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

Contents lists available at ScienceDirect

International Journal of Information Management

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

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

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

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

ARTICLE INFO

Article history:
Available online 13 August 2010

Keywords:
Ethics
Radio frequency identifiers
Library management
Processes

ABSTRACT

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

1. Introduction

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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