


Provided by the author(s) and University College Dublin Library in accordance with publisher policies. Please cite the published version when available.

<b>Title</b>	Do RFIDs (radio frequency identifier devices) provide new ethical dilemmas for librarians and information professionals?
<b>Author(s)</b>	Thornley, Clare V.; Gibb, Forbes; Ferguson, Stuart; Weckert, John
<b>Publication date</b>	2011-12
<b>Publication information</b>	International Journal of Information Management, 31 (6): 546-555
<b>Publisher</b>	Elsevier
<b>Link to online version</b>	<a href="http://dx.doi.org/10.1016/j.ijinfomgt.2011.02.006">http://dx.doi.org/10.1016/j.ijinfomgt.2011.02.006</a>
<b>Item record/more information</b>	<a href="http://hdl.handle.net/10197/3606">http://hdl.handle.net/10197/3606</a>
<b>Publisher's statement</b>	This is the author's version of a work that was accepted for publication in the International Journal of Information Management. Changes resulting from the publishing process, such as peer review, editing, corrections, structural formatting, and other quality control mechanisms may not be reflected in this document. Changes may have been made to this work since it was submitted for publication. A definitive version was subsequently published in The International Journal of Information Management., 31 (6): 546-555 DOI: 10.1016/j.ijinfomgt.2011.02.006
<b>Publisher's version (DOI)</b>	<a href="http://dx.doi.org/10.1016/j.ijinfomgt.2011.02.006">http://dx.doi.org/10.1016/j.ijinfomgt.2011.02.006</a>

Downloaded 2018-08-19T00:20:37Z

The UCD community has made this article openly available. Please share how this access benefits you. Your story matters! (@ucd\_oa) 

Some rights reserved. For more information, please see the item record link above.



Elsevier Editorial System(tm) for International Journal of Information Management  
Manuscript Draft

Manuscript Number: IJIM-D-10-00246

Title: Do RFIDs (radio frequency identifier devices) provide new ethical dilemmas for librarians and information professionals?

Article Type: Research Paper

Keywords: RFIDs; information ethics; library management; privacy

Corresponding Author: Dr Clare Victoria Thornley, MA MSc PhD

Corresponding Author's Institution: University College Dublin

First Author: Clare Victoria Thornley, MA MSc PhD

Order of Authors: Clare Victoria Thornley, MA MSc PhD; Stuart Ferguson, PhD; John Weckert, BA (Hons), MA, Dip CompSc, PhD; Stuart Ferguson, PhD; John Weckert, BA (Hons), MA, Dip CompSc, PhD

Abstract: This paper provides an analysis of the current and potential ethical implications of RFID technology for the library and information professions. These issues are analysed as a series of ethical dilemmas, or hard-to-resolve competing ethical obligations, which the librarian has in relationship to information objects, library users and the wider social and political environment or state. A process model of the library is used as a framework for the discussion to illustrate the relationship between the different participants in the library system and it is argued that ethical analysis should involve the identification of future developments as well as current issues. The analysis shows that RFIDs do currently pose some dilemmas for librarians in terms of the conflicts between efficient service, privacy of users and an obligation to protect the safety of society as a whole, and that these are likely to become more problematic as the technology develops. This paper is part 2 of a series of papers on RFIDs and the library and information professions.

Dear Dr Hill

As discussed previously in my email please find attached our paper on RFIDs and ethical dilemmas for the library and information profession. I look forward to receiving feedback from the reviewers on how to improve this paper.

Yours faithfully

Clare Thornley

Do RFIDs provide new ethical dilemmas for librarians and information professionals?

### Research Highlights

- Examination of existing and potential benefits and threats of RFID technology
- Development of ethical framework to examine these issues for the profession
- Discussion of competing moral obligations of library and information professionals to information objects, library users and the state and how particular contexts and new technologies, such as RFIDs, may alter these
- Discussion of role of codes of ethics and management practices in resolving these dilemmas and developing best practice

## **Do RFIDs (radio frequency identifier devices) provide new ethical dilemmas for librarians and information professionals?**

Clare Thornley<sup>1</sup>, Stuart Ferguson<sup>2</sup>, John Weckert<sup>3</sup> and Forbes Gibb<sup>4</sup>,

1. School of Information and Library Studies, University College Dublin, Belfield, Dublin 4, Ireland

2. Faculty of Arts and Design, University of Canberra, ACT 2601, Australia

3. Centre for Applied Philosophy and Public Ethics, Charles Sturt University, Wagga Wagga, New South Wales 2678, Australia.

4. Department of Computer and Information Sciences, University of Strathclyde, 26 Richmond Street, Glasgow G1 1XH, Scotland

### **Abstract**

This paper provides an analysis of the current and potential ethical implications of RFID technology for the library and information professions. These issues are analysed as a series of ethical dilemmas, or hard-to-resolve competing ethical obligations, which the librarian has in relationship to information objects, library users and the wider social and political environment or state. A process model of the library is used as a framework for the discussion to illustrate the relationship between the different participants in the library system and it is argued that ethical analysis should involve the identification of future developments as well as current issues. The analysis shows that RFIDs do currently pose some dilemmas for librarians in terms of the conflicts between efficient service, privacy of users and an obligation to protect the safety of society as a whole, and that these are likely to become more problematic as the technology develops. This paper is part 2 of a series of papers on RFIDs and the library and information professions.

### **1. Introduction**

This paper tackles the question of whether RFIDs should be of ethical concern to librarians and information professionals and, in particular, whether they raise any new ethical dilemmas or significantly change the nature of some already existing dilemmas. We frame the question as one of dilemmas since in many cases the scenarios which librarians encounter involve competing and irreconcilable obligations to which there is no clear-cut ethical solution. The role of technology in raising new ethical issues, in particular the invasion of privacy, has been discussed in the academic literature for some time and, increasingly, is impinging on public awareness as can be seen by recent actions by Facebook and Google to improve its privacy protection (Ionescu, 2010; Timson, 2010). Thus far, in terms of information storage, search and retrieval, most public concern seems to be focussed on networked electronic systems rather than on the new possibilities which RFIDs may create for tracking the lending and use of physical information objects. Is this a correct assumption and, if not, what kind of ethical questions are raised for the librarian in terms of safeguarding the privacy of library users? This is an important question to clarify both in terms of accurately educating and informing library users, and also for librarians in order that the profession can be clear as to how to deal with any potential new ethical challenges which RFID technologies may bring.

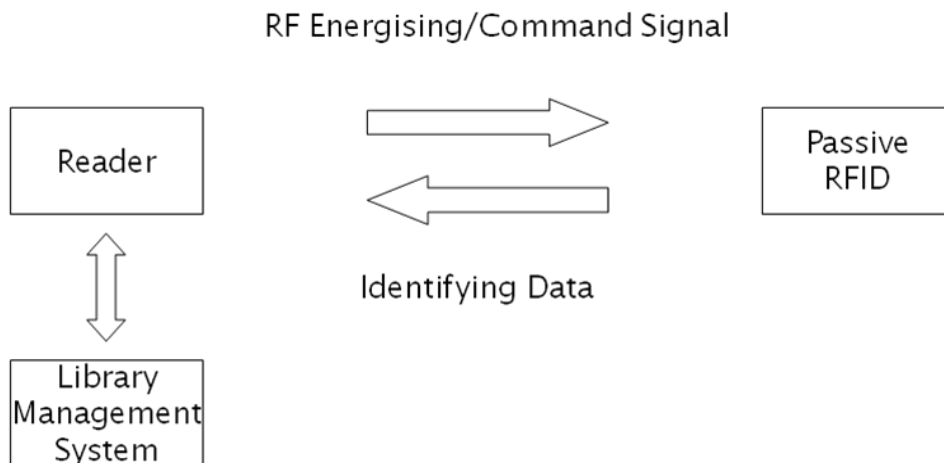
First, we provide a description of RFIDs and outline the potential new privacy issues which they may raise. Second, we provide a model of what a library is, in terms of a process perspective (Gibb, Buchanan & Shah, 2006), as a framework in which to analyse the potential impact of RFIDs. Third, we explore what an ethical dilemma is and discuss some approaches to solving such dilemmas, one of which is establishing the primary role of the moral agent. This impact of RFIDs in terms of creating new value conflicts in the context of medicine has been discussed by Rodota and Capurro (2005), and ethical dilemmas concerning RFIDs in the consumer context have been discussed by Wasieleski and Gal-Or (2008). We argue that this approach can usefully be developed and extended to the library and information context, and that the ethical framework in this case can be modelled as a number of ethical dilemmas. Fourth, we examine the role of the moral agent, in this case the librarian, and explore whether this helps to resolve the dilemmas. We then examine some of the dilemmas in terms of competing obligations which the librarian has to different participants in the library process (including information objects) and, in the case of each dilemma, analyse the extent to which RFIDs may or may not change the nature of the dilemma. Finally we weigh up the evidence from this analysis to determine whether RFIDs do change the ethical context in which librarians deal with competing obligations (both now and potentially in the future). In our conclusions we discuss the ethical implications for the profession irrespective of whether the answer is "more of the same" or "new type of threat". This will then provide a context for our future work on the use and efficacy of ethical and management guidelines (e.g. NISO) for the profession in terms of providing advice on the use of new technologies which may pose ethical dilemmas.

## **2. What is a RFID?**

A radio frequency identifier (RFID) is a small chip-based device which can store data that can be used to identify objects uniquely. Identification is an important aspect 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. Identification has evolved through local accession and call numbers to internationally recognised ISBNs. The technology used to store an identifier has also evolved from a book accession ticket, through barcodes, to security tags and other electronic devices, such as a RFID. An information object that is tagged with a RFID can be detected and tracked as it moves from one location to another, although it should be emphasised that RFIDs only allow the presence of an object to be detected within an area rather than providing a specific location. RFIDs are generally promoted as providing economic and operational benefits to libraries including (Gibb et al, 2010): the reduction or elimination of the physical handling of goods; reduction or elimination of data errors; self-service opportunities; more efficient and effective stock management; and improved security.

A RFID stores data which may describe the information object as well as identify it. The storage capacity 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 hand held devices without the need to have a line of sight between the information object and the reading device (see Figure 1). This makes RFIDs considerably more effective and versatile than conventional barcodes, although their cost is currently higher. RFIDs can be divided into two main types: passive and active. Passive RFIDs, the cheaper type, do not

have their own power supply but convert energy from transmissions generated by a reading device into a signal which can be delivered across very short (up to 60cm) or short ranges (up to 5m). 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, since they have their own power supply, can transmit data over much longer ranges (typically up to 100m). In general active RFID are re-writable and hence reusable devices. RFIDs were initially based on proprietary technologies but international standards, such as ISO 28560-2, have been developed to address aspects such as tag content and structures.



**Figure 1. Transfer of data in a RFID application**

RFIDs can be integrated with library management systems (LMS) in which the identification data is linked to borrower data for the purpose of recording a loan transaction. This data need only be held for the duration of the loan and need not describe the object itself. However, there is at least a temporary link between a borrower and an information object. The RFID tag attached to the information object must also remain live while the borrower is in charge of the information object outside the library environment. It is worth noting, however, that the great majority of libraries use HF (high frequency), 13.36 MHz tags, which have a maximum read distance of around one metre (Organization for Economic Co-operation and Development, 2008). As a consequence, it is argued by some that the risk of tracking is not serious. It would appear to be confined for the present to tracking item use within the library and not once it has left the building. Consequently library borrowers have no reason to fear anonymous vans driving down their streets to check what they are reading (currently their privacy is at far greater risk from the ability to collect computer data via insecure wifi connections) and in a recent webcast, Shai Robkin (Various, 2010) emphasised the relative difficulty of tracking library tags because of the short read distances.

RFIDs raise two main privacy concerns in the library environment both of which relate 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 potential practice of compiling a list of hot or dangerous publications (such as books on jihad and bomb-making) and checking who has borrowed or otherwise used these items. The capacity for RFIDs to allow tracking of items has for several years generated privacy concerns, as reflected in papers by Lockton and Rosenburg (2005) and Slette-meås (2007). In a well-publicised case involving the library sector, there was public concern over the San Francisco Public Library's proposal to tag its



book stock, revolving around the potential for inferences to be made about life-style, sexual orientation, politics and so on, based on their reading habits (Garofoli and Podger, 2007).

Palmer (2009) suggests that much of the concern about the potential of RFIDs to enable privacy invasions stems from a tendency to lump a variety of RFID technologies under the single term 'RFID', arguing that RFIDs would be better thought of as a range of technologies, sharing similar components and physics to those of the radio frequency transponders that were attached to allied aircraft in WWII for identification. Each of these technologies, he suggests, perform quite differently. Equally, well-publicised privacy breaches in the retail sector should not necessarily cause concern in the library world.

Nonetheless, privacy concerns were sufficient to prompt the American Library Association (ALA) to produce a set of guidelines which, if followed, could cut the potential of privacy breaches considerably. Its guidelines provide a set of best practices, which include continuing "commitment to securing bibliographic and patron databases from unauthorized access and use", use of "the most secure connection possible for all communications with the Integrated Library Systems (ILS) to prevent unauthorized monitoring and access to personally identifiable information", protection of "the data on RFID tags by the most secure means available", limitation of "the bibliographic information stored on a tag to a unique identifier for the item" and prevention of "the public from searching the catalog by whatever unique identifier is used on RFID tags to avoid linking a specific item to information about its content" (American Library Association, 2006).

Both tracking and hot-listing rely on the capacity to identify items that are being used by library clients but, provided practices such as those outlined by the ALA are observed by libraries, those seeking to identify library items being used by others would need to be able to both read library tags and hack into the LMS (or ILS in the ALA Guidelines) in order to make sense of the identifiers stored in the tags. It could be argued that this means the use of RFIDs in libraries does not increase the dangers of surveillance since anyone or anybody such as the security forces with the technical means to hack into an LMS would not gain anything from being able to read item tags. It is suggested here, however, that the addition of tag tracking makes surreptitious surveillance more likely.

Moreover, such surveillance would become easier should read distances be increased. At present this is unlikely but it is worth noting the point 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). There has also been some interest in Ultra High Frequency (UHF) RFID, which would provide greater read ranges (Butter 2008). Finally, one should ask whether library managers, if offered new 'improved' tags a few years from now by their vendors, are likely to re-evaluate the benefits listed above and ethical risks of RFID technology and insist on sticking to the older, short-range tags.

### **3. What is a library: the process model**

Any technology is only one part of a library system and, to understand its potential impact, it has to be understood in the wider context of the organisation as a whole. We have previously (Gibb et al, 2010) analysed the role of RFIDs in libraries using a process model (see Figure 2).

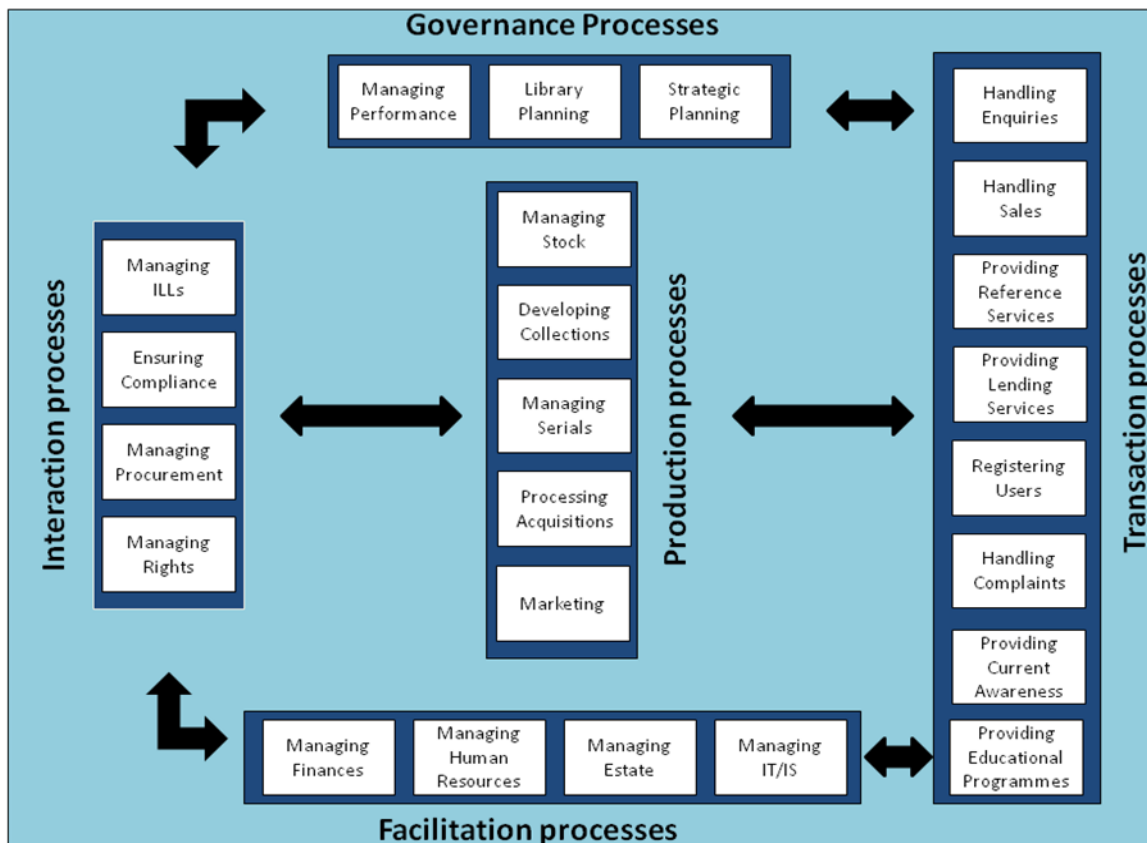


Figure 2. Library process model

This provides a model which identifies the key processes in a library and the people and/or objects involved in those processes who create, acquire, store, analyse, retrieve, manipulate, communicate, archive and dispose of information, i.e.:

- Transaction processes: librarians dealing with users
- Production processes: librarians dealing with information objects (stock, serials etc.)
- Governance processes: library managers involved in strategic planning, policy formulation and oversight
- Facilitation processes: managing human resources, IT, buildings etc.
- Interaction processes: managing inter-library issues, engagement with professional bodies, compliance with regulatory requirements, dealing with suppliers, and interaction with the social and political context

In this paper we also use the process model as a framework for examining the potential ethical issues raised by RFIDs. The aim is to explore the ethical issues raised by RFIDS within the framework of the process model. This is a useful and appropriate approach as we argue that the ethical issues raised by RFIDS can generally be seen as a series of dilemmas or competing obligations between the different participants involved, whether as suppliers, consumers, or managers. An ethical dilemma, discussed more fully in the next section, is a scenario in which there are competing and irreconcilable duties or obligations in which the fulfilling of one duty will result in the neglect of another. An important factor in solving these dilemmas is often an examination of the role of the participant which can, in some cases, lead to a clarification as to which duty should be their primary obligation. Thus a clear

view of the different participants in the library process and their respective roles can help clarify the nature of these obligations.

We examine the role of some of the participants in the library process and explore the nature of the ethical dilemmas raised by RFIDS. We argue that in some cases these duties and obligations will conflict, i.e. the duties to one participant in the process will conflict with the duties and obligations to another participant of the process. Thus the problem can be seen as one in which the nature of obligation is based on the nature of one's relationship with the other participants and one's role in the library process. Our discussion is not limited to ethical analyses of actual and current uses of RFIDs in libraries. In our view applied ethics should be more than the examination of what is the case now. Rather it should anticipate and reflect upon possible unethical use of technology in order to better develop policy to prevent it. These future developments can occur both in terms of technological developments, for example increased range of RFIDs, as discussed earlier, and also possible future political changes, e.g. further fears of terrorism resulting in less protection for privacy in new legislation.

#### **4. What is the role of an applied ethicist?**

Considerable discussion has arisen in recent years about the role of ethicists with respect to new technologies. Traditionally the subject matter of ethics of various technologies has focused on problems that have arisen as a result of that technology. In computer ethics, for example, most discussions have been on issues such as intellectual property and the particular problems computer technology raises, or on perceived invasions of privacy facilitated by the technology. Questions as to the responsibilities of those who develop software for any harm that results from the software are also common. With the advent of other new technologies, particularly nanotechnology and synthetic biology, the almost purely reactive role of the ethicist has been questioned. Many argue that there is also a proactive role to play (Moor and Weckert, 2004; van de Poel 2008) and ethicists should therefore work with scientists and technologists to predict future problem areas. This is of course fraught with danger given the uncertain nature of prediction but, if care is taken, it is a useful and important activity. In many cases it is at least plausible that ethical problems will arise. For instance, in the case of RFID chips it is known that they have been developed much further than the passive chips currently used in libraries and that research is continuing. For example a new passive RFID chip is under development that will be able to be printed onto clothing and paper, with a range eventually of around 300 metres (Williams, 2010).

It is fairly clear that developments in nanotechnology, particularly nanoelectronics, will lead to further miniaturisation of chips and that readers and other sensing devices will become more powerful and sensitive. Given these developments and the uses of chips in other contexts, for example in warehouses, it is certainly plausible that libraries will extend their uses in ways that are more threatening to privacy and make them much more than merely fancy barcodes. Indeed the efficiencies that can accrue in the commercial sector, as highlighted by Kelly and Erickson (2005), are all areas which have application in the library sector: inventory control, manufacturing processes, retailing, transportation, logistics, security and recalls. This threat is not inevitable of course. We are not proponents of technological determinism: the view that technology will move on regardless of what we do. However, given the extent to which the values of efficiency and productivity override other

values, the pressures to extend their uses will be intense if it is seen to aid efficiency. Resistance might also be weak. In other areas privacy is being eroded a little at a time in a way that is almost unnoticeable. Imagine if about twenty years ago, before paying for groceries with credit cards was popular, the supermarkets had employed people to sit and watch all customers as they paid, and made a record of their purchases and their names and addresses. Most of us probably would have been a little concerned about this. Now it all happens automatically for those who pay by credit card and/or use loyalty cards, and most people do not give it a second thought. This suggests that what the eye doesn't see doesn't really bother most people and what happens gradually also goes largely unnoticed.

It is here that proactive ethics comes in to play. The argument is not that RFID chips should not be used in libraries because of future dangers. The questions to be asked are: is it morally responsible to use the chips in certain extended ways? And how can the technology be designed to mitigate the dangers? What regulations need to be put in place to control the use of the chips? These are all legitimate questions for the proactive ethicist and their answers should feed into policy decisions about the future use of RFID chips.

## **5. What is an ethical dilemma?**

If ethics is doing the right thing then an ethical dilemma is a scenario in which doing the right thing means that one is also doing, or is about to do, a wrong thing. These dilemmas come in a variety of forms and the overall ethical theory that one holds can make a difference to how they are analysed and assessed. Some dilemmas arise when a choice must be made between two actions, both of which one ought to do. For example, two children are drowning and it is physically possible to rescue only one. A second is where doing the right thing will have serious consequences, for instance in Kant's (1785) liar case in which he argues that one should always tell the truth even if, as in the scenario he describes, it means telling a murderer the location of his intended victim. A third is where there is a clash of principles. This can be the case in the clash between the principles of protecting privacy and that of protecting security, which is often the central issue when discussing the ethics of any kind of surveillance technology.

An important factor in these dilemmas is the overarching ethical theory. From a consequentialist view (Mill, 1859) what makes an action right or wrong is purely its consequences. Some dilemmas can be easily resolved (or are not real dilemmas at all). In the Kantian case, on consequentialist grounds, one should clearly lie given the enormity of the harm caused by not doing so. In the first and third cases, the consequentialist must try to work out which of the actions will have the better, or less bad, consequences. On deontological grounds (Kant, 1785) actions are morally right or wrong in themselves, regardless of consequences. For Kant therefore, the lying case is not a dilemma: one should never lie regardless. In the first case, both actions would be based on the principle that saving life is something that one ought to do, so acting in accordance with that principle does not help; the dilemma remains. In the third example, there is a clash of principles, one concerning privacy and the other security. The deontologist could either appeal to some ordering of principles, or if they are of equal importance, either say that it does not matter what one does, or more likely, fall back on comparing likely consequences.

In analysing ethical dilemmas it is useful to examine the primary role of the participants, e.g. a doctor's primary role is to save life so he or she might feel justified in breaking patient confidentiality in a scenario in which not doing so would endanger the patient's life or those

carrying for him or her. The librarian's professional position of trust with regard to library users, as discussed by Prior (2008) in her analysis of library ethics, can be compared to the duty of confidentiality held by other professions towards their clients, for example doctors, clergy and lawyers. In all these professions, however, it is possible to think of scenarios in which maintaining the duty of confidentiality could cause harm. In all these professions also, particularly in the case of the clergy, the professional will have higher authorities, as well as their actual clients, towards which he or she will also have obligations. We all also, by virtue of living in society, have certain obligations to the social and political structures in which we live, at least if we live in a liberal democracy, on the assumption that we wish to be part of that society. If we are aware that someone is about to harm another person, for instance, and are in a position to help stop that happening then generally we have a social obligation to do so. Is confidentiality an end in itself or just a means to an end, in which case, it can be discounted when it conflicts with that higher purpose? In the medical context, for example, one could argue generally that patients are more likely to tell their doctor important medical details which could save their life if they believe their doctor won't tell everyone about it. The main point, however, is to save life, and confidentiality is a means to that end. So, if we wish to look at the possible ethical dilemmas which librarians may face, it is useful to examine the different people and objects to which they may have obligations, and also to consider their primary role or purpose.

Examining *actual* dilemmas that a librarian may face is obviously part of the role of the ethicist but given the argument of the previous section, an important part of the role is to consider *potential* dilemmas as well. These potential dilemmas can arise because of the introduction of new technologies or through new uses of current technologies. For example, RFID technology that allowed for reading tags at 300 metres would potentially create a dilemma for library management; should such technology be introduced to advance efficiency and security or should it be resisted because of dangers to privacy? The issue here is not only how to solve existing ethical problems but how to avoid or mitigate new ones that can be created through new technologies.

## **6. The role of the librarian**

Here we should distinguish between the overall purpose or function of a librarian and the more practical issues of what librarians do to help them fulfil that role. It is understood that the term 'librarians' covers a range of participants, including librarians at the operational level, who are expected to interpret and implement library/organisational policies, and library managers who are also developers, imposers and monitors of ethical and other policy. Librarians operating at different managerial levels will have differing amounts of influence on the development and implementation of ethical policies; ethical dilemmas raised by new technologies are, however, likely to impact in some way on most of them at some point. Thus we discuss the librarian's role in a general way to provide a context in which to discuss particular dilemmas of competing obligations in the next section. As can be seen in the process model a librarian's role involves a complex set of relationships between many different components and participants in library processes. Can the librarian's primary role therefore be seen as one of being an intermediary and facilitator between the users of the library service and the information objects in the library? By intermediary we mean the librarian has the role of facilitating access to information in a wide variety of ways including aggregating, analysing, describing and publishing information as well as the lending of books

and other information objects. In the context of our discussion on ethical issues of RFIDs the librarian is also potentially an intermediary between information held about library users and the forces of the state who may wish to access that information. Thus the librarian has a particular kind of relationship with the participants in a library process and the nature of this role and its associated relationship has ethical implications.

This doesn't however, necessarily help in determining what their action should be if, for example, the state's security forces were to seek details of the type of information objects that library users were consulting or, in terms of protecting information objects, what to do if they suspected that a particular user was likely to damage or deface particular information objects in the library. Should librarians always put the user first on the grounds that their primary role is to provide access to information to promote knowledge and learning? Is confidentiality just a means to this end since reading and researching in privacy is more likely to promote knowledge and creativity than reading and researching with one's mind on who is looking over one's shoulder? So the role of the librarian is to promote knowledge through access to information and, in most cases, users should be able to do this in reasonable privacy. There may, however, be scenarios in which privacy does not promote knowledge or, rather, in which it promotes dangerous knowledge in the user and possibly dangerous ignorance in the forces of security?

In terms of the more practical tasks which librarians undertake to fulfil their role it is useful to examine these in more detail to see at what point, if any, RFIDs may potentially alter their nature and thus potentially impact on the role of the librarian. As has been outlined in the process model a library service can be seen as a series of inputs (the resources in the model such as information objects) which are processed to produce value-added outputs.

At the production process level input can be seen as resources, particularly information objects, and the output can be seen as the provision of these objects in different formats, modalities and packaging (depending on the service, e.g. current awareness service as distinct from taking out a book) to library users, or access and use by them. At the interaction process or political level the input can be seen as data in a system operated by security services on library user information use patterns (available, say, via library management systems or RFID technologies) and the output as potentially useful information for the state in terms of gathering intelligence on criminal or undesirable behaviour of its citizens. Thus the different participants in library processes include: librarians, users, society, the state, managers and suppliers. The librarian is an active part in these information processes and thus has duties and obligations to a number of different participants at different stages of these processes.

What kind of duties exactly does the librarian have with respect to these different participants in a process? As an intermediary between information objects and their users and, potentially, between the state and the user information it seeks, where should the primary moral obligation lie and what factors or different contexts should change the priority of obligations? If we use the primary role of facilitating access to knowledge and information as a guide does that help answer these questions or just raise new ones? The promotion of knowledge, unlike a doctor's appeal to his or her primary role in saving life, is a far more ethically ambiguous role since it does rather depend on who has the knowledge, what their intentions (and powers) are, and what the knowledge is about.

## **7. Ethical dilemmas in libraries and RFIDs**

In this section we look at some particular duties the librarian may have with respect to different participants in a library process and examine whether RFIDs have the potential to change in any way the nature of those duties and any possible conflict between them. Do RFIDs change how it is possible to find out what someone is reading or researching, and/or the role of the librarian in protecting access to this information? As discussed earlier, this analysis is not only restricted to what is currently happening but also future scenarios that RFID technology may make more likely.

### **7.1 Moral duties to information objects**

We will start with a discussion about the moral duties a librarian may have towards information objects. First, what is an information object? According to Floridi, all objects, be they sticks, stones, atoms, animals or human beings, are information objects, and they all have intrinsic value. There has been recent debate on whether we have moral duties to inanimate information objects and Brey (2008) argues against Floridi's (2003) claim that all information objects have intrinsic value. Rather, Brey argues, inanimate information objects have extrinsic value or alternatively instrumental or emotional value to other people. Thus information objects (we will limit our use to inanimate information objects) are the kind of thing we can have moral duties towards but only inasmuch as they are used and/or valued by other people. They deserve respect not for their own sake but because of what they mean or how they might be used by others. We may, for example, value an information object both in terms of the information itself, a result of the author's work, or because of the container, as in the case of book-binding that reflects the beauty of the binder's or printer's art and craft. We argue then, that in most cases, we do not have moral duties to information objects nor owe them respect, rather we have duties to and owe respect to those people who need them, or those who created them.

In order to make the relation of these possible duties to the role of the librarian clearer, the concept of an information object can be narrowed. While Floridi's broad use of the term has interest, what is required here is some way of picking out those objects with which a librarian typically works and seeing whether they deserve special consideration over and above objects in general. Books, DVDs, paintings and the like contain information in the sense that someone created them with the general intention of communicating something. Therefore it is plausible to argue that, while the books and DVDs have no intrinsic value, librarians do have duties to them typically by virtue of the fact that they are vehicles of communication. By not treating these objects appropriately, their creators are not being respected as they ought to be and neither are those people who should be able to benefit from the information contained in them.

In the case of the potential role of RFIDs in libraries might it be that the moral duty the librarian could have to an information object should be based on how and by whom that information object will be used? In this case, the use of RFIDs to track usage of information objects may be justified depending on one's views of the users. This is following the consequentialist view in so far as the moral obligations of the librarian would depend on the possible consequences or effects that provision of, access to, or use of the object could have. This means that, in certain cases, it may be justified to monitor the use of particular individuals or organisations. Do I, as a library manager, have a moral obligation to prevent the loan of a resource to a member of a group if I know that this group opposes availability

of the resource and that its members have previously been suspected of destroying or altering the resource? This could occur, for example, when secret societies deface publications which threaten to reveal their secrets as in a case known to one of the authors. Is the person or organisation that will use the information object the kind of person that one should have a moral obligation towards? Should one's moral duty towards such a person or group take second place to one's moral duty towards other library users if how the person or group intends to (or actually) use it is likely to have morally negative effects on other library users or people in general? RFIDs make it easier to track who has what information object and perhaps, as it can be tracked outside the library, to ascertain how they might use it. In the case of valuable material being removed from libraries, for instance, an understanding of where, when and by whom they were used would provide an audit trail. There is still, however, the difficulty of how to predict accurately or infer use and then, assuming the former is possible, how to judge whether it constitutes an ethical use of an information object.

So does Brey's appeal to the potential and actual use of information objects as a justification for moral duties assist us in clarifying the ethical implications of the role of RFIDs in libraries as regards information objects? We argue that as an intermediary between information and its use the librarian does have at least some kind of moral duty towards the information objects in his/her care and that RFIDs have the potential to affect how that duty is carried out. Information objects in a library do not just happen to be there but have been collected and organised for a purpose. Thus, in one sense, once an information object is in a library, it has extrinsic or instrumental value. Indeed, collecting institutions such as archives and many libraries have an ethical imperative to collect and preserve information objects, within the parameters of well-established policies. The role of the librarian implies some kind of duty towards the information objects in his or her custody/care. There is already a potential dilemma *within* this duty as one could argue that there is a duty not to limit the use or potential value of an information object and one could also argue that one has a duty to ensure that an information object is not used in an inappropriate or evil way or that it is not damaged or destroyed through use. This is related to the dilemma of allowing access to rare or delicate books in which any use causes damage yet allowing no access or use also seems a failure to value the book. Thus a librarian has to facilitate *and* limit use of the information objects (this indeed is the essence of the lending process). RFIDs can play a role in both protecting the integrity of delicate information objects through increased tracking of their use and also for more mundane information objects, to assist librarians in monitoring their integrity and accuracy in terms of identifying and removing editions with errors. In one sense this is limiting use but it is also facilitating use as it is protecting the integrity of the information object being used.

So in conclusion we argue that librarians do have moral duties towards the information objects in their care because they operate in the role of an intermediary not just as a bystander to the information objects and because a library, by definition, adds value to its contents by virtue of including them in its collection and organisation. There is a tension, and a relationship, between access and preservation, and RFIDs, through increased tracking of information objects, can provide librarians with new information on both, with resulting issues about how that information should be used. Is it, for example, justifiable to use RFIDs to track detailed use of delicate information objects within the library or should the obligation to the library user to have reasonably private research take precedence? As RFIDs



provide the potential ability to track items outside the library, if increased range is possible in the future, what role can the librarian take in using this information when the information object is the library's property but it is also on loan to the user?

## **7.2 Moral duties to library users**

We will now proceed by examining the kind of moral duties that a librarian has to library users. As both librarians and library users are human beings, and thus clearly moral agents or the kind of thing towards which we think we should have moral duties, there is, unlike the case of information objects, less debate on whether these moral duties exist. Rather, the discussion focuses on what exactly they may be and how they are related. Just as the librarian's obligation towards information objects is defined in terms of various humans (information users, potential and actual, authors, publishers and retailers) so his/her obligation towards information users can be defined in terms of information objects (loosely encompassed in the term 'collection'). The clearest obligation is to provide efficient and reliable access to information and, within the context of the reference enquiry, to provide reasonably authoritative information, in so far as taking appropriate steps to ensure the reliability of information provided. (though the provision of such information will, of course, always need to be viewed within certain context-dependent parameters, such as regulatory constraints, strategic objectives, finances and internal policies). A book may be about creationism and while the truth of this view isn't, under normal circumstances, the librarian's concern, there is a duty to make best endeavours to ensure that the catalogue holds correct information about the book as a book. In terms of this obligation RFIDs could be argued to facilitate greater accuracy and currency of information through more effective collection management and the increased speed of book loans enabled by self-service and automation. They can also help to translate corrections in the catalogue to reference and lending activities. For instance, they can help support the authority of information by facilitating the rapid location and removal of books known to have serious mistakes that have been highlighted by a publisher or author, or can ensure that an amended record is still linked to the same information object. There is also an obligation to hold information objects and resources of a valuable or unique nature, e.g. rare first editions, in trust so they can be accessed by everyone, not just a private owner, and RFIDs can help protect such items for future readers. It is if RFIDs are used to draw conclusions about the user based on the actual content of an information object (rather than its catalogue record) that ethical issues may arise.

There is another obligation to protect, to a reasonable level, the privacy of library users in terms of not sharing records about their lending and information use. This obligation can be in conflict with the obligation to provide an efficient service to well-protected information objects. The rationale for the protection of privacy is often linked to free speech (American Library Association, 2004; San Francisco Public Library Technology and Privacy Advisory Committee, 2006) in so far as that one should be allowed to research one's own area of interest without the state or others knowing about it. In this case RFIDs can provide the means, through increased tracking of information items, to facilitate the breaking of this obligation. It also has the potential to break the long established role of the librarian as an intermediary since, at least in principle, others who could crack the RFID's security, could also gain access to lending and information use records. In the technical literature (see for example Molnar & Wagner, 2004; Cai et al, 2009) there does seem to be real concern that a determined user would be able to intercept RFID signals. These people would not (normally)

be in a position of professional duty towards the library user so might use the information for harm. This has serious ethical implications since, if RFIDs reduce the ability of librarians to access information on library users, they increase the likelihood that a person who means harm to the user could access the information

The librarian then could be said to both have a moral duty to protect the library user from clearly misleading information material but also a moral duty to allow them to access information which, even if it is potentially harmful, they should as adult users have the right to access, if they so wish (the case may be different for minors, depending on the jurisdiction). The difficulty then becomes identifying the scenarios, if any, in which this right to privacy in using information should be curtailed because of the interests of wider society or the state. As an information intermediary what kind of role should the librarian play in identifying these scenarios or, assuming the scenario had been identified or at least suspected by a state agency, allowing any breach of privacy?

### **7.3 Moral duties to the state**

This leads us on to a consideration of the moral duties the librarian has to the state. This is itself an intriguing information problem. First, how much information does a state agency need to suspect an individual reliably, and second, how much extra information should it be allowed to access on that individual to either confirm, or at least in principle exonerate, that individual? Suspicion is by its very nature uncertain. In one sense everyone is a potential threat to the state (as indeed, the state is to the individual) but generally, in democracies, the convention is that the state should only collect information or monitor people who constitute a reasonably likely level of threat. All other things being equal citizens should be allowed privacy about how they carry out their lives, certainly in terms of their reading and research habits.

In practice the first question on the burden of certainty is heavily influenced by current political context, either international or national, and the level of actual or perceived threat to the state provides different guidelines on the level of certainty required before proceeding against suspects. This can be seen in the US where The PATRIOT Act<sup>1</sup> has increased government powers to access information on citizens even if the grounds for suspicion were not that strong. Thus the level of certainty required is reduced as the threat to national security is perceived to be high. Librarians as intermediaries or as champions of their users have campaigned against demands for increased government access to library records in the US (Miga, 2007) and also, in some cases, have reduced the amount of information they hold on their users in an attempt to sabotage the process silently. Thus in these cases they, or at least the librarians who protested, have felt that their duties toward the privacy of their users was primary to their duty to the state. This is not necessarily in an absolute sense but because the USA PATRIOT Act measures were seen as overzealous inasmuch as they radically reduced the burden of certainty of suspicion before privacy could be invaded by the state (Prior, 2008). Whether this reduction in privacy protection was or is justified given the raised level of threat, the extent to which this threat remains real or perceived, and, perhaps more pertinently, the extent to which this kind of surveillance has a

---

<sup>1</sup> The official title of the USA PATRIOT Act is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001."

successful track record of actually identifying and preventing terrorists carrying out violent actions, is a difficult question. It raises another potential ethical trade-off or dilemma. What ratio of innocent people under surveillance to criminals being caught is deemed acceptable, or, in the case of mass terrorism, if the potential evil is so great that a larger number of innocent people can be spied on, is there any chance that one of them at some point may commit an atrocity? A recent report (Anon, 2009), by the London police forces revealed that only one crime was solved per 1000 CCTV cameras, raising debates regarding the actual benefits of this kind of surveillance versus its impact on the privacy of the general public.

RFIDs have the potential to change the ways in which state agencies would collect enough information to decide if they could reasonably suspect an individual and the potential to change the type of information libraries would hold on their users, which could then, in turn, be assessed by state agencies. RFIDs also, as they are active away from the library, could allow state agencies to access information on users without necessarily even having to tell the library, thus removing the role of the librarian as an intermediary between users and information objects and therefore protector of the user's privacy. At present the distances over which signals may be read makes this unlikely but if newer types of RFIDs are implemented then there is the potential for the range to be increased, This may prompt concerned librarians to sabotage security processes by deciding not to implement RFID technologies, should they decide that user privacy takes precedence over the many benefits of RFIDs, already noted. An alternative scenario is that the library (not necessarily every individual librarian) abandons any defence of client confidentiality when it introduces RFID technology. The librarian is privy to the link between information object and user by virtue of access to a system or technology, and if the state wants to be privy to that link it can, in principle and perhaps particularly in the US in practice through the PATRIOT Act, enact laws to get it. At the moment the librarian stands between the state and the object/client link but RFIDs provide a new and potentially easier to access means of making the link visible to anyone with technology as good as or better than the library's. Since the security forces are almost certain to have better technology than a library, library managers who introduce RFIDs are, at least potentially, compromising client confidentiality to a greater degree than they did with the introduction of library management systems.

Thus we argue that the librarian does, in some cases, have duties towards the state in terms of assisting in the apprehension of those who pose a serious threat to the state but that these duties need to be balanced against the reasonable expectations of most library users towards their privacy. There is also an important ethical factor in terms of the moral legitimacy of a particular state, in the case of totalitarian regime, in that those who threaten the state probably have more ethical legitimacy than the state itself. Assuming that the state is a reasonably legitimate one, accurately identifying those who do actually pose a threat and deciding how certain one needs to be before proceeding, however, is fraught with complexity and highly dependent on a changing political context and scenarios. In what scenarios is it ethically justified to breach the privacy of either all library users, those library users under a high level of suspicion, or those library users under a low level of suspicion? Even if one believes that RFIDs do not necessarily change the principles of this debate, they do change how, and by whom, information can be collected on library users. Thus, as and if the political context changes, which is something that we have to assume is certainly possible, they provide a new and more effective means for the state to collect information on its citizens. The librarian who is conscious of obligations to users and society, however,

might argue that the game *has* changed since recent laws such as the PATRIOT Act significantly reduce the burden of suspicion required by security forces before they compel third parties (e.g., libraries, doctors, etc.) to hand over client or user records (American Civil Liberties Union, 2003). Thus there is a combination of a changing legal and political framework as well as the development of new technologies which, in principle, facilitate the state's ability to collect information on people. This means that if RFID technologies become widespread in libraries, they may provide another means by which the security forces have the power to invade *anyone's* privacy, particularly if librarians do not take appropriate measures to separate reader, transaction and information object data. In other words, it becomes more possible to make a trawl of people's reading habits, discover who has read a specific items currently regarded as suspicious (as they can already do on the Internet), and identify potential threats using that information. Linking the use of an information object with particular users would require access to the LMS as well as RFID data so, at present, third parties wishing to access data on users would also have to gain access to the LMS. Although accessing the LMS is likely to be a much simpler task than accessing encrypted RFID data it seems reasonable to adopt a cautionary approach, and be wary of any new additional means of collecting data on users.

The principles of the debate regarding privacy, have perhaps not really changed. Rather technology provides a new means to implement surveillance, in which case historical parallels seem relevant. The most obvious parallel with the PATRIOT Act is McCarthyism in the USA during the 1950s, which was characterised by similar arguments about national security and involved the invasion of privacy by the state under measures that radically reduced the burden of certainty of suspicion. We know in this case the outcome in terms of how real the threat was and what role, if any, information collected on individuals had on reducing the threat, versus the negative and often destructive impact on the lives and careers of those under surveillance. Indeed, we now know that many of those affected adversely by the security provisions, for example Arthur Miller, were not, in fact, threats to the state, which raises an issue concerning the accuracy of information gathered. Indeed McCarthyism had the opposite of the stated effect: in trying to discredit communists it created a climate of state control of ideas and creativity rather similar to the communist states of which it was so frightened. It also reveals how the Arts, in terms of what is created or viewed, can be used as evidence against people, which should be of concern to libraries. In the past, evidence of what one read, researched and wrote was normally used to make completely unfounded political conclusions, with terrible consequences for the accused. This was done with the limited technology available at the time so, it is disturbing to consider, what could be done with current technology. It also shows, however, that it is perhaps less important what information on people one collects but rather the political context in which it is collected and the influence that has on how it is interpreted and used. It is the harm that can be caused by the information, which is facilitated by the power and intentions of those who use it, rather than the information in isolation, which is the concern. Any technology including RFIDs, however, that enables and facilitates the collection of such information, provides a potential tool of oppression if the political climate changes.

## **7. Moral duties within the process model**

The discussion so far has identified the librarian's moral duties toward information objects, library users and the state. In terms of the process model these operate at three levels: the relationship between the librarian and information objects, the relationship between the

librarian and his/her library users, and the relationship between the librarian and the external environment including, in particular, the state. RFIDs do have the potential to change this relationship by providing one more way of facilitating access to the relationship between information on users and information objects without consent (either from the user or from the librarian). The difference in RFID technology as opposed to existing technology used in libraries is that it is actually attached to physical information objects and that it has the potential to be tracked surreptitiously within the library and, if the range over which it can be read is increased, possibly outside the library. This in turn changes the ability and ways in which the librarian as intermediary can carry out his or her moral duties.

We argue that in many cases these moral duties can be in conflict or present dilemmas to which there is no clear answer in so far as that they reflect perennial dilemmas about the competing rights of individuals and the collective and, to some extent, information objects. In particular the ethical response to these dilemmas, in terms of where the primary moral duty should lie, is heavily influenced by the particular nature of the information objects (their rarity and value and/or possible negative uses), the library users (Rodota and Capurro, 2005, for example, in their paper on ethical issues in RFIDS in medicine highlight the principle of non-discrimination, i.e. people deserve equal treatment *unless* there are reasons, which are of course difficult to identify, to justify a difference) and the state (in terms of its current political context and indeed on the ethical status of the state, e.g. democracy versus totalitarian regime). How do we solve them?

## **8. Conclusions: possible solutions?**

From our discussion so far we can conclude that RFIDs pose some new threats to privacy in terms of providing one more way for information about library users to be collected. It is not yet clear whether this is a radically different means of collecting information, or just one additional source, but as we suggested earlier, it seems prudent to be alert to ways in which it could be developed, as is highlighted by Palmer (2009), discussed in section 2. At present the ways to reduce this threat are mainly technology or system based in terms of limiting the range of RFIDs and also providing safeguards that data from a RFID cannot be linked to data on a LMS, in line with the ALA Guidelines. This means that it is not possible to connect information from an information object to a user by exploiting the RFID unless one also has access to the LMS. Were it not for these safeguards then RFIDs would definitely pose a privacy threat.

Should the library and information professions regard these as adequate safeguards? Should we be concerned that future developments, either in technology and/or the political climate, will render these safeguards ineffective or even redundant? Wasieleski and Gal-Or (2008) in their discussion of Lessig's (1999) cyberspace framework argue that technological solutions to privacy are always problematic because they require trust from the user that the technology is in fact secure. The problem here is that most users do want privacy but most groups who may wish to gain access to information on users have much to gain from the information and also superior power and technology to gain access than the users have to prevent access. It is not an equal relationship and for it to allay concerns would require a level of trust that not all users will have. There are also legal safeguards, varying from state to state, for the protection of privacy for individuals. These all, however, will have some scenarios in which it is legal to invade that privacy (e.g. reasonable suspicion of ill intent or guilt).

Our main question, however, is whether RFIDs raise new ethical dilemmas for librarians and information professionals. If they are completely secure then some may argue there is no cause for concern. Librarians need also to be aware that this security operates at different levels architecturally: there is the security of the chip and the servers (technology); there is the security of the application (access rights, etc.); there is the security of the data (integrity, encryption); and there is security of the process (completeness, reliability, etc.). None of these is inherently 100% secure and the librarian must be aware of how and where these might be breached and that there are obligations to take appropriate steps to address the threats and mitigate the risks. So are we really looking at the question of the potential role of librarians when these safeguards to uphold security may break down either on a technological or political level, or in some way be perceived to fail? Given that this will almost inevitably happen, at least in some cases, is the development of new technology, in this case RFIDs, worth the risk? Are the benefits more important than the risks and who should make that decision? The benefits of RFIDs are the improvement of service in terms of speed and accuracy for the library user and the librarian. An effective library service requires the accurate collection of data on information objects and library users. At present there are some technological and legal frameworks in place to reduce the likelihood that this data will be used for any other purpose than the efficient running of the library. Connections between users and the information they consult will not normally be given to third parties. The ethical dilemmas may come to the fore in the decision making process about whether a particular scenario is indeed one in which the principle of privacy should take second place to another principle.

It would appear that in dealing with information and library issues, these dilemmas can change in nature particularly quickly, as we are dealing with evidence and information as it is collected and assessed, rather than with a fixed situation as, for example, in Kant's liar case. In that case we already know the caller is a murderer and we already know where the victim is. The question, at least in terms of Kantian ethics, is should we tell a lie (a bad action) to prevent a murder (another bad action)? Privacy and surveillance issues, as potentially facilitated by RFIDs as well as other technologies, within the context of Kant's liar dilemma concern identifying scenarios in which trying to find out if someone may be a murderer (or indeed a victim) become more important than allowing people to live their lives in relative privacy.

Thus we can conclude perhaps that RFIDs provide an additional tool for data collection but that the ethical dilemmas that are raised in terms of what to do with this data are a complex mixture of the exact nature of the technology, which is developing all the time, and the wider context in which it may be used. Both of these are fast developing, hence our argument that we need to look at potential issues that may arise in the future rather than survey the current situation. The problem is for libraries that data collection is so pervasive, with RFIDs an additional factor, that it becomes difficult to be sure that the safeguards, either technological or legal, are adequate, almost certainly in the case of malicious intent (somebody wants to harm a library user) but also in terms of mistaken intent (somebody mistakenly believes a library user is guilty of a crime). A librarian then will find it difficult to be sure that if the privacy of library user is broken that it is indeed to honour a higher ethical principle than privacy in that case. We conclude that RFID technology certainly raises new ethical questions, some of which are very complex dilemmas, for the library and information professions and also that the professions needs to have perhaps a better ethical policy framework to deal with and anticipate these new challenges. In our next paper we look at

different approaches to the development and use of ethical guidelines in the profession and whether current models are still adequate in the context of fast changing technology.

## References

- American Civil Liberties Union. (2003) Surveillance under the National PATRIOT Act. Available from: <http://www.aclu.org/safefree/general/17326res20030403.html>. Last accessed 13/9/2010
- American Library Association. (2004) Policy concerning confidentiality of personally identifiable information about library users. Available from: <http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=78178> Last accessed 13/9/10
- American Library Association. (2006) RFID in libraries: privacy and confidentiality guidelines. Available from: <http://www.ala.org/ala/aboutala/offices/oif/statementspols/otherpolicies/rfidguidelines.cfm> Last accessed 13/9/10
- Anon. (2009) 1000 cameras solve one crime. Available from: <http://news.bbc.co.uk/1/hi/england/london/8219022.stm> Last accessed 13/9/2010
- Brey, P. (2008) Do we have moral duties towards information objects? Ethics and Information Technology, 10(2-3) pp.109-114.
- Butter, A. (2008) RFID for libraries: a comparison of high frequency and ultra high frequency options. APLIS, 21(3), pp.120-134.
- Cai, S., Yingjiu, L., Tieyan, L. & Deng, R.H. (2009) Attacks and improvements to an RFID mutual authentication protocol and its extensions. In: Proceedings of the second ACM conference on wireless network security, Zurich, Switzerland. ACM New York: ACM, pp.51-58.
- Floridi, L. (2003) On the intrinsic value of information objects and the infosphere. Ethics and Information Technology, 4(4), pp.287-304.
- Garofoli, J. & Podger, P.J. (2007) Ethics of library tag plan doubted. San Francisco Chronicle, October 6.
- Gibb, F., Buchanan, S. & Shah, S. (2006) An integrated approach to process and service management. International Journal of Information Management, 26(1), pp.44-58.
- Gibb, F., Thornley, C., Weckert, J. & Ferguson, S. (2010) The application of RFIDs in libraries: an assessment of technological, management and professional issues. International Journal of Information Management. Accepted for publication.
- Ionescu, D. (2010). Google resumes street view driving: more trouble looming? PC World, 9 Jul, 2010. Available from: [http://www.pcworld.com/article/200753/google\\_resumes\\_street\\_view\\_driving\\_more\\_trouble\\_looming.html](http://www.pcworld.com/article/200753/google_resumes_street_view_driving_more_trouble_looming.html) Last accessed 13/9/2010
- Kant, I. (1785) Groundwork for the metaphysics of morals. Translated by Thomas K. Abbott (2005); with revisions by Lara Denis; edited by Lara Denis. Peterborough: Broadview Press.
- Kelly, E.P. & Erickson, G.S. (2005) RFID tags: commercial applications v. privacy rights. Industrial Management and Data Systems, 105(6), pp.703-713.

- Lessig, L. (1999) Code and other laws of cyberspace. New York: Basic Books.
- Lockton, V. & Rosenberg, R.S. (2005) RFID: the next serious threat to privacy. *Ethics and Information Technology* 7, pp.221-231.
- Miga, A. (2007) Librarian who resisted FBI says Patriot Act invades privacy. *The Washington Post*, 12<sup>th</sup> April, p.12. Available from <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/11/AR2007041102041.html> Last accessed
- Mill, J. S. (1859) *On liberty: annotated text, sources and background criticism*. Edited by D. Spitz (1975). New York: W.W. Norton.
- Molnar, D. & Wagner, D. (2004) Privacy and security in library RFID: issues, practices, and architectures. In: *Proceedings of the 11<sup>th</sup> ACM conference on computer and communications security*, Washington DC. ACM: New York.
- Moor, J. & Weckert, J. (2004) Nanoethics: assessing the nanoscale from an ethical point of view. In: J. Schummer & A. Nordmann (eds). *Discovering the nanoscale*. Amsterdam: IOS Press.
- Organization for Economic Co-operation and Development. (2008) *Radio frequency identification*. Paris: Organization for Economic Co-operation and Development.
- Palmer, M. (2010) *Making the most of RFIDs in libraries*. London: Facet Publishing.
- Prior, J.L. (2008) *Library ethics*. Westport: Libraries Unlimited.
- Rodota, S. & Capurro, R. (2005) Ethical aspects of ICT implants in the human body. *Opinion of the European Group on Ethics and New Technologies*, No. 20. Available from: [http://www.ec.europa.eu/european\\_group\\_ethics/docs/avis20\\_en.pdf](http://www.ec.europa.eu/european_group_ethics/docs/avis20_en.pdf) Last accessed 13/9/2010
- San Francisco Public Library Technology and Privacy Advisory Committee. (2005) *Radio frequency identification and the San Francisco Public Library*. San Francisco: LTPAC.
- Sletteemeås, D. (2007) RFID – the "next step" in consumer-product relations or Orwellian nightmare? *Journal of Consumer Policy*, 32(3), pp.219-244.
- Timson, L. (2010). Facebook bows to privacy pressure. *The Sydney Morning Herald*, 27<sup>th</sup> May. Available from: <http://www.smh.com.au/technology/technology-news/facebook-bows-to-privacy-pressure-20100527-wgho.html> Last accessed 13/9/2010
- van de Poel, I. (2008) How should we do nanoethics? A network approach for discerning ethical issues in nanotechnology. *NanoEthics: Ethics for Technologies that Converge at the Nanoscale*, 2, pp.25-38.
- Various. (2010) The power and pitfalls of RFIDs. Available from: <http://www.libraryjournal.com/webcasts> Last accessed 12/9/2010
- Wasieleski, D.M. & Gal-Or, M. (2008). An enquiry into the ethical efficacy of the use of radio frequency identification technology. *Ethics and Information Technology*, 10(1), pp.27-40.
- Williams, M. (2010) Nano-based RFID tag, you're it. Available from: <http://www.media.rice.edu/media/NewsBot.asp?MODE=VIEW&ID=13899> Last accessed 13/9/2010