



**A Privacy Code of Conduct
for RFID Technologies**

Enterprise Privacy Group

3rd May 2005

**Enterprise Privacy Group
Old Bank House
59, High Street
Odiham
Hants RG29 1LF
T: +44 (0)1256 702325
F: +44 (0)1256 702375
W: www.privacygroup.org**



A Privacy Code of Conduct for RFID Technologies

Toby Stevens, Enterprise Privacy Group

Introduction

Radio Frequency Identification (RFID) technologies enable the remote identification of any object to which a suitable 'tag' has been attached, and have a broad range of applications, such as stock control, theft detection and security access control. The application of RFID for mass serialisation of any group of items – or people – is fast becoming one of the most important technologies in identification systems.

However, the potential for misuse of the technology gives rise to significant privacy concerns. RFID tags can be used to monitor the location of individuals without their knowledge; secretly build up a detailed profile of the individual based upon items in their possession; or even to impersonate individuals by replicating their RFID tags. Organisations that implement consumer-facing RFID Systems without first considering these possibilities have suffered adverse media publicity from watchdog groups, and in consequence have had to modify or abandon their plans.

Any RFID implementation should therefore incorporate privacy safeguards, based upon a rigorous risk assessment process coupled with 'best practice' recommendations for controls. One such control is a Code of Conduct to ensure that every user associated with an RFID System understands their responsibilities for protecting personal information, and acts accordingly. Such a Code of Conduct is described below.

What is RFID?

Radio Frequency Identification (RFID) is the name given to a group of technologies that can be used to remotely identify an item to which a suitable transponder has been attached. An RFID system has three main elements:

- the *tag* comprises a processor and antenna, and can be any size upwards of a few millimetres diameter;
- the *reader* contains a radio frequency module to transmit an interrogation signal to the tag and receive the response. The reader may also have an on-board computer, and will normally have an interface to the host computer system;
- the *host computer system* manages the information generated by the tag and reader.

The usable range of the RFID tag to the reader can be any distance from a few millimetres upwards, and in certain applications can be many miles. Tags most commonly take their power from the electrical resonance of the reader, but can have their own power supplies, on-board rewritable data storage, or built-in sensors for temperature, pressure etc.

The concept of RFID is not new: the earliest incarnation was the Identify Friend or Foe (IFF) system developed during the Second World War to verify the identity of inbound aircraft from distances of 25 miles or more. It was only in the 1980s that small RFID tags became commercially available for applications such as stock control or security.

Recent years have seen a rapid acceleration in RFID technologies. A key development in the commercial viability of RFID has been the development of the Electronic Product Code (EPC) initiative¹ by a group of companies and academic institutions. EPC provides a standard that allows each RFID tag to carry a unique code that incorporates information about the item to which it is attached, and provides users with information to interpret that code.

¹ <http://www.epcglobalinc.org/>



RFID Applications

Applications for RFID technologies can generally be categorised into four groups:

- *Electronic Article Surveillance (EAS)* systems: mostly used in retail stores as a security control to sense the presence or absence of an item;
- *Portable Data Capture* systems: use an independent or wireless-connected portable RFID reader, most commonly in warehouses or retail stores for stock control;
- *Networked* systems: use fixed RFID readers which are connected directly to a central information management system, and are particularly common for handling of bulk items in factories;
- *Positioning* systems: used to identify the location of individuals, vehicles or other items. These systems can incorporate 'active' RFID technologies that can increase the range of the system up to many miles.

It is likely that the boundaries between these groups will become blurred as the technology continues to develop and new uses are found for RFID.

The Privacy Impact of RFID

Despite their potential for beneficial applications, RFID technologies are almost unique in their ability to impact personal privacy in any of the four 'dimensions' of privacy:

- *territorial privacy*: RFID tags can be used to monitor the location of the individual carrying them, derive information about the items around that individual, or track the movements of items such as banknotes between individuals;
- *bodily privacy*: RFID tags with in-built sensors can be used to monitor the health of an individual, or even be embedded in their skin to track their movements²;
- *communications privacy*: a letter, package or banknote can be tracked with an RFID tag;
- *data privacy*: RFID tags embedded in tokens are now commonly used as authentication mechanisms for computer users.

Clearly these impacts give cause for concern, particularly amongst privacy advocates³, who argue that RFID technologies may be deliberately or unintentionally used to undermine civil liberties in a number of ways:

- *hidden tags*: RFID tags can be secretly affixed to objects and documents, and then used to track the movements of the individual or build a profile of the individual by aggregation of the tags in that individual's possession (for example, clothing sizes and styles, medicines, electronic devices);
- *hidden readers*: if RFID readers are secreted into doorways, floors, counters etc. then the individual has no way of knowing when tags in their possession are being read, or for what purpose;
- *hidden processing*: if the use of tags is associated with personal data, then it becomes possible to profile an individual based upon the tags in their possession (whether they know about the tags or not). Individuals can be associated with other individuals simply by proximity (for example at political rallies) or have complex marketing profiles associated with them and used by retail organisations.

² http://zdnet.com.com/2100-1103_2-5285815.html

³ <http://www.privacyrights.org/ar/RFIDposition.htm>



There are also risks arising from the use of duplicate RFID tags (where a false tag is reprogrammed to appear legitimate) or the destruction of data on existing tags; items could then be stolen, diverted, disguised or tracked by an attacker. Counterfeit or stolen products could be returned to a retailer for a cash refund by adding a duplicate tag. Simple tools to permit this are readily available.⁴

Managing RFID Risk

Any organisation that pilots or implements an RFID-based system should carefully consider the potential impact that the project may have. Companies that have identified clear commercial benefits that can be gained through the use of RFID in applications such as stock control, security, patient safety or loyalty management have been subject to organised campaigns by privacy advocates, many of which have attracted significant adverse media coverage.⁵ Such problems are nearly always avoidable, and if RFID users are to avoid reputational damage – and the risk of legal action – then privacy-related risks should be considered prior to implementing an RFID system. This is best achieved through a risk management process, which should address a number of key questions including:

- Will RFID tags be affixed to items that may pass beyond the control of the organisation (such as consumer goods)?
- Is it really necessary to store or process personal information within the RFID system?
- Does the potential impact of a privacy-related incident outweigh the possible benefits arising from the use of RFID technologies?
- Can the organisation ensure that every employee and partner organisation will respect the privacy of personal information, and use the RFID system in the intended manner?

This last question is particularly important, since no amount of privacy or security controls will function correctly if the RFID system is open to accidental or deliberate abuse by authorised users. A Code of Conduct for system use can be an effective mechanism to reduce the risk of abuse, and protect both the organisation and the individual in the event of a problem.

The Code of Conduct

Because of the potential for the accidental or deliberate misuse of RFID technologies when they are associated with personal information, any organisation that implements RFID should ensure that all stakeholders understand what constitutes acceptable use of the system. This is particularly important since the public are generally unfamiliar with RFID or its potential impact on personal information.⁶

This Code of Conduct was derived from recommendations of RFID technology providers,⁷ Information Commissioners⁸ and privacy rights bodies,⁹ coupled with real-world experiences and risk assessments of RFID implementations. Several civil liberties groups have reviewed the an earlier version of the Code, and whilst some of those groups remain opposed to the use of RFID in principle, the Code was greeted as a positive development in protecting individual privacy.

⁴ <http://www.rf-dump.org/>

⁵ <http://www.spychips.org>

⁶ Research by Aegate Ltd, <http://www.privacygroup.org>

⁷ <http://www.epcglobalinc.org>

⁸ <http://www.ipc.on.ca/docs/rfid-lib.pdf>

⁹ <http://www.privacyrights.org/ar/RFIDposition.htm>



Key Principles of the Code of Conduct

The key principles that underpin the Code of Conduct are as follow:

- the RFID system and any data stored or processed within it should be ***used only for the stated purpose***;
- the organisation operating the system should be ***transparent about the system's purpose***, the technologies used, the locations of RFID tags and readers, and who is accountable for the proper use of the system;
- the system should be ***protected by appropriate security controls***, and subject to internal and independent audits;
- RFID tags should ***not be used to store or process personal information***. Any other data should be erased from the tag before it is released from the organisation's control;
- where personal data must be associated with the system, that ***personal data should be limited to that which is required for operation of the system***, and should be destroyed after use;
- no member of the public should be forced, coerced or tricked into accepting an item with an RFID tag attached. The ***public should be able to remove or destroy tags***, and provided with instructions on how to do so.

Use of the Code of Conduct

The Code of Conduct is primarily intended for situations where RFID tags are affixed to consumer items, such as retail goods or pharmaceuticals. However, the principles apply to any use of RFID technologies, and the Code requires little modification to other scenarios, so long as the organisation adopting the Code does not intend to track individuals or covertly gather information about them.

Information should be inserted in the Code of Conduct where indicated by brackets eg [...].

Legal

Note that this Code of Conduct has not been scrutinised by legal experts. Any organisation adopting the Code of Conduct should ensure that it is subject to legal review.



A Code of Conduct for the Use of RFID Technologies

Purpose

[Organisation] is using RFID technology to [purpose of application]. Any change to this purpose will be made clear to all affected parties and reflected in this Code of Conduct.

Privacy stance

It is the intention of [Organisation] that the RFID System will in no way undermine the privacy of the individual.

Legal

The RFID System is owned and operated by [Organisation], a [nationality] company with registered offices at [address]. All data will be stored and processed in [country]. The RFID System is subject to [nationality] legal requirements, and will be operated in compliance with those laws.

Applicability

This Code of Conduct applies to all employees of [organisation] and any partner organisation that may handle RFID tagged items or the data associated with or derived from those items.

Compliance with this Code of Conduct

[Organisation] and its partner organisations will operate effective security, privacy, employee confidentiality and employee conduct policies that apply to all individuals, processes and computer systems that are associated with the RFID System.

[Organisation] will supply appropriate education and training to all employees and partner organisations to ensure compliance with this Code of Conduct and other relevant policies. This should include ensuring that all employees and partner organisations are aware that their activities are subject to audit and that they may be called upon to justify any misuse of the RFID System.

[Organisation] will obtain written acknowledgement from employees and partner organisations to confirm that they have read and understood the Code of Conduct and relevant policies, and have agreed to abide by the requirements therein.

[Organisation] will investigate any incident or breach of this Code of Conduct or other relevant policies, and instigate disciplinary proceedings against any employee who has knowingly breached the Code of Conduct, other relevant policies or applicable laws. [Organisation] reserves the right to terminate its relationship with any partner organisation that deliberately or repeatedly misuses the RFID System.

Management

[Organisation] will designate a senior staff member (known as the RFID System Manager) to be responsible and accountable for managing obligations under this Code of Conduct.

Oversight

[Organisation] will self-assess compliance with the operational policies and procedures; audit partner organisations to ensure their compliance; and ensure that all aspects of the RFID System are regularly audited by an independent third-party organisation.

The RFID System Manager should immediately rectify any deficiencies or concerns identified by any of these audits.



Use of Personal Information

Any personal information obtained or stored using RFID technologies will only be used for the stated purpose.

No personal information, or any identifier that is used to link to personal information, may be written to an RFID tag at any time. Where there is a requirement to associate the RFID tag identifier with personal information, the personal information will be held in an external system, and cryptographic controls will be used to ensure that while the RFID tag number may be used to link to personal information, details of the tag(s) associated with an individual(s) cannot be derived from their personal information.

Technology

The RFID System will use 'passive' short-range tags / 'active' RFID tags (those that incorporate their own independent power supply or on-board processing *[delete as applicable]*). These tags may / may not *[delete as applicable]* incorporate Electronic Product Code (EPC) technologies.

The use of read/write RFID tags (those that permit the embedded data to be changed) is permitted subject to ensuring that the rewritable component is erased prior to the RFID tagged item being forwarded to another party. *[Organisation]* will audit to ensure that this takes place.

RFID tags will be issued in a non-sequential pseudo-random order to prevent the possibility of guessing information about the item to which a tag or group of tags are affixed.

The data stored in the RFID System will be limited to that which is necessary for the operation of the application.

Retention of Information

There will be only one record of the RFID tag numbers, and this will not be copied into any other system except for archive/backup purposes. RFID tag information, and any associated personal information within the RFID System, will be destroyed as soon as its purpose of use is complete.

Transparency

[Organisation] will be as open as reasonably possible about the use of RFID technology. The RFID System Manager will make available any reasonable information about the system to any individual or organisation that may request it.

Where RFID tags are affixed to items that may be passed to the public, the presence and location of RFID tags will be clearly marked, together with links to further information about their use. Information should include provision of signs, leaflets, Internet web pages and a telephone helpline.

Any member of the public receiving a RFID tagged item will be offered the opportunity to remove the tag or transfer the item to packaging that does not include an RFID tag if they so wish. *[Organisation]* will not force or coerce the public into accepting RFID tags on items or packaging.

Members of the public may read, remove or destroy RFID tags in their possession, and will be provided with instructions on how to remove them if requested. This will not affect their statutory rights, so long as the item to which the tag is affixed is not damaged.

There will be no mechanism provided to render RFID tags inoperable or dormant, since such mechanisms may prove to be unreliable or ineffective.

[Organisation] will not knowingly permit any other RFID tag (including hidden tags) to be affixed an item or its packaging.

All RFID readers will be clearly marked to indicate their presence, and will be located in 'obvious' positions, i.e. on a counter as opposed to in a doorframe. The use of hidden or unmarked RFID readers will not be permitted.

RFID readers will be marked with a summary of the purposes for which the RFID tags and RFID readers are used.



Where RFID tags may be passed to the public (eg in a retail environment), the public will be informed of the purpose and implications of the RFID System, including:

- the location of RFID tags and RFID readers and which personnel are authorised to operate the RFID System;
- the type of RFID tags in use and their readable range;
- the exact nature of the information embedded in the RFID tags.

Tags will not be tracked after the point that their intended use is complete, and the tags will not be used other than for the stated purpose.

Security

All components of the RFID System, and the processes used to manage them, will be subject to security controls to prevent the loss, theft or modification of information. This includes components and processes operated by *[Organisation]* or any partner organisation. The controls will take into account the requirements of ISO17799, the Code of practice for information security management, and will comply with those requirement where appropriate.

Any security incident will be reported immediately to the RFID System Manager, and will be fully investigated in a prompt and efficient manner. Where the impact of the incident may involve loss or disclosure of personal information, *[Organisation]* will endeavour to notify the affected individual(s).

Redress

[Organisation] will endeavour to handle Subject Access Requests under the Data Protection Act promptly and accurately. No fee will be levied for requests relating to the RFID database, and any payments offered will be returned to the sender with their report.

Enquiries

All enquiries regarding the system should be passed to:

[RFID System Manager contact details]



About the Author

Toby Stevens is a Director of Enterprise Privacy Group (EPG), a consulting firm that is committed to the development of excellence in data protection, freedom of information and related privacy issues. EPG consults to business, academia and central government organisations on topics as diverse as Radio Frequency Identification (RFID) technologies, data protection awareness and identity cards. Toby has worked in privacy and information security management for the past 13 years, in roles that cover finance, technology, life sciences and consultancy. He specialises in analysing and resolving problems associated with privacy management, and establishing privacy as a business enabler.

**Enterprise Privacy Group
Old Bank House
59, High Street
Odiham
Hants RG29 1LF
T: +44 (0)1256 702325
F: +44 (0)1256 702375
W: www.privacygroup.org**

