

# RFID



## RFID : Private & Personal or Open & Public?

*CoreRFID's views on the use of RFID and personal privacy – advice to users.*

RFID tags differ from other devices storing personal data because of their ability to be interrogated without the holder being aware. What does that mean for the design of RFID systems?

### What's Different About RFID & Personal Data?

A feature of RFID tags is that the data held on them can be accessed without the tag being placed in a reading device. Indeed for some variants of RFID technology, tags can be accessed and data read from a distance of several metres.

With this ability it is perfectly possible for data held on an RFID chip to be accessed without the intervention or knowledge of the individual carrying the tag. And, with tags becoming progressively smaller, someone carrying a tagged item may not even be aware of the fact that they have one. Further difficulties result because data from multiple tags can potentially be associated, providing information about the the carrier of the tag that they do not intend to divulge. Also data placed on a tag for one purpose (inventory control, say) might then be used for some other purpose (purchaser behaviour and usage monitoring). As a result concerns have been expressed over the use of personal data in conjunction with RFID systems. How should systems be designed to respond to these concerns?

The problems that have to be addressed fall into two main categories; those involving explicitly stored personal data (either on tags or in data files accessed by reference to the data on the tag); and those due to the ability of the tag data to be used with other tag data in a context. Examples of the first kind of data might be a personal identity or account number, details of an individual's home address, or their age. Examples of the second kind of data include the fact that they were at a certain position at a certain time, that they had collected certain items together in a shopping trolley, or that an individual carries a collection of RFID tags (different loyalty cards from multiple stores, for example).

Personal data stored on or held in a way related to an RFID tag is covered (in the UK) by the provisions of the Data Protection Act 1998. This requires that personal data is not held without the consent of the data subject, not stored for longer than necessary and held only for registered purposes. This is the minimum for the handling of personal data in RFID systems.

Handling of personal data in RFID based systems has been considered by the EU as part of its programme to promote the use of RFID technology. This programme understands that for business to gain benefits from RFID there must be public confidence that data is not deliberately misused, accidentally misused or fraudulently accessed. This issue of public confidence on aspects of RFID security and privacy is also being addressed by various groups concerned with personal liberty.



**How will privacy concerns and the potential offered by RFID systems be reconciled?**

Concerns over "skimming" (illicit access to card data) have been increased by recent demonstrations<sup>i</sup> that have shown that a passive, ISO1443 compatible, RFID tag (normal read distance circa 5cm) can be read from 25cm with sub-\$100 technology purchased from an electronics hobby store and by the exposure of deficiencies in the security mechanisms of the first generation of MiFare (passive, high frequency) tags. However, as has been demonstrated by the rapid growth in the use of magnetic stripe or chip +pin cards and by the rapid growth in internet shopping, public acceptance can be driven by perceived value over the perceived risk of security deficiencies.

As yet, no RFID specific legislation has been enacted in Europe. The European Data Protection Supervisor has published views<sup>ii</sup> on the potential future of EU RFID legislation which include recommending legislation to prevent information being used beyond the point of sale without the data subject's consent, even if this only becomes personal data by association. At the time of writing the EU has just published their recommendations on how this issue will be addressed by Member States.

In the USA, however, around 20 states have implemented or are implementing legislation relating to RFID. In 2006, the state of Wisconsin enacted legislation banning human implanting with RFID chips without the subject's consent. The state of Washington enacted legislation in 2008 relating to the issue of personal data privacy in relation to RFID systems. Most recently in New Hampshire (Jan 2009) a more widely reaching law has been enacted that requires consumer products or identification documents with remotely readable devices to include a consumer notice to that effect, that prohibits the implantation of a remotely readable device in a human without the individual's informed, written consent, that prohibits electronic tracking of another individual (except by the emergency services) and requires that any tagged consumer product can be deactivated or the tag removed at the consumer's request, without the consumer being treated any differently from those that are prepared for the tag to remain in place. As yet no Federal legislation has been put forward.

The effect of individual states legislating and a lack of impetus behind federal legislation in the USA or EU-wide legislation is likely to lead to a considerable period of uncertainty over privacy issues, especially as technology continues to develop.

## Issues For Systems Designers

This uncertainty makes it difficult for those planning public-facing RFID systems. CoreRFID consider that the best way of addressing personal privacy issues in RFID systems is to minimise the potential impact of any future legislative initiative and to most encourage public confidence in the security and privacy associated with RFID usage. Systems designers should include the following design criteria in systems where the public is likely to be come in to contact with RFID enabled products:

1. Designers should ensure that any personal data on or linked to an RFID tag is handled in accordance with the provisions of the Data Protection Act and the best practice guidelines published by the Information Commissioner.
2. Where RFID data (for example items purchased) can be linked with personal data (for example a credit card), the data subject should give their informed consent for the combined use.
3. Designers should build in to the overall system the need for data subjects to opt in to the usage planned at any stage where the usage of the data changes.
4. Systems need to provide for disabling the RFID tags affected if data subjects decide to opt out of RFID enabled services.
5. Networks of RFID tags and readers should be designed to include appropriate security measures to minimise the risk of impersonation (by tags or readers) or interception of traffic.

## About CoreRFID

Contact us at:

CoreRFID Ltd. Dallam Court, Dallam Lane, Warrington, U.K. WA2 7LT

T: +44 (0) 845 071 0985 F: +44 (0) 845 071 0989 W: [www.corerfid.com](http://www.corerfid.com) E: [info@corerfid.com](mailto:info@corerfid.com)

<sup>i</sup> Kirschenbaum & Wool, May 2006, School of Electrical Engineering Systems, Tel Aviv University

<sup>ii</sup> Opinion of the European Data Protection Supervisor on ... 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework' COM(2007) 96. (23/4/2008, Official Journal of the EU, C101)