

What's the frequency - are RFID tags a threat to privacy?

Although it has been around for well over 20 years, it has only really been in the last 18 months that RFID has become newsworthy in the mainstream press. In that time, however, RFID has gone from being perceived as merely a useful technological advance to being viewed as a possible threat to the privacy of the world's citizens.

Tags in our money, our post, our clothes, our food, our car tyres, our credit cards, our passports, our bodies: are these merely privacy advocates' paranoid fears, or are there real issues of concern at stake?

What is RFID?

RFID or Radio Frequency Identification is an automatic non-contact identification system, similar in concept to a barcode, but far more robust and sophisticated. An RFID tag can be read through fur, snow, paint, clothing and skin. The system works by using an RFID reader to read information/data stored on an RFID tag. The data on the tag may provide such information as location, identification details, price, colour, size, date etc.

Tags are categorised as either active or passive:

- *Active tags* are powered by an internal battery, with the ability to rewrite and modify the data on the tag. These tags can operate with up to 1MB of memory.
- *Passive tags* operate without an internal battery and obtain their operating power from the tag reader. These are the less expensive version of the tags and, due to the lack of their own power source, only have a short read range.

It is in the latter category that the real potential for the growth in RFID lies. Industry analysts predict that the value of the RFID market is set to more than double between 2002 and 2008 from \$1.15 billion to \$3.1 billion.

The attractions of RFID, especially in the supply chain, are obvious. The ability to track the whereabouts of goods as they pass from the factory along the distribution network, to the shop or retailer and eventually to the customer via the point of sale, is one that all producers would like to possess. This ability to track goods in real time would help manufacturers and retailers reduce losses and theft. A recent study by Vanson Bourne found that 41% of European retailers were planning RFID pilot programs in 2004.

History

The barcodes comparison is a good one. It seems like barcodes have been with us for so long that they have become ubiquitous. Yet, while the patent for barcodes was issued back in 1952, it wasn't until the mid-1980s that Wal-Mart decided that barcodes would be a more effective way to manage its inventory and informed anyone that wanted to do business with the company that they should start using them. And when Wal-Mart shouts jump, the thousands of small business and suppliers that rely on Wal-Mart for their business shout, 'How high?'

The grocery chain has now asked its 100 biggest suppliers to ensure that all their companies use RFID by 2005, and wants all of its suppliers to have converted to the technology by 2006, suggesting that the barcode's days may be numbered.

That said, barcodes are still likely to be around for many years to come because of their perceived cost-effectiveness for most businesses. Whilst the cost of RFID tags is falling - now around 20p (35

cents) each - the cost of a barcode is almost zero. This of course ignores the potential saving businesses could make through using RFID tags and minimising theft. Even so, the initial outlay would be huge for most companies. Not until the price per tag falls to around 1-2p a tag is that cost likely to become feasible.

Standards

A possible barrier to the widespread use of RFID has arisen regarding the frequencies deployed and the standards adopted. The main standards body for RFID technologies is Electronic Product Code Global (EPCglobal). The RFID standard it created - the Electronic Product Code (EPC) standard - was the result of an agreement between standards bodies EAN International and the Uniform Code Council (which oversee the barcode system). The EPC coding structure is made up of:

- the Object Naming Service;
- the tag (physical implementation); and
- the air interface.

The EPC is a unique 96-bit number that identifies a specific item in the supply chain. The EPC is stored on the RFID tag. The tag is detected by a reader, which passes the number to a computer or local application system, known as the Object Naming Service (ONS). ONS tells the computer systems where to locate information on the network about the object carrying an EPC, such as when the item was produced. EPCglobal has selected VeriSign Inc to maintain the key electronic product codes ONS system for EPCglobal.¹

The service will function along similar lines to the Domain Name System that VeriSign now operates. When a pallet, package or individual item passes an RFID scanner, the scanner will look up the EPC code contained in the tag on the 'root' ONS run by VeriSign. This directory will contain all the important data related to that product code, before pointing to more detailed information on local manufacturer-maintained ONS servers.

Interestingly, Wal-Mart has announced that it has no current plans to use the Verisign-operated EPCglobal Network and ONS, preferring its suppliers to communicate RFID data via its RetailLink extranet and electronic data interchange systems.²

On the international front, the International Organization for Standardization is making progress on a number of standards related to the use of RFID in the supply chain. The ISO committee cleared drafts of six of the seven proposed standards (ISO 18000 parts 1-7). These primarily cover the 'air interface', or the way readers communicate with tags, not the content or the physical implementation of the tags and readers.

ISO 18000-6, which covers the air interface for RFID tags operating at ultra high frequency (860-930 MHz), is perhaps the most important standard because UHF is widely seen as the frequency that will be used for supply chain applications, and is the frequency favoured by EPCglobal. The remaining standards cover frequencies at 13.56 MHz, 2.45GHz, 433MHz, and below 135KHz. ISO 18000-5, which covers the air interface for tags operating at 5.8 GHz, was rejected in 2003 and will not become a standard unless an ISO member re-introduces it.

As the ISO standards only deal with the air interface, it seems logical and beneficial that at some point in the future EPC will need to adopt the ISO standards in preference of its own interface to ensure interoperability. The standards are expected to be fully approved early this year.

Be afraid, be very afraid

Privacy advocates argue that RFID technology could become one of the biggest threats to the civil liberties and privacy of the world's citizens. Imagine a world where you could be tracked by what you are wearing, what you buy, your National ID card, or even by a chip embedded under your skin. Is this George Orwell's 'Big Brother' or the plot from that latest sci-fi blockbuster? All fantasy? Well maybe.

Even the most paranoid privacy advocate would be hard pushed not to accept that using RFID tags for logistical purposes, to track goods from manufacture to the shop floor, is a valuable and acceptable use of the technology. According to Marks & Spencers' Technical Director, James Stafford, consumers have nothing to fear. Stafford told the *Financial Times* in November 2003 that 'the business case doesn't require us to scan at check-outs, and we've no plans to do that at all in future'.³

This sounds reassuring, but supermarket chain Metro sees a different world where when entering one of their stores, the shopping trolley will recognise your store card, tell you what you bought last time and offer to guide you through the store suggesting what to buy based on the profile it has developed from previous purchases. Once you have finished, the trolley will have added up the cost of your purchases and will debit the total from your credit card/store card as you leave the store.

Where does it all end? RFID in birth certificates? University degree and diploma certificates? RFID in us - humans? Designed for people, the VeriChip RFID tag made by Applied Digital Solutions is injected under the skin. The company markets VeriChip as an ideal method of controlling authorised access to prisons, government buildings and nuclear power plants. It also feels that VeriChip could help curb identity theft and prevent fraudulent access to banking and credit card accounts. The manufacturer sees the chip as the ultimate tamper-proof personal verification technology, which could function on its own or with standard ID badges and advanced biometric devices.⁴

VeriChip is also being seen as a way for hospitals to keep track of patients - and was used by some hospitals during the recent SARS outbreak. Governments are trying to sell the idea to parents as a great way to keep track of children. What price babies tagged at birth?

The possible nightmare scenarios continue when we get onto the issue of money. Visa has already started combining smart cards and RFID chips in South Korea. The smart cards can be installed in mobile phones and other devices, and allow people to pay for items from a vending machine without opening their wallets just by waving the device containing the card close to the terminal. Wireless transmissions would conclude the electronic payment.

Governments and banks are also looking at tagging our currencies (the European Commission is very keen on the idea of tagging the Euro). Were it to be allowed to be embedded in money, one of the last genuinely anonymous ways of living our lives would vanish in an instant. Such a move would make it technologically possible for banks to know exactly how much money you were carrying and would allow governments to track the passage of cash from person to person. Useful information for banks? Maybe. It would certainly be very useful for those in other lines of work. Criminals with transceivers able to spot the best targets for their crimes, by being able to divine exactly how much money a person was carrying before they relieved him of it.

Many people are now starting to fear that literally everything on the planet, us included, could one day be tagged. In the US, this has led the Electronic Privacy Information Center (EPIC) and a coalition of privacy organisations to produce a position paper on the use of RFID in consumer products, recommending a framework of Fair Information Practices for data collected by the technology.⁵ The coalition recommends following a set of minimum guidelines based in part on the eight-part Privacy Guidelines of the Organisation for Economic Co-operation and Development (OECD) while the larger assessment of RFID's societal implications takes place.⁶ The position paper argues that RFID must undergo a formal technology assessment, that RFID tags should not be affixed to individual consumer products until such assessment takes place, and that under no circumstances should

some uses of RFID be permitted, namely:

- Merchants must be prohibited from forcing or coercing customers into accepting live or dormant RFID tags in the products they buy.
- There should be no prohibition on individuals to detect RFID tags and readers and disable tags on items in their possession.
- RFID must not be used to track individuals without the informed and written consent of the data subject. Human tracking is inappropriate, either directly or indirectly, through clothing, consumer goods or other items.
- RFID should never be employed in a fashion to eliminate or reduce anonymity. For instance, RFID should not be incorporated into currency.

Killing the tags

Can the tags be killed? There are several ways to kill or disable the tags. You can puncture them, crush them and microwave them. Of course, you need to know that the item is tagged to begin with and then you need to actually find the tag itself before you can do this. The microwaving method is a particularly interesting one. For starters, where money is concerned, money laundering would soon be replaced by money microwaving. But this in itself could prove problematic. If as a law-abiding citizen you decided to microwave your money to kill the tags, you may then be seen as suspicious for carrying non-tagged money and, almost certainly - with every shop equipped with a reader to look for the tags to ensure the money's legality - your money would be presumed to be counterfeit unless it contained an active tag. Indeed, were tags to be introduced into currency, it seems certain that legislation would be introduced to make sure that tampering with the tags would be illegal. On individual items, shops could disable the tag at the time of purchase. But how would you know that the tag could not then be reactivated?

Is there a law against it?

No one is suggesting that RFID is illegal, or indeed should be, but certainly, if used at item level, there would be legal issues. There is little doubt that current privacy and data protection laws *will* catch RFID. In Europe, any personal data collected and processed in relation to RFID would have to comply with EU data protection law in the form of the Data Protection Directive 1995. So any data would need to be processed fairly and lawfully, be used for specified, explicit and legitimate purposes, and not be kept for longer than is necessary. The person or organisation collecting and processing that data would also have to inform the individual of that fact and the purpose(s) of the data collection. Under the Directive, the data controller would, given the fears that anyone with a RFID reader will be able to read the tag information, need to make sure appropriate technical and organisational measures are in place to protect personal data against accidental or unlawful destruction or loss or disclosure.

The European Commission is beginning to look at RFID as a separate issue. It has issued a consultation based on the conclusions it reached after an internal workshop on RFID tags in July 2003. It recommends action in three areas:

- ensuring worldwide interoperability of RFID tag systems and globally harmonised spectrum resources;
- catalysing the initial demand for RFID systems; and
- addressing the emerging concerns of privacy and user acceptance, including getting the RFID industry to formulate clear recommendations, codes of conduct and guidelines on

the appropriate use of these technologies.

In America, two states have introduced RFID Bills. In Utah, the House of Representatives has passed the first ever RFID privacy Bill. If approved by the Utah Senate, the Bill - Radio Frequency Identification Right to Know Act - will take effect on 5 May 2004. The Bill 'requires a product containing a radio frequency identification tag to contain a label describing the radio frequency tag' and to allow the tag to be disabled 'prior to the completion of sale unless the consumer chooses to leave it active'.

In California, Senator Debra Bowen has introduced a Bill (Senate Bill 1834) that would require a person or entity that uses RFID systems to comply with certain conditions. These include obtaining an individual's written consent before attaching or storing personally identifiable information with data collected via an RFID tag or before any personally identifiable information collected via an RFID system is shared with a third party. The Bill also states that if 'a retail store uses an RFID system on consumer product, the RFID tag shall be detached or destroyed before a consumer leaves the store'. The Bill would make a violation of its provisions an act of unfair competition that is subject to specified enforcement provisions, including actions brought by the Attorney-General or a district attorney or city attorney.

Links

Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data:

http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett

Commission consultation: http://www.cordis.lu/ist/directorate_d/ebusiness/workshop.htm

Utah Bill: <http://www.le.state.ut.us/~2004/bills/hbillamd/hb0251.pdf>

California Bill:

http://www.leginfo.ca.gov/pub/bill/sen/sb_1801-1850/sb_1834_bill_20040220_introduced.pdf

Conclusion

With new technology comes fear - this is an established fact. In most instances this fear turns out to be unfounded.

For those intent on turning us into an RFID world, the future looks bright. History has shown time and again that consumers can be bought off. If the technology will save them time or money, or both, they will usually readily surrender our privacy for it. Store cards, especially supermarket ones, are a classic example; where you can earn 'reward points' to get money off future goods, in return for letting the retailer keep track of what you buy, enabling it to build a profile of you from your purchases? It is, perhaps, important not be fooled into thinking that the problem just rests with advances in RFID technology but to look instead at the bigger picture. The picture that could be made from multiple sources of data already available. The CCTV camera following your every move through the city streets, the mobile location data given off by a mobile phone, the money trail left by store and credit card purchases, travel details pinpointed by travel smart card technologies, such as London's 'Oyster Card'. Add to that a national ID card and biometric passport, and we don't even need to cover RFID to get paranoid - if we so choose that is.

RFID, like many before it, is a great technological advance with a myriad of highly sought-after uses to make our lives easier. This is why the UK Government, the European Commission and the US Congress should step in now and ensure that consumers are notified about products with embedded RFID tags. Rules need to be adopted as to what can and cannot be tagged, currency being one such category.

If used sensibly, RFID could make the future brighter; so bright you'll have to wear shades ... tagged ones of course.

References

- 1 See http://www.verisign.com/corporate/news/2004/pr_20040113.html?sl=070802
- 2 See <http://www.computerworld.com/mobiletopics/mobile/story/0,10801,89036,00.html?from=imutopicheads>
- 3 Alan Stewart, 'Understanding supply chain execution - case studies - 1. Taking stock of radio tags - Marks & Spencer' *Financial Times*, 26 November 2003.
- 4 See <https://gvsregistry.4verichip.com/index.htm>
- 5 RFID position paper: <http://www.privacyrights.org/ar/RFIDposition.htm>
- 6 OECD's Privacy Guidelines: http://europa.eu.int/comm/internal_market/privacy/instruments/ocdeguideline_en.htm

Everybody's doing it

Wal-Mart isn't the only big player to think RFID is the way ahead - there are many more:

- The US Defence Department employed an item-specific tagging system on goods transported to Iraq as part of a Pentagon policy to use RFID to track supplies. The items were monitored by a DoD satellite network.
- Many airlines are testing RFID as a method for tagging traveller's luggage. RFID is seen as an ideal way of minimising baggage loss and ensuring that luggage reaches its designated destination.
- Several seaport operators have agreed to deploy RFID tags to track containers that arrive at US ports. Currently, less than 2% are inspected. RFID tags will be used to track the containers and the employees handling them.
- Marks & Spencer has conducted a month-long trial tagging a selection of men's clothing with RFID tags, in order to monitor the goods as they moved from the distribution centre to the store. This allowed the business to monitor size, colour and style of clothing to ensure that stock was always up to date. Marks & Spencer does not have any current intention of using tags at the point of sale.
- Woolworths piloted an RFID system in the UK to improve logistics and reduce shrinkage as part of the Home Office's 'Chipping of Goods' initiative. Unilever, Allied Domecq Spirits and Wines, and Safeway have also been running pilot logistics schemes under the initiative.
- Carrefour, Tesco and Metro Group (the world's fifth largest retailing firm) collectively formed EPC Product Retail Users Group of Europe. Metro has been working with IBM, Intel, SAP and Microsoft on its RFID project.
- Selfridges' London store is also working with Exel to integrate the RFID trial into the firm's PKMS warehouse management system from Manhattan Associates early next year.

- In Canada, RFID was used in a trial carried out by the Canadian Cattle Identification Agency. The goal was the implementation of the world's first fully functional 'stable to table' tracing system, which will dovetail with the barcode system used in food packaging systems around the world.
- Tyre manufacturer Michelin is experimenting with adding tags into its tyres. The tag will store a unique number for each tyre which will be associated with the car's VIN (vehicle identification number).
- Casinos such as the Star City Casino in Sydney, Australia placed RFID tags in 80,000 employee uniforms in order to put a stop to theft. Not content with tagging their staff, many casinos are now beginning to tag the chips themselves. This would allow them to check that big winners are not cheating the house, and also - by being able to see how many chips a player has - to encourage 'high rollers' to keep playing by treating them to free meals, drinks, and hotel rooms.
- Several countries are looking at utilising RFID in passports. The Thai Government is researching the possibility, Australia is planning trials during 2004, and the US is pushing ahead with the idea under the guise of protecting the nation's security.
- The European Central Bank is seriously examining the idea of embedding RFID in Euro notes. This would have the advantage of allowing banks to count large amounts of money in seconds, and would also help stem the tide of money laundering and counterfeiting.
- San Francisco's Public Library Commission will start using RFID to track books this year.

In countries such as Korea, China and Thailand, RFID is being used in contact-less smart cards for the purposes of travel, road tolls and national identification. In China, where ID cards are compulsory, the National Peoples Congress passed the National Citizens ID Law on 28 June 2003, which authorised the introduction of RFID-embedded ID cards to replace old-style plastic ones. The Chinese Government hopes to have the whole country converted to the new cards by 2010. The cards will include information such as name, age, gender, date of birth, address, national ID number, photo etc.

'Spy chips' discovered in German supermarket's loyalty cards

After a tour of the German Metro Group's 'Future Store' -- set up in 2003 to test experimental RFID technology on shoppers -- Katherine Albrecht, founder of CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering), was shocked to find 'spy chips' with unique ID numbers in the store's customer loyalty cards. 'The card application form, brochures, and signage at the store made no mention of the embedded technology and Metro executives spent several hours showing us the store without telling us about it,' she said.

Albrecht also discovered that the store did not -- indeed *could not* -- deactivate after purchase the unique ID number contained in RFID tags in the products it sold. The use of such unique item-level ID numbers is one of the key privacy concerns in relation to the use of RFID tags in consumer goods. According to Albrecht, 'Customers are misled into believing that the tags can be killed at a special deactivation kiosk, but the kiosk only rewrites a portion of the tag, while leaving the unique ID number intact.'

Further Information

See the website of German civil liberties group Foebud at: <http://www.foebud.org/rfid/>