ASPEN PUBLISHERS

The COMPUTER & INTERNET Lawyer

Volume 24 ▲ Number 2 ▲ FEBRUARY 2007

Arnold & Porter, Editor-in-Chief*

Is Big Business Watching You? RFID Tags, Data Protection, and the Retail Industry in the European Union

By Sarah Kirk, Jamie Fraser, and Jackie Vincenti

A transformational technology that has the potential to transform supply chain management, reduce errors, *and* cut fraud? It is no surprise that manufacturers, retailers, and other technology companies throughout the world are fascinated by the claims made by advocates of Radio Frequency Identification (RFID). Some consumer groups, however, feel that the introduction of RFID is a little too like "Big Business is Watching You."

At their most basic, RFID systems work by transmitting the identity of an object (in the form of a unique serial number) wirelessly. While there are many helpful and positive applications for this technology, there are potential privacy concerns relating to how businesses and governments use the technology, which may breach the principles of the European Union's (EU) Data Protection Act. The surreptitious collection of an individual's data; the ability to track customers as they walk in public places; the creation of profiles based on the monitoring of consumer behavior in shops; and the ability to read the details of clothes and accessories worn, as well as medicines carried—what retailers might see as an enhanced consumer experience can also be viewed as a violation of human dignity, as well as data protection rights.

The UK Information Commissioner's Office (ICO) has recently published guidance on RFID

Sarah Kirk is a UK solicitor and a Partner at Arnold & Porter (UK) LLP, in London. Her practice focuses on transactional intellectual property and information technology matters, including advising in the field of emerging technologies. Ms. Kirk also specializes in data protection and privacy and has advised many multinational companies on compliance issues. **Jamie Fraser** is a UK solicitor and an Associate at Arnold & Porter (UK) LLP, where he focuses on transactional intellectual property and information technology. Mr. Fraser also specializes in data protection, privacy, and issues relating to international transfers of data. **Jackie Vincenti** is a trainee solicitor in the London office of Arnold & Porter (UK) LLP. She has experience in both contentious and non-contentious intellectual property matters, as well as advising clients on data protection issues.

Wolters Kluwer
Law & Business

technology,[1] which addresses the many implications for RFID. On October 16, 2006, EU Information Society Commissioner Viviane Reding opened the EU RFID 2006 Conference entitled "Heading for the Future," which is part of a public consultation in advance of legislative proposals due by the end of the year.

This article focuses on the EU and uses of RFID in the retail sector and the need to process data in accordance with the rights of the data subject. The fact is that the concerns about RFID are similar to concerns that arose when Internet technology was gaining wider acceptance. Cookies downloaded from an Internet browser are able to identify an individual as having previously visited a Web site and can be used to build up a profile of users of the site, similar to the potential uses of RFID technology. This article will suggest that methods used to ensure compliance with data protection principles in relation to cookies can be used with RFID technology to remove many of the current consumer fears of consumers.

What Is RFID?

RFID tags are a way in which information can be transmitted and recorded using radio signals. The key parts of an RFID system are: (1) the tiny radio device, or tag, which consists of an electronic circuit that stores data, and an antennae to receive and transmit signals via radio waves; and (2) the reader that contains an antennae that is able to translate incoming analog information from the radio tag into digital data, which can then be processed by a computer system.

When a tag receives a signal from a reader, it will respond to the signal by transmitting its own unique number. In this way, the reader can identify the tag, relate it to the information within its database, and therefore identify the product. The operating range of RFID tags depends on the frequency used, varying from a few centimeters for low frequency tags to more than 100 meters for microwave tags.

RFID systems have been hailed as the next-generation barcodes, whose limitations in the face of this technology are now apparent: Barcode labels have a low storage capacity and simply transmit the type of product or series of items, whereas RFID has the ability to have a unique number for each individual product. In addition, whereas barcodes have a low read range and can be read only one at a time when line of sight is established, RFID tags can be read at a distance from the product and more than one can be read at a time. Finally, whereas barcodes are fixed and cannot be rewritten, the micro-chip technology in RFID can be reprogrammed as necessary, making them much more flexible.

Current Applications of RFID

EU Information Society Commissioner Viviane Reding said at the EU RFID Conference, "[i]t is estimated that by 2015 there will be 1 trillion sensors linking the physical and digital worlds. These two worlds will merge to become an 'Internet of Things.' The applications are numerous; the list is limited only by our imagination."

RFID are currently used in a wide range of applications to improve the tracing of goods and assets. Examples include pre-paid travel cards, such as London Underground's Oyster travel-card system; improving management of moveable assets for logistics providers, such as monitoring livestock or passengers' baggage at airports; anti-counterfeit initiatives, such as for drugs in the pharmaceutical industry; child safety devices; key-fobs; and secure access entry systems.

By far the most widely used current application, however, and the application that this article will concentrate on, is use by retail managers and wholesalers to monitor particular goods and aid supply chain management. This can assist with product recall procedures, as RFID can easily identify a single batch, and help to prevent shoplifting and fraud.

Data Protection Rights

The EU Data Protection Directive[2] (the Directive), which the UK implemented by the Data Protection Act[3] (DPA), regulates the *processing* of *personal data* by *data controllers* and also awards data subjects certain access rights in relation to any data that is being processed about them. "Processing" includes almost any act done in relation to the data. "Personal data" is very widely defined in the DPA and includes any information that relates to a living individual; and the information collected concerns an individual who is identified or identifiable. Data relates to an individual if it relates to the identity, characteristics, or behavior of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated. The information does not have to be specifically linked with an actual person if the individual can be distinguished from others around him.

The DPA sets out eight data protection principles that have to be adhered to when processing personal data. These state that:

1. Processing of personal data shall be lawful and fair in accordance with conditions identified in the DPA and Directive to legitimize data processing;[4]

2. Personal data shall only be obtained for specified and lawful purposes;

3. Personal data shall be adequate, relevant, and not excessive for the purposes for which they are collected;

4. Personal data shall be accurate and kept up to date;

5. Personal data shall be kept for no longer than necessary for the purposes for which the data were collected;

6. Personal data shall be processed in accordance with the rights of the data subjects; these rights include the right for a data subject to know what data is being collected and held, to be told how data is being processed, and who has access to the data;

7. Appropriate technical and organization measures shall be taken to prevent unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and

8. Personal data shall not be transferred outside the EU or European Economic Area without adequate protection being in place.

Perceived Problems with the System Regarding Data Protection

Does the Directive apply to the collection of data through RFID technology? Personal data rights may be breached when deployment of RFID technology is used to collect information that is directly or indirectly linked to personal data. Whether the Directive will apply to a particular application will depend on the specific application of the RFID technology in question.

There will be situations in which information within an RFID system neither contains personal data nor is combined with other identifying materials, such as the name and address of the individual. If this is the case, the provisions of the Directive and DPA will not apply. For example, in most current applications, such as when RFID technology is used in supply chain management to monitor individual products and is switched off (or killed) at the point of sale, there is unlikely to be any breach of an individual's data protection rights. The tags do not store or communicate personal data and are not linked to other personal information. There is, therefore, no problem with the application of the technology.

Although there are many applications of RFID that do not interfere with an individual's data protection right, however, critics of the system have identified a number of potential applications of the technology that *do*, or have the *potential* to, process personal data. This can occur when information that identifies an individual, such as closed circuit TV footage, credit card details, or supermarket loyalty card information, are linked to the RFID tag number of the individual product purchased. This personal data could then be collected and processed. For example, the store could follow an individual as he or she shopped because the individual item can be identified, or the data could be used for direct marketing purposes.

In addition, if the RFID tag is not killed at the point of sale, the individual item can be read on subsequent visits to the shop if the shopper returns with the item. This can be used to build a profile on the shopper to give valuable information on the amount of time spent in a given section of the supermarket, the number of visits during which no products are purchased, or which products are purchased in combination.

Another privacy concern arises when personal data is stored in RFID tags themselves. In addition, as RFID technology is small and can be contained on almost any type of product, a consumer may not know that an RFID tag is incorporated in the product that he or she has purchased or that information is potentially being collected. Of further concern is the fact that, because the presence of RFID tags can be detected by anyone with a standard reader, a third party could surreptitiously obtain the information contained on the tag.

At the EU RFID Conference, Viviane Reding, the EU Information Society Commissioner, said that "[t]he overriding message that comes out of the consultation is that citizens have concerns over privacy issues. The large majority are willing to be convinced that RFID can bring benefits, but they want to be reassured that it will not compromise their privacy."

Implication and Application of the Data Protection Principles

Of the principles mentioned, the most relevant in relation to RFID technology is that processing should be in accordance with the rights of the data subject (Principle 6). This factor also relates to the fact that any such processing must be lawful, fair, relevant, not excessive, and not retained for longer than necessary (Principles 1, 2, 3, and 5). There are also concerns that the security and privacy of the technology are safeguarded, however (Principle 7).

As there are so many factors to consider in relation to the technology, and so many Principles relevant in any discussion surrounding it, this article will concentrate on the rights of the data subject—Principle 6—and related issues.

Comparison with "Cookies"

RFID technology and its possible implications for data protection rights are not new problems for the retail

industry. Although barcodes identify the type of products that are bought, rather than an individual product, it is possible to link such a purchase with the personal information of the customer, if combined with the credit or store card details obtained at the point of purchase. This can be used to build a general profile about the shopper; this is no different from the possible use of RFID.

The additional application of RFID is the fact that the individual item can be identified, and therefore the individual item can be linked with the individual customer during shopping, or on subsequent occasions. As previously stated, if the RFID tag is killed at the point of sale and only generic information about customer movements are gathered, the application is no different from the use of barcodes. Problems arise, however, if the RFID tag is not killed when purchased. There is then the potential for the individual user to be identified after sale if, for example, the shopper returns to the shop with the item and the RFID tag is read. This means that the potential to be identified increases in both frequency and duration.

Although barcodes do not have the capability to identify an individual past the point of sale, there are other systems that most people are familiar with in their everyday lives that identify us on multiple occasions. Whenever someone visits a Web site, the pages seen, along with the cookie, are downloaded to that person's computer. A cookie is a small amount of text-data identifier, which enables Web site owners to find out whether the computer (and, by extension, its user) has visited the Web site before. This is done on a repeat visit by checking to see, and finding, the cookie left there on the last visit. This can identify an individual on multiple visits, similar to the potential uses of RFID.

How Do Cookies Work?

A Web site will transfer the cookie to a user's browser cookie, which is then stored on the user's computer hard drive. A cookie will typically contain the name of the domain from which the cookie has come, the lifetime of the cookie, and a value, usually a randomly generated unique number, similar to the unique number of the RFID.

Each Web site can send its own cookie to a user's browser if the browser allows it. Many Web sites do this whenever a user visits in order to track online traffic flows. In addition, cookies record information about a user's online preferences. Information supplied by cookies can help a Web site owner to provide the user with a better online user experience and assist them to analyze its visitors' profile. For example, if on a previous visit a user went to a particular page of the site, the owner might identify this from the cookies and highlight similar information on subsequent visits. These uses are similar to those proposed for RFID within the retail sector, such as profiling shopper's movements.

Cookies cannot be used by themselves to identify the user and are not necessarily linked to personal data. Cookies simply unlock a computer's memory and allow a Web site to recognize users when they return to a site; it is technically impossible for cookies to process personal information. Similarly, RFID has data protection implications only if the unique number is combined with other personal data collected at the point of sale; the technology itself cannot read or process personal information.

Both cookies and RFID have the ability to build profiles of customers and monitor use of Web sites or shops over multiple visits. Both systems can also be used to flag certain items that a customer may be interested in based on experiences of past visits. So, although the technology and hype surrounding RFID may be new, the actual implications and concerns for individuals in relation to data protection are the same as arose when cookies were beginning to be used on the Internet. Similarly, the same methods and policies will need to be put in place to comply with obligations that arise under the DPA and to calm consumers' fears.

Effect of Data Protection Implications: Privacy Policy

Under most scenarios in which RFID technology is used, consent from individuals will be the only legal ground available to data controllers to legitimize the collection of information through RFID. For example, a supermarket will need either explicit contractual regulations or the individual's consent to link any personal information obtained in the context of obtaining the loyalty card or using a credit card with information gathered through RFID technology. It is important that any use of RFID in the retail sector is done openly and that customers understand how their data is being used.

Web sites comply with data protection principles and obtain individual's consent by providing a "Privacy Policy" and a "Cookies Policy" on the site. These set out for the users what data are being collected, how that data are used, who has access to the data, and how the individual can access this data. They also inform users about how cookies are used and provide advice on how a consumer can refuse or block cookies.

Similarly, as RFID technology may also collect and process personal data, and in compliance with the obligation to provide information to shoppers, the data controller should produce a similar Privacy Policy or

RFID Policy. This will need to provide shoppers with a clear notice about:

- The presence of the RFID tags on products or packaging, the presence of readers, and whether the technology is killed at the point of sale;
- The consequences of such presence in terms of information gathering, in particular data controllers should be very clear in informing individuals that the presence of tags enables information to be read without the individuals engaging in any active action;
- What information is being collected and how such data can be linked to other personal data in order to identify the individual concerned;
- The purposes for which the information is intended to be used, including (1) the type of data with which RFID information will be associated, (2) whether the information will be made available to third parties, (3) how long the data is going to be retained, and (4) whether this data will be used for direct marketing purposes; and
- The identity of the data controller.

In addition, depending on the specific use of RFID, the data controller may also have to inform individuals about:

- How to discard, disable, or remove tags from the products, thus preventing the shopper from disclosing further information;
- How to opt out of any direct marketing; and
- How to exercise the right of access to information. This will entail disclosing all information linked to a person, which may include the number of times the person entered the shop and the items bought, for example. If RFID tags contain personal information, individuals should be entitled to know the information contained in the tag and to make corrections using easily accessible means.

Such polices will have to be clearly identified to shoppers in the same way such policies are set out for Web site users and will become as frequent as Privacy Policies on Web sites. Shoppers have the right to be told about such collection and use of any personal data; retailers and supply managers will have to be aware of the need to tell shoppers this information.

Transparency is the key: If today's consumers are to be convinced about the benefits of RFID technology, they must be fully informed and assured that their privacy is not being compromised. If this is provided, then the "Internet of Things" will be more likely to gain wider acceptance and live up to some of the current hype.

Notes

1. "Data Protection Technical Guidance—Radio Frequency Identification," V1.0 09.09.06, at *http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/radio_frequency_indentification_tech_guidance.pdf* and *http://www.ico.gov.uk/upload/documents/pressreleases/2006/rfid_advice_on_tagging.pdf*.
2. Directive 1995/46/EC.
3. Data Protection Act 1998, which came into force on March 1, 2000.
4. Article 7 of the Directive lists the following legal grounds to legitimize the data processing: (1) the data subject has unambiguously given his consent for the processing; (2) the processing is necessary for the performance of a contract to which the data subject is a party, (3) processing is necessary for compliance with a legal obligation to which the controller is subject (4) the processing is necessary in order to protect the vital interests of the data subject (5) the processing is necessary for the performance of a task carried out in the public interests (6) the processing is necessary for upholding the legitimate interests of the responsible party, except when the interest of fundamental rights and freedoms of the data subject, in particular the right to protection of individual privacy, prevail.

Reprinted from *The Computer & Internet Lawyer*, February 2007, Volume 24, Number 2, pages 1 to 5, with permission from Aspen Publishers, Inc., a Wolters Kluwers business, New York, NY, 1-800-638-8437, *www.aspenpublishers.com*.