS was hosted by the outsourcer who was responsible for the security of all personal data. The outsourcing contract assumed that desktop systems were accessed by staff, who were authorised users as they were employees, rather than customers or other systems suppliers. The use of self-service devices had therefore brought them into conflict with security policies as customers, rather than staff, needed to carry out transactions; i.e. they needed to 'touch the systems'. This had been circumvented by installing firewalls on all the self-service units and effectively creating a closed user group on the VPN. A further problem in terms of imposed security was that the provider of the self-service units could not remotely access the units, which meant that diagnosis and maintenance were constrained.

Ethical concerns

The majority of participants reported no ethical concerns. Interviewees at the three academic institutions saw no privacy or data protection issues. One pointed to the fact that only a numerical identifier appears on the tag and that read distances are short and another mentioned the fact that 'because the RFID machines don't contain themselves any personal information', they saw no need to look into potential ethical issues. A participant at one of these institutions suggested that library staff 'might have been more worried about things like privacy' than students but that the latter expressed no concerns.

A public library participant stated that there were no staff concerns or client queries about privacy or data protection issues. Two participants indicated that they 'sort of knew' there were no real ethical issues because of 'the way in which the system was working', adding 'some of the vendors might have highlighted... that there could be an issue if you went down a certain way and that was about it’. One of the latter interviewees also referred to the technical safeguard: to know what someone is reading would require access to the IT system (IT person) although earlier this individual suggested that someone could identify a title only if he/she had already had it. Another public library participant stated: ‘we didn't have any concerns, because we were limiting the information that went on to the RFID tags to information about the item to which they applied, so we felt that there were no ethical issues from our perspective.' The key for them was that no borrower data would be stored on the tag. There had been no public consultation but 'given the positives that RFID was going to offer us and the fact … it was certainly no secret that it was being implemented and we had … no enquiries whatsoever about invasion of privacy or any other issues.'

For one Australian public library network, it was significant that the relevant state library had no objections when another local government region received grant funding for RFIDs since their state library is 'particular … in terms of ethics and compliance and … they would have certainly raised any issues.'

It is worth recording that the language used in one of the public library interviews suggested a slightly dismissive attitude towards any perceived ethical issues: 'We basically heard through various professional forums bits of *scuttlebutt* about how people were concerned that… that some sort of devices, external to the library, could read their RFID tags and … extract information' and 'it did come through a list … or maybe an American Library Journal article about a group in New York or San Francisco or somewhere … who were *getting their ire up* about … the introduction of RFID at their local library and they were very concerned that … people would be able to scan their personal details [italics added by authors]'.

There was some 'vague concern' at one of the public libraries: 'well, we have some people saying … that maybe if they went somewhere that somebody would be able to read what book they had in their bag.' There was no public concern about being tracked with their books, only staff anticipating queries but, as one interviewee put it, 'we were able to allay it and just show that all the information that was on the tags was the fourteen digits of the item number, that was all.' In other words, concerns were managed. This specific participant also stated 'I don't think we need to explain to people what RFID is', arguing that one does not explain what a light switch does – an interesting comment that would be worth revisiting. At this library, concerns about data protection and privacy centre around people leaving cards in machines, leaving details visible on screen or printing their details out and leaving them on printers; none of which, as one participant observed, is 'an RFID issue'. Lack of concern about RFID-related privacy or data protection issues stems from the fact that RFID stations show only books going out, not personal details. An academic library acknowledged the problem of legacy identification from different systems (barcode and tail-tags) and accepted that this should form part of a more general risk evaluation, as could the aggregate information stored on multiple RFIDs on objects held by an individual.

However, and worryingly, the general view appears to be that the risks are so low that they do not merit consideration, rather than including them as part of overall risk assessment and demonstrating that the risks have been formally appraised and their impact considered. There also appears to be a conflation between preserving the security of data and ensuring that ethical aspects have been considered: it is perfectly possible to secure data that has been obtained, or stored, unethically.

At the only special library in the study, the sole privacy concern raised had been staff concern that management could find out if they were hiding the Library's books in their offices by holding up the read device in their doorways – clearly not seen as a major concern and one that could easily be managed. In the interview, it emerged that the Library does lend books but participants saw no privacy issue, on the grounds that RFIDs are not actually used for loans (although the tag does leave the Library with the book) and, in any case, tags contain only an item number.

The only strong awareness of ethical concerns was expressed by one of the public library participants, who noted that around the time of RFID implementation there was some publicity around the introduction of RFIDs in San Francisco Public Library and some media interest in 'spy tags' in the commercial sector (for instance, Gillette's use of RFIDs for market tracking), adding that some of the public were concerned about 'their privacy with the technology, so we'd had to look into that very carefully and how we approached that.' The interviewee was also 'aware of some of the stuff that was happening around the standards of the writing of data to tags' and of 'the different frequencies of tags' and noted a practical reason for minimising data on tags, namely, ability to choose suppliers: 'you want to have that intra-operability … we wanted to future-proof ourselves as much as possible so we kept the amount of data that we wrote to the item tags quite minimal.' The participant went on to say, 'But also we didn't want to be in the situation where people felt that you could have somebody sneak up behind you and scan and find out what you were reading. Now there are limitations in terms of the technology … but we wanted to minimise any perception around that sort of thing.' In other words, there was an informed awareness of the technical limitations of RFID's potential for privacy breaches but, in view of the negative publicity, a determination to manage public concerns.

Asked about sources used for ethical decision making, participants had little to say. One of the public library interviewees mentioned the book, 'RFID in Libraries' (probably a reference to Palmer, 2009). As noted above, one of the public library participants said that some vendors brought up potential issues. At the same institution, it was reported that the relevant government authority had a code of ethics, to which library staff adhered, and that the policies of the Australian Library and Information Association are referenced in some of the internal policies. One Australian public library participant noted the information privacy legislation of the relevant state and another noted that their state library sends them 'a lot of… bulletin information that they've found elsewhere.' All this suggests some delegation of ethical concerns, which will be discussed later in the paper.

Client consultation

In only two cases, one of which is mentioned in the previous section, was there any significant public consultation. In one public library the consultation involved pre- and post-implementation surveys in which key issues were identified, responses generated and issues followed up. The attitudes from customers often demonstrated fears and resistance and it was seen as important that these should be addressed as part of the roll-out and promotion of the service. Bad experiences with retail systems were mentioned (customers did not want systems that barked out instructions, for instance) as were concerns about the loss of staff contact. Two public library participants said that the public were informed about RFIDs but that what they were told was framed in terms of self-service, which would be no surprise since 'they were used to supermarket technology', and not the technology itself: 'we didn't say that it was RFID; that mightn't make any sense to them'. Another public library interviewee said there had been no public consultation but added 'it was certainly no secret that [RFID] was being implemented and we had … no enquiries whatsoever about invasion of privacy or any other issues.' At one of the academic libraries, the student union asked about 'that kind of stuff' (data protection, privacy issues) but was clearly satisfied with the response from the Library. At another, members were told about the switch from the current self-check system to RFIDs but only one comment was reported, about books setting off alarms in shops. At the latter institution, there was a reference to the security element: 'they [students] do realise that the RFID tag is very connected to the security and stuff, but I don't know that they've figured out how it actually works, and that's probably no bad thing that they don't … so we don't enlighten them too much on that.' One academic library reported that students from other institutions using the library do indeed set off the security systems since the RFID tags in their books were readable as a presence but were not identifiable as being on loan. At the special library, members were not consulted because RFID tags were not going to be used for loans and there was therefore no perception of a privacy issue, although one participant did note that in an environment like theirs some of the Library's clients would be 'quite sensitive about people finding out what they are reading.'

In one public library network staff consultation was raised within the context of a wider 'People Plan' for both professional and para-professional staff and that this had been implemented through a change management package. This included the identification of coaching and training requirements to help staff ensure a successful roll-out and led to the implementation of, for instance, new staff counters, floor walkers and a simplification of some of the self-service units.

Changes in technology

A key point that informed this study was that one needs to take into account the likelihood that further developments in a technology will affect the ethical issues and may, in some cases, heighten ethical concerns (Thornley et al., 2011). Asked, for instance, whether an increase in the tag read range would make any difference, participants responded differently. One public library interviewee said that, if they ever decided to 'go down the track of having a borrower RFID card instead of a normal borrower card' then they would have to revisit the privacy issue but that longer read ranges would make no difference as far as tags are concerned: 'all they're going to be looking at is the barcode, the majority of the time, and title, maybe the title of the item, but unless you know who you're targeting … there's not much you can do with that information'. Another public library participant noted that if the standard adopted by library suppliers meant that tags were provided with title and other information 'we'd certainly then need to just see where the standards are still sitting in terms of the readers and devices to make sure that people just can't skim that information' – at the moment, even if they could, 'all they've got is the item barcode', but if bibliographic information started appearing on tags, 'we'd then have to review where, how much of a potential risk that would then put us.' One of the special library participants responded that if read ranges became substantially longer and information on tags could be read 'from a distance without anyone realising that you're doing that, it could possibly be an issue' in the sensitive environment in which the Library operates.

Other issues raised

In two of the public library networks, reference was made to the 'internet threat/relativity' argument: it is 'drawing a fairly long bow to suggest that judging by what people borrow is going to somehow invade their privacy when there's so many other ways that people's lives are invaded that they probably don't even know about.' Asked about storing bibliographic information on tags and the ALA guideline about storing only the item number on tags, one of the interviewees responded 'once again, I guess, it's a question of risk management … my supposition is they'd [the security services] be more likely to be … looking on the Internet and through their ISP or something than they would be watching them come out of the library.' At another network, the interviewees put it this way: 'Wouldn't cookies and web browsers, you know, where companies or whatever can know every click you do on a computer be much more dangerous to ethical concern for… [second respondent adds] for people rather than this is, you're not going to get much information, really, unless you have access to the system.'

The respondent who mentioned risk management, went on to refer to potential privacy breaches in terms of a risk management matrix (see Gibb et al, 2011 for an example) – likelihood and gravity, she/he suggested, both fall into the low quadrants, compared, for instance, with Facebook: 'its ability to show your mobile phone number to every contact you've got if you don't go and actually switch that thing off … it is quite bizarre and quite scary in lots of ways. So where that sits in terms of risk compared to what information's held on a library tag is an interesting sort of question.' The other participant in this interview added that if people had sufficient sophistication to read your tag then 'it would be easier for them to hack into the LMS' (Library Management System).

Discussion

This study identified a gap in the literature in terms of research into how RFIDs are implemented and in particular what part ethical considerations play. In general, the interviews suggest some awareness of the potential privacy issues raised by RFID technology on the part of participants but not as much as one might expect, given the extent to which privacy issues have been raised in the literature on RFIDs in libraries. Where the issue of tag data came up, most interviewees indicated that they would not want to see personal data included on tags, although one public library participant was keen to have RFID tags on borrower cards so that books would issue or discharge as borrowers walk through the security gates. While this was an atypical view, there was also a surprising level of vagueness about – and even ignorance of – what is actually on the RFID tags, which does not suggest significant engagement in ethical issues. In the case of one public library network, there was support for having brief bibliographic information on tags, despite the fact that this would make privacy breaches easier – a point underlined in the ALA Guidelines.

Linked to the vagueness about RFID technology on the part of some participants is a degree of reliance on vendors. Two of the participants, for instance, mentioned the fact that it was some of the vendors who highlighted the potential ethical issues if the Library were to go down a particular (undefined) path in RFID implementation. Reliance on others is also evident in the case of those public librarians who deferred to a leading institution such as a state library (Australia) or local government authority. It was noted, for instance, that for one Australian public library network it was enough that the relevant state library had not raised issues when a similar network had received funding for RFID development. While this may be preferable to over-reliance on vendors, it does tend to suggest a delegation upward of ethical concerns by library managers.

How then do managers decide that the technology is acceptable? There is some evidence of environmental scanning, such as the use of bulletins issued by a specific state library, and of the use of internal sources of information, such as policies created by IT departments. In the latter case, the concern is largely with security, as distinct from privacy as such. There were also general references to professional bodies but only two references to specific sources: one to the ALA Guidelines and another that the internal policies of the relevant government authority referenced the policies of the Australian Library and Information Association.

The sample of managers and librarians interviewed for this study was not large enough to draw any definite conclusions about the decision-making process but some trends do emerge. Levels of ethical reflection varied, from significant environmental scanning, public consultation and study of the technology, at one end of the spectrum, and over-reliance on vendors and on the decisions made by other library managers, at the other – 'over-reliance' because, the delegation of decision-making raises the issue of who a manager should trust. If managers are going to put any store in the recommendations/applications provided by vendors, they need to be clear about what the technology does and has the potential to do.

In the case of two public library authorities, there was public consultation roughly along the lines of the San Francisco City Library implementation but in the other cases discussed there was little if any consultation with stakeholders. There is nothing in the relevant professional codes of ethics that obliges library managers to inform clients and other stakeholders about the implications of technology roll-outs although the ALA Policy Guidelines do promote user education and consultation as part of the RFID selection process (2006). Moreover, given the well-publicised concern about the privacy implications of RFID technologies and the trust that libraries generally enjoy in the wider community (Coombs, 2004, p.495), library managers would seem to have some obligation to include these communities in their decision-making processes. With the exception of one public library authority implementation, however, there was no sign in this study of the application of a 'Precautionary Principle' to the adoption of new technologies, of the kind demonstrated in San Francisco. This does raise a significant concern about the level of strategic ethical engagement of the library profession in questions concerning the implications of new technology. In relying on vendors and generic public management policies there is no clear picture that anyone is bringing to the debate the current needs and rights of library users and also any future potential threats to their interests.

The comment, noted in the findings, that one need not explain to people what a RFID is, on the grounds that one does not explain what a light switch does, suggests a significant lack of ethical concern. It is also based on the false assumption that light switches and complex technology containing high levels of data are somehow equivalent in terms of potential harm to individuals. It is widely accepted that technology has at least two ethical dimensions – its development and its impact through use - but those that store and potentially analyse information have particular issues.

Where the issue of risk came up, managers regarded risks as low, basing their judgement mainly on the current state of the technology, with short read ranges and the general (though not universal) practice of limiting data largely to an identification number. In one case, risks were dismissed in the suggestion that, at the time of the San Francisco implementation, there had been some 'scuttlebutt' about the potential for privacy breaches. Two managers minimised the risks, as they saw them, by measuring the privacy/ethical issues against those presented by social media such as Google and Facebook. The suggestion seems to be that, since these pose a greater threat to privacy, we should ignore library/book based issues or at least not be too concerned about the latter.

This is an odd argument since it could be adopted by one of the social media ('Facebook presents far greater privacy threats than Google therefore Google has decided to do nothing about the concerns of consumer groups'). In the case of some social media, there is also the fact that people knowingly sign up to put their personal details on the web whereas people who borrow library books do not realise their borrowing habits could potentially become known to others. Finally, it could be argued that librarians who espouse a set of professional standards have a duty of care towards their clients that social media may not.

The reference to, what could be characterised as, the 'internet threat/relativity' argument in two of the public library networks also suggests a potentially worrying normalisation of the threats that technology can pose to privacy. This is reinforced in the comment that anyone with enough sophistication to read an RFID tag would find it easier still to hack into the Library Management System, although 'LMS are not as "hackable" as they used to be.' Again, the fact that there are other ways in which 'snoopers' could breach the privacy of library clients hardly justifies ignoring the potential misuse of RFID technologies.

Finally, it is worth noting that managers' and librarians' accounts of the drivers of RFID implementation were framed in terms of the practical, material benefits of RFIDs, mirroring the literature on RFIDs in libraries. It could be argued, however, that drivers such as the freeing up of staff time to spend with clients or prevention of library closure could be seen as ethical positives that may cancel out or mitigate the ethical risks presented by new technologies such as RFID. Such an argument is notable for its absence.

Conclusion

In conclusion, how do librarians make ethical decisions when implementing new technologies? This study of RFID implementation suggests that an analysis of potential ethical issues was not a central part of the process of implementing RFID technology in nine of the ten libraries studied. In many cases the consideration of these issues had either been delegated to the local government in charge of the libraries with the assumption that they would have picked up on any issues, or, perhaps more worryingly, to the vendors, whose claims for privacy protection had simply been taken at face value. In some cases, there was even a suggestion that ethical issues tend to be peripheral. Among the librarians interviewed, there was awareness of professional standards around confidentiality and clients' right to privacy but there was little reference to specific guidelines.

RFID implementation is an informative example of what appears to be current practice in the implementation of new technologies in libraries. As a profession we should be exploring the best ways in which to prepare/educate/support library managers in incorporating ethical concerns into related decision making. We should also look at management structures and decision-making processes to clarify where exactly responsibility for ethical considerations should lie. Managers have a range of players to consult, including professional associations, leading library institutions, vendors, IT colleagues, staff and clients, but if they are primarily responsible for technology projects then they need to understand the technical potential of the new technologies, not simply take it on trust that someone else has thought it through. Moreover, if librarians are central to the provision of information to their clients they also need to be central to the careful consideration of any ethical issues that may arise when new technologies provide new ways of storing and managing that information.

All of this suggests the need for greater professional development and a more proactive role for professional associations in offering guidance on the implementation of new technologies. This would require a review of policies and related statements on the part of the associations. In particular, adoption of the ‘Precautionary Principle’ represented by San Francisco’s establishment of a Library Technology and Privacy Advisory Committee is recommended. It would also be worth adopting the concept of Privacy Impact Assessment (PIA), as recommended by the European Commission (2011) and implemented by several governments over the past few years. PIA is aimed to help people/agencies 'assess and identify any privacy concerns and address them at an early stage, rather than leaving the solutions to bolt on as an expensive afterthought' (Information Commissioner's Office, n.d.; *see also* Australian Government, Office of the Australian Information Commissioner, 2010; United States, Department of Homeland Security, The Privacy Office, 2007). It is also proposed here that professional associations, educators and trainers develop case studies that not only capture the complexities of ethical dilemmas and decision-making but also factor in the extent to which scenarios change as the technologies develop. These would not only assist librarians and library managers in the decision-making process but would raise ethical awareness. If the sample studied here is indicative of the broader profession, there needs to be less managerialist reliance on risk assessment and more on doing the right thing, which is the whole point of ethics.

Acknowledgements

With thanks to all the libraries that agreed to participate in this research project and to Shane McLouglin of the Department of Library and Information Studies at University College Dublin, who assisted with the interviews in Ireland.

References

American Library Association (2002) *Library bill of rights: Interpretations of the library bill of rights: Privacy*. Available at http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy (accessed 22 March 2013).

American Library Association (2006) *RFID in libraries: Privacy and confidentiality guidelines*. Chicago: American Library Association. Available at http://www.ala.org/offices/oif/statementspols/otherpolicies/rfidguidelines (accessed 26 March 2013).

ANEC & 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.* Brussels: ANEC(ICT-2007-G-059). Available at www.anec.org/attachments/ANEC-ICT-2007-G-059.pdf (accessed 2 December 2012).

Angwin, J & Valentino-Devries, J (2012) Google's iPhone tracking. *The Wall Street Journal,* 17 February. Available at http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html (accessed 3 December 2012).

Archer, JD (2007) An RFID primer and intellectual freedom catution [sic]. *Indiana Libraries* 26: 21-26.

Arthur, C (2012) Google's privacy policy: EU data chiefs 'to act within days'. Guardian, 8thOctober. Available at http://www.guardian.co.uk/technology/2012/oct/08/google-privacy-policy-data-protection (accessed 3 December 2012).

Australian Government. Office of the Australian Information Commissioner (2010) *Privacy impact assessment guide*, Revised May 2010. http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-impact-assessment-guide (accessed 14 August 2013).

Ayre, LB (2004) Position paper: RFID and libraries. Draft chapter to be published in: Garfinkel, S and Rosenberg, B (2005) *Wireless Privacy: RFID, Bluetooth and 802.11*. New York: Addison-Wesley/Prentice Hall. Available at http://www.fatburen.org/wpbagen/bagenmappar/dokument/arx/rfid-permission.pdf (accessed 22 March 2013).

Ayre, LB (2012) The RFID opportunity: Use tags to deliver new services to your patrons. *American Libraries* 43(9-10): 17.

Blansit, BD (2010) RFID terminology and technology: Preparing to evaluate RFID for your library. *Journal of Electronic Resources in Medical Libraries* 7(4): 344-354.

Braun, V and Clarke, V (2006) Using thematic analysis in psychology. *Qualitative Research in Psychology* 3: 77-101.

Butters, A (2007) RFID systems, standards and privacy within libraries. *The Electronic Library* 25(4): 430-439.

Butters, A. (2008) RFID for libraries: a comparison of high frequency and ultra high frequency options. *Australasian Public Libraries and Information Services* 21(3): 120–134.

Cadoo, S & Cadoo, A (2004) *New librarians' symposium 2*, Adelaide, 3-4 December 2004. Available at http://conferences.alia.org.au/newlibrarian2004/zobjects/presymppapers/Cadoowebsitepaperfinal.pdf (accessed 7 May 2012).

Cai, S, Li, T, Li, Y & Deng, RH (2009) Attacks and improvements to an RFID mutual authentication protocol and its extensions. 2nd ACM conference on wireless network security (WiSec' 09), Zurich, Switzerland, March 16-18, 2009. Available at http://www.mysmu.edu/phdis2009/shaoyingcai.2009/WISEC.pdf (accessed 7 May 2012).

Cavoukian, A (2004) Tag, you’re it: Privacy implications of radio frequency identification (RFID) technology. Toronto: Information and Privacy Commissioner of Ontario. Available at http://www.ipc.on.ca/images/resources/up-rfid.pd f (accessed 7 May 2012).

Coombs, KA (2004) Walking a tightrope: Academic libraries and privacy. *The Journal of Academic Librarianship* 30(6): 493-498.

Coyle, K (2005) Management of RFID in libraries. *The Journal of Academic Librarianship* 31(5): 486-489.

Engels, E (2006) *RFID implementation in California libraries: Costs and benefits*. Sacramento: California Library Association. Available at http://www.clanet.org/included/docs/IT3.pdf (accessed 3 December 2012).

European Commission (2011) *Privacy and data protection impact assessment framework for RFID applications, 12 January 2011.* Available at http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf (accessed 22 March 2013).

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

Gibb, F, Thornley, C, Ferguson, S & Weckert, J (2011) The application of RFIDs in libraries: an assessment of technological, management and professional issues. *International Journal of Information Management* 31(3): 244-251.

Hall, J (2012) Google accused of invading privacy with pictures of house numbers. *Telegraph,* 15 April. Available at http://www.telegraph.co.uk/technology/google/9205486/Google-accused-of-invading-privacy-with-pictures-of-house-numbers.html (accessed 3 December 2012).

Information Commissioner's Office (UK) (n.d.) *Privacy impact assessment*. Available at http://www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment (accessed 14 August 2013).

International Federation of Library Associations and Institutions (2012) *IFLA code of ethics for librarians and other information workers* (full version). Available at http://www.ifla.org/news/ifla-code-of-ethics-for-librarians-and-other-information-workers-full-version (accessed 13 August 2013).

Ionescu, D (2010) Google resumes street view driving: More trouble looming? *PC World*, 9 July. Available at http://www.pcworld.com/article/200753/google resumes street view driving more troublelooming.html (accessed 3 December 2012).

Lockton, V & Rosenberg, RS (2005) RFID: the next serious threat to privacy. *Ethics and Information Technology* 7: 221–231.

Mehrjerdi, YZ (2011) RFID: the big player in the libraries of the future. *The Electronic Library* 29(1): 36-51.

Moessner, M & Khan, GN (2012) Secure authentication scheme for passive C1G2 RFID tags. *Computer Networks* 56(1): 273-286.

Molnar, D & Wagner, D (2004) Privacy and security in library RFID issues, practices, and architectures. CCS '04 Proceedings of the 11th ACM conference on computer and communications security. Available at http://delivery.acm.org/10.1145/1040000/1030112/p210-molnar.pdf?ip=149.157.1.188&id=1030112&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF1C517B38E12D13249503B474E5DC23DD5&CFID=359794273&CFTOKEN=36463715&__acm__=1378812800_434aac65f4f13de591ae8aa6da0b24a2 (accessed 10 September 2013)

Mostyn, B (1985) The content analysis of qualitative research data: a dynamic approach. In: Brenner, M, Brown, J & Cauter, D (eds) *The Research Interview*. London: Academic Press, pp.115-145.

Muir, S (2007) RFID security concerns. *Library Hi Tech* 25(1): 95-107.

NISO (2007) *RFID in U.S. Libraries: a recommended practice of the National Information Standards Organization*. NISO RP-6-2008. Baltimore, MD: National Information Standards Organization. Available at http://www.niso.org/publications/rp/RP-6-2008.pdf (accessed 01 March 2010; inactive and replaced by NISO RP-6-2012).

NISO (2012) *RFID in U.S. Libraries: a recommended practice of the National Information Standards Organization*, prepared by the NISO RFID Revision Working Group. NISO RP-6-2012. Baltimore, MD: National Information Standards Organization. Available at http://www.niso.org/apps/group_public/download.php/8269/RP-6-2012_RFID-in_US_Libraries.pdf (accessed 22 March 2013).

Palmer, M (2009) *Making the Most of RFIDs in Libraries*. London: Facet Publishing.

Preer, J (2008) *Library Ethics*. Westport, CT: Libraries Unlimited.

Rogers, K (2012) Facebook users raise privacy concerns as company tweaks security settings. *Guardian,* 15 October. Available at http://www.guardian.co.uk/technology/2012/oct/15/facebook-users-privacy-concerns-security (accessed 3 December 2012).

San Francisco Public Library Technology and Privacy Advisory Committee (2005) *Radio Frequency Identification and the San Francisco Public Library: Summary Report.* San Francisco: LTPAC. Available at http://sfpl.org/pdf/about/commission/RFID-and-SFPL-summary-report-oct2005.pdf (accessed 22 March 2013).

Sarhan, F (2009) Telemedicine in healthcare 2: the legal and ethical aspects of using new technology. *Nursing Times* 105(43): 18-20.

Standards Australia Working Party (2006) *RFID for Libraries*. Standards Australia Working Group IT-019-01-02. Sydney: Standards Australia. Available at http://www.sybis.com.au/IT-019-01-02%20minutes%2012-1-06.pdf (accessed 7 May 2012).

Strickland & Hunt (2005) Technology, security, and individual privacy: New tools, new threats, and new public perceptions. *Journal of the American Society for Information Science and Technology* 56(3): 221-234.

Thornley, C, Ferguson, S, Weckert, J & Gibb, F (2011) Do RFIDs (radio frequency identifier devices) provide new ethical dilemmas for librarians and information professionals? *International Journal for Information Management* 31(6): 546-555.

United States, Department of Homeland Security, The Privacy Office (2007) *Privacy Impact Assessments: Official Guidance*. Available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf (accessed 14 August 2013).

Van Grove, J (2012) Your address book is mine: Many iPhone apps take your data. *VB Mobile*, 14 February. Available at http://venturebeat.com/2012/02/14/iphone-address-book/(accessed 3 December2012).

Webinar - The Power and Pitfalls of RFID: Questions, Comments, and Responses, hosted by Library Journal on 16 March, 2010.Available at https://www.jiscmail.ac.uk/cgi-bin/webadmin?A3=ind1005&L=LIB-RFID-UK&E=base64&P=205642&B=------%3D_NextPart_000_003F_01CAF763.AB55CB70&T=application%2Foctet-

stream;%20name=%22Webinar%20Questions%20final.pdf%22&N=Webinar%20Questions%20final.pdf&attachment=q&XSS=3 (accessed 7 May 2012).

Zanetti, D, Sachs, P & Capkun, S (2011) On the practicality of UHF RFID finger printing: How real is the RFID tracking problem? In: Fischer-Hübner, S & Hopper, N (eds) *Privacy Enhancing Technologies.* Berlin: Springer, pp.97-116. (Lecture Notes in Computer Science, 6794).

Zimerman, M (2011) Radio frequency identification (RFID): Time to take another look. *OCLC Systems & Services: International digital library perspectives* 27(2): 146-154.