ARTICLE 29 Data Protection Working Party

10107/05/EN
WP 105

Working document on data protection issues related to RFID technology

January 19, 2005

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate E (Services, Copyright, Industrial Property and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.

Website: www.europa.eu.int/comm/privacy

WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Article 29, Article 30(1)(c) and Article 30(3) of the above Directive,

having regard to its rules of procedure, and in particular Articles 12 and 14 thereof,

HAS ADOPTED THE PRESENT working document:

1. Introduction

The use of Radio Frequency Identification (commonly known as "RFID technology") for different purposes and applications may benefit business, individuals and public services (governments included). As further illustrated in this paper, RFID can help retailers manage their inventory, enhance consumers' shopping experience, improve drug safety as well as allow better control access by persons to restricted areas.

While the advantages related to the use of RFID technology seem obvious, the widespread deployment of the technology does not come without its potential drawbacks. On the data protection front, Working Party 29 ("Working Party 29") is concerned about the possibility for some applications of RFID technology to violate human dignity as well as data protection rights. In particular, concerns arise about the possibility of businesses and governments to use RFID technology to pry into the privacy sphere of individuals. The ability to surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; read the details of clothes and accessories worn and medicines carried by customers are all examples of uses of RFID technology that give rise to privacy concerns. The problem is aggravated by the fact that, due to its relative low cost, this technology will not only be available to major actors but also to smaller players and individual citizens.

The awareness of this new risk has compelled Working Party 29 to look into the privacy and other fundamental rights implications of RFID technology. To this end, among others, Working Party 29 has consulted with interested parties, including manufacturers and deployers of the technology as well as with privacy advocates. The outcome of the subsequent analysis carried out by Working Party 29 is the current working document which has the following two main purposes: firstly, it aims to provide guidance to RFID deployers on the application of the basic principles set out in EC

[1] Official Journal L 281, 23.11.1995, p. 31, available at: http://europa.eu.int/comm/internal_market/privacy/law_fr.htm

Directives, particularly the data protection Directive[2] and the Directive on privacy and electronic communications[3] and secondly, with this working document Working Party 29 wishes to provide guidance to manufacturers of the technology (RFID tags, readers and applications) as well as RFID standardization bodies on their responsibility towards designing privacy compliant technology in order to enable deployers of the technology to carry out their obligations under the data protection Directive.

Taking into account the relatively low level of experience of the use of RFID technology, Working Party 29 regards this paper as a first assessment of the situation. The Working Party will continue examining the situation, and as more experience is gained, it will provide further guidance. This will be particularly necessary if RFID technology becomes, as expected, one of the main “bricks” of the future ambient intelligence environment. In sum, this is an initial paper, and the Working Party 29 will continue working on this issue.

2. Radio Frequency Identification Technology: An Overview of the technology and its usages[4]

1. The basics of Radio Frequency Identification Technology

The main components of Radio Frequency identification technology *or* infrastructure are a *tag* (i.e. a microchip) and a *reader*. The tag consists of an electronic circuit that stores data and an antenna which communicates the data via radio waves. The reader possesses an antenna and a demodulator which translates the incoming analogue information from the radio link into digital data. The digital information can then be processed by a computer.

As further illustrated in the next section, RFID technology can work in different ways depending on the types of tags and readers. Those who will be deploying the technology will have to choose between the different technical possibilities according to their needs. Deployers will have to decide whether to use active or passive tags. “Passive” tags have no own power supply (battery) and can therefore be wakened decades after having been manufactured. The tag is powered by the radio signal. A RFID reader sends radio signals that wake up the tag within a range, triggering it to respond by transmitting the information that is stored on it. “Active” tags have their own battery which reduces their life cycle. They either broadcast their information without being interrogated by the reader, or stay quiet until triggered by a reader.

2 Multiple usages in many sectors- Examples

Directive 95/46/EC 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.

[3] Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[4] A more extensive description of RFID technology and the usages for which is suitable is attached as an annex at the end of this document.

The use of RFID technology is taking off in a variety of *sectors* (e.g., healthcare, aviation, transportation). Moreover, the specific *functions* that RFID tags can deliver in the different sectors is also increasing and its possibilities are just beginning to emerge. This section aims to illustrate the main functions that RFID technology can provide in different sectors or applications, i.e., transportation, healthcare. Whereas some of the RFID applications described below are still in a testing phase, others are a reality, sometimes without data subjects being aware of it.

Transportation/Distribution. RFID systems are well suited for some transportation applications. With an appropriate distribution of RFID readers, vehicles equipped with a tag can be tracked on the way to their destination. Many public transportation tickets are already based on RFID technology. According to industry sources, there are millions of car keys worldwide that incorporate RFID.

Aviation. RFID technology can be used for baggage handling purposes. At the checking point, baggage will be tagged and readers installed in different sections of the airports will track the baggage as it moves from one airport to another and within the airport itself. Projects exist to equip boarding cards with tags enabling the location of late passengers.

Healthcare. RFID systems are used in the pharmaceutical industry to make tracking of medicines easier and to prevent counterfeiting and loss derived from theft during transportation. This may be achieved by manufacturers inserting tags into each medicine thus authenticating its origin. Pharmacists or stores selling the medicines will be equipped with readers which will verify that the medicine originates from its purported manufacturer. The US Agency FDA has already issued guidelines for RFIDs on drugs packaging for tracking and against counterfeiting.[5] In hospitals too, by attaching tags to certain items, RFID improves patient safety and hospital savings for example where it eliminates the risk of leaving an item inside a patient at the conclusion of an operation. RFID labels can also be attached to the patients themselves to verify their identities, location and the exact procedure to be performed by the hospital staff. Hospital personnel can also be tracked so that they are easy to locate in case of an emergency. The FDA has just authorised a company application (VeriChip) based on the injection/setting under human being skin of a RFID tag giving the medical file index of a patient usable in emergency cases[6]

Security and Access Control. Movement and use of valuable equipment can be tracked with RFID systems as tags will broadcast information about their location to readers in the appropriate range. For example, in the automotive industry, RFID is already used as a component of a car immobilizer system. In the consumer and retailer

Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs; Guidance for FDA Staff and Industry; Compliance Policy Guide; Sec. 400.210; Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs; November 2004.

Department of Health and Human Services; Food and Drug Administration; 21 CFR Part 880; Docket No. 2004N–0477]; published in Federal Register / Vol. 69, No. 237 / Friday, December 10, 2004 / Rules and Regulations.

sector, special RFID tags can be used to ensure the origin of an item of merchandise. In this way, high value goods can be checked for forgery. Securing bank notes with RFID is a topic which has been researched over the last few years.

According to the work done within the ICAO[7], RFID will also be used in passports[8]. The access of persons to restricted areas can also be managed by attaching an RFID tag to them or equipping them with contact-less smart cards such as those for the World Summit on Information Society or for a congress of the Chinese communist party.

Retail Applications. Several major retailers have asked manufacturers to tag their products. The retailer can take advantage of using tagged products in several contexts. For example, RFID improves retailers' storage management functions. As each individual product is identified in various stages (i.e., upon arrival at the store, on the shelf, at the point of sale), RFID provides the retailer with a flexible tool to handle and monitor the availability of products in the store and in storage. RFID has the potential to improve in-store efficiency, benefiting retailers and potentially consumers as well. For example installing readers at the check out points enabling checkouts to be bypassed will reduce the time a consumer has to spend in a shop. RFID may help with product traceability, allowing more effective recalls of faulty or unsafe products or products for which the sell-by-date has been passed.

In the context of RFID in the retail sector, it's important to take into account the standardization work done by EPC Global towards creating a 'Electronic Product Codes' which will identify individual items[9].

3. Data Protection and Privacy implications

Whereas some applications of RFID may not pose any data protection concerns, as illustrated below, many do. This section aims to give an overview of the main data protection implications that derive from different usages of RFID technology.

3.1. RFID used to collect information linked to personal data

A first type of data protection concerns arises when the deployment of RFID technology is used to collect information that is directly or indirectly linked to personal data. First, one can consider the case where the RFID tag number of a product is linked to the record of the customer who bought it. For example, a consumer electronics store could tag its products with unique product codes which the retailer systematically combines with customer names collected upon payment with credit cards and later on linked with the retailer customer database. This could be done for, among others, guarantee purposes. As a second example, one can consider the case where supermarket tags loyalty cards or similar devices which identify individuals by their names to learn

[7] International Civil Aviation Organisation.

[8] In 2003, ICAO specified the technical requirements for RFID technology used in electronic passports. These specifications were published in ICAO Doc 9303.

[9] See section 5.2 for further information on EPC Global.

and record consumer habits while consumers are in the store, including the time spent on a given section of the supermarket, the number of times the consumer visits in the supermarket without buying, etc.

In the above cases, insofar as the information gathered through RFID technology is linked to personal data, the privacy implications are obvious. In addition to enhancing the existing ability of learning consumer habits and making individual profiles enabled by loyalty cards, RFID technology increases the potential for direct marketing with item-level tagging, as individuals could be recognised on entering a store and their habits in-store monitored. Furthermore, widespread deployment of the technology will cause a boost in data (both in type and in number) to be processed by a wide variety of controllers, giving cause to concern.

3.2. RFID used to store personal data on each tag

A second type of privacy implication arises where personal data is stored in RFID tags. One example of this use could be in transport ticketing. One should consider the hypothetical case where an organisation decides to implement a contactless ticketing system based on RFID technology for monthly passes where the name and contact details of the holder of the pass is inserted into the tag. This would have the effect of allowing the organisation to know where an identified individual travels at all times. This obviously impacts individuals privacy. In addition to the organisation having this information, because anyone can detect the presence of particular RFID tags with a standard reader, third parties could also surreptitiously obtain the same information. It should be noted that RFID systems are very susceptible to attacks. As they work non-line-of-sight and contactless, an attacker can work remotely and passive readings will not be noticed.

3.3. Use of RFID to track without “traditional” identifiers being available

A third type of data protection implication arises from uses of RFID technology which entail individual tracking and obtaining access to personal data. Several examples will illustrate how RFID technology may impact an individual’s privacy.

For example, there is the possibility for a chain grocery store to give out tagged devices to customers (e.g., like tokens) enabling the operation of shopping carts, which customers re-use each time they visit the store. Such a mechanism would permit the store to set up a file using the identification number stored in the tagged device enabling it to monitor which products an individual (identified by the token) purchases, how often such products are used and in which of the chain grocery stores the consumer buys them. The store could make inferred assumptions about an individual’s income, health, lifestyle, buying habits etc. This information could be used for various decision making, such as marketing, purposes or even for dynamic pricing. Since the device would identify the individual each time he/she entered the store, the consumer could be marketed to in the light of the recorded consumer habits. In addition to the store being able to collect the above information, a third party could potentially also obtain such information. In this way, various decisions could be made about that identified individual without his or her informed consent. As it happens, with the use of cookies in the on-line environment, even if the individual is not immediately and directly identified at the item information level, he can be identified at an associative level because of the possibility of identifying him without difficulty via the large mass of information surrounding him or stored about him. Furthermore, the data collected from him can influence the way in which that person is treated or evaluated. This RFID use also carries serious data protection implications.

A further example could be where the use of RFID tags can lead to the processing of personal data, even when RFID technology does not involve the use of other explicit identifiers. Take the hypothesis where person Z walks into Shop C with a bag of RFID-tagged products from Shops A & B. Shop C scans his bag and the products in it (more likely a jumble of numbers) are revealed. Shop C keeps a record of the numbers. When person Z returns to the shop the next day, he is rescanned. Product Y, that was scanned yesterday, is revealed today – the number is for the watch he always wears. Shop C sets up a file using the number of product Y as a 'key'. This allows them to track when Person Z enters their shop, using the RFID number of his watch as a reference number for him. This allows shop C to set up a profile of Person Z (whose name they don't know) and to track what he has in his shopping bag on subsequent visits to Shop C. By doing this, Store C is processing personal data and data protection law will apply.

Finally, take the example of the use of tags on certain objects which contain information that reveal the nature of the object. Belongings of a person are very personal and hold information whose knowledge by third parties would invade the privacy of the person who owns the object. The following examples illustrate this hypothesis. Consider the case where anyone in possession of a reader can detect banknotes, books, medicines or valuable objects of passers by. The knowledge of this information by third parties will invade the privacy of the person who owns the object The same concerns apply where terrorists were able to detect specific nationalities among crowds. An even more dramatic intrusion would occur when, as described above, the device itself contains important personal information as for example passport related information or information that was highly sensitive.

As illustrated in these examples, some of the main data protection and privacy concerns that arise from the use of RFID technology derive from the surreptitious, unwanted individual tracking performed by unauthorized access to the tag's disclosed information or memory content.

As further described in the next sections, it is important to provide guidelines as to the application of the basic principles set out in the EC Directives, particularly the data protection Directive to the above data processing operations.

4. Application of EU data protection legislation to information collected through RFID technology

4.1. Guidelines regarding the application of the data protection Directive to the gathering and further processing of data through RFID technology.

In terms of scope, the data protection Directive applies to the processing of all personal data. Under the Directive, 'personal data' is very broadly defined and includes '*any information relating to an identified or identifiable natural person'*. It may then be asked whether this means that the data protection Directive necessarily applies to the collection of data through RFID technology. The answer will depend in general on the specific concrete application of RFID technology, particularly on whether the specific RFID application entails the processing of personal data as defined by the general DP Directive.

In assessing whether the collection of personal data through a specific application of RFID is covered by the data protection Directive, we must determine (a) the extent to which the data processed *relates* to an individual and, (b) whether such data concerns an individual who is *identifiable* or identified. Data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated. In assessing whether information concerns an identifiable person, one must apply Recital 26 of the data protection Directive which establishes that "*account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person"*.

In light of the above, while it is obvious that not all data collection by RFID technology will fall within the scope of the data protection Directive, it is also evident that there will be many scenarios where personal information is collected through RFID technology, the processing of which is covered by the data protection Directive.

Those who are considering using information gathered through RFID technology before doing so will have to carry out prior assessment to determine whether such information is deemed "personal data" in accordance with the data protection Directive. If RFID information neither contains personal information nor is combined with personal data as defined above, then the provision of the data protection Directive would not apply. Indeed, if tag information is not combined with other identifying material, for example someone's photograph or name and address, or with a recurring reference number, then the data protection Directive will not apply.

In the three scenarios described under section 3, the provisions of the data protection Directive would apply. In the first case, this is because the item level information gathered through RFID technology is directly linked to personal data contained in either a credit card or loyalty cards. In the second scenario, the application of the data protection Directive kicks in as soon as personal information such as a name is embedded in the RFID tags. Finally, the use of RFID technology to track individual movements which, given the massive data aggregation and computer memory and processing capacity, are if not identified, identifiable, also triggers the application of the data protection Directive.

4.2 Guidelines on the compliance of the data protection requirements

The data controllers for data gathered through RFID technology will be under an obligation to comply with the obligations of the data protection Directive (throughout this paper this is often referred to as "deployers of the technology"). While it is not feasible to establish how such requirements apply in each RFID scenario, it may be possible to give some general guidelines which data controllers can use and adapt in the light of the circumstances surrounding the data processing. As further described under section 5 below, manufacturers have a direct responsibility in ensuring that privacy compliant technology exists to help data controllers to carry out their obligations under the data protection Directive and to facilitate the exercise of an individual's rights.

Principles:

The Working Party would like to stress that the framework applying to the use of RFID technology, as well as of any other technology, is set out in Recital 2 of the data protection Directive which says that "*data processing systems are designed to serve man; (…) they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, in particular the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals*".

Principles related to data quality: Data controllers collecting data in the context of RFID applications must comply with several **data protection principles**, including the following:

Use limitation principle (purpose principle): This principle partially embodied in article 6(1)(b) of the data protection Directive, among others, prohibits a further processing which is incompatible with the purpose(s) of the collection.

The data quality principle: This principle in the Directive requires personal data to be relevant and not excessive for the purposes for which they are collected. Thus, any irrelevant data must not be collected and if it has been collected it must be discarded (Article 6.1. c)). It also requires data to be accurate and kept up-to date.

The conservation principle: This principle requires personal data to be kept for no longer than is necessary for the purpose for which the data were collected or further processed.

Legal grounds for processing: Pursuant to Article 7 of the data protection Directive personal data may be processed only if such processing can be based on one of the grounds for legitimize data processing[10].

[10] Article 7 lists the following legal grounds to legitimise the data processing: (i) the data subject has unambiguously give n his consent for the processing; (ii) the processing is necessary for the performance of a contract to which the data subject is a party, (iii) processing is necessary for compliance with a legal

Under most of the scenarios where RFID technology is used, consent from individuals will be the only legal ground available to data controllers to legitimise the collection of information through RFID. For example, a supermarket that tags loyalty cards will need either explicit contractual regulations or the individual's consent to link the personal information obtained in the context of obtaining the loyalty card with information gathered through RFID technology. However, consent is not always the appropriate legal ground to legitimise the processing of personal data collected in the context of RFID systems. For example, a hospital that uses RFID in surgical instruments to eliminate the risk of leaving an item inside of a patient at the conclusion of an operation may not need the patient's consent insofar as this processing might be legitimised in the vital interests of the data subject, which is another legal ground foreseen by Article 7 of the data protection Directive[11].

If consent is used, pursuant to Article 2 and 7(a) of the Directive it must comply with certain requirements. (i) It must be freely given, i.e., it must be given free of "deceit or coercion." (ii) It must be specific, in other words, it must relate to a particular purpose. (iii) consent must be an indication of the individual's effective will. (iv) consent must be informed. Finally, consent must be "*unambiguous*" meaning that consent that is capable of having more than one meaning would not be deemed consent.

Information requirements: Pursuant to Article 10 of the data protection Directive data controllers processing information through RFID technology must provide the following information to data subjects: identity of the controller, the purposes of the processing as well as, among others, information on the recipients of the data and the existence of a right of access[12]. In compliance with this obligation in the context of the scenario described under 4, the retailer store will have to provide data subjects at least with clear notice about the following:

(i) the presence of RFID tags on products or their packaging and the presence of readers;

(ii) 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 such devices enables the tags to broadcast information without individual engaging in any active action;

obligation to which the controller is subject (iv) the processing is necessary in order to protect the vital interests of the data subject (v) the processing is necessary for the performance of a task carried out in the public interests (vi) the processing is necessary for upholding the legitimate interests of the responsible party, except where the interest of fundamental rights and freedoms of the data subject, in particular the right to protection of individual privacy prevail.

[11] The Working Party 29 notes that ultimately the appropriate legal ground foreseen by Article 7 of the data protection Directive to legitimise a given data processing will depend on the specific circumstances of such processing.

[12] Information on the recipients of the data, the response obligation and the existence of access and rectification rights must be provided insofar necessary having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

(iii) the purposes for which the information is intended to be used, including (a) the type of data with which RFID information will be associated and (b) whether the information will be made available to third parties and,

(iv) the identity of the controller.

In addition, depending on the specific use of RFID, the data controller will also have to inform individuals about: (v) how to discard, disable or remove tags from the products, thus preventing them from disclosing further information and (vi) how to exercise the right of access to information. For example, this information will be necessary in the scenarios described under section 3.1. Whereas notices such as that proposed for EPC Global to be given in consumer products serves for the purpose of providing the information described above under (i), this should be complemented with further documentation adding the information listed above[13].

The principle of fair processing recognised in Article 6 (a) of the data protection Directive requires the information to be provided to data subject in a clear and comprehensible manner.

Finally, in providing the above information, the Working Party considers it important to highlight that the data subject should be in a condition to understand easily the effects of the RFID application.

Data subject's right of access: Article 12 of the data protection Directive gives data subjects the possibility of checking the accuracy of the data and ensuring the data are kept up to date. These rights fully apply to the collection of personal data through RFID technology. If we go back to the example of the supermarket which tags loyalty cards, providing for the right of access will entail disclosing *all* the information linked to a person, which may include the number of times the person entered the shop, the items bought, etc.

If RFID tags contain personal information as described under 3.2, individuals should be entitled to know the information contained in the tag and to make corrections using means easily accessible.

Security related obligations: Article 17 of the data protection Directive imposes an obligation upon data controllers to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or unauthorised disclosure. The measures can be organisational or technical. This requirement is developed under section 5 entitled RFID and the necessary use of privacy enhancing technology**.**

5. Technical and organizational requirements to ensure the adequate implementation of data protection principles

[13] See section 5.1 for an overview of EPC Global activities.

Compliance with the principles outlined above, as well as with the principle of data minimisation embodied Article 6.1 of the data protection Directive is essential for those who deploy RFID applications.

Working Party 29 considers that technology may play a key role in ensuring compliance with the data protection principles in the context of processing personal data collected through RFID technology. For example, the design of RFID tags, RFID readers as well as RFID applications driven by standardization initiatives may have a great impact in minimising the collection and use of personal data and also in preventing any unlawful forms of processing by making it technically impossible for unauthorised persons to access personal data.

In this context, Working Party 29 wishes to emphasize that while the deployers of an RFID application are ultimately responsible for the personal data gathered through the application in question, manufacturers of RFID technology and standardization bodies are responsible for ensuring that data protection/privacy compliant RFID technology is available for those who deploy the technology. Mechanisms should be developed in order to ensure that such standards are widely followed in practical applications. In particular RFID privacy compliant standards must be available to ensure that data controllers processing personal data through RFID technology have the necessary tools to implement the requirements contained in the data protection Directive. The Working Party therefore urges manufacturers of RFID tags, readers and RFID applications as well as standardization bodies to take the following recommendations into account.

5.1 Standardization and interoperability impacts on the implementation of data protection principles.

Whatever technology is under consideration, the process of standardization usually constitutes the main driver for interoperability which is important for successful adoption and implementation of new technologies. Standardization can also facilitate the adoption of data protection and privacy requirements.

All the components of an RFID system are or will be subjected to a standard, such as the design of the tag and the reader, the data stored in the tag, the communications protocol (air interface) between the reader and the tag, the management of the data collected by the reader, etc. Standardization bodies and other groups have already undertaken some work in the RFID domain. It should be noted that RFID standardization will have an influence on a considerable number of markets which will affect in particular transactions involving goods.

Originally introduced in response to the mad cow crisis, the International Organization of Standardization (ISO) has developed sector specific standards (Freight containers, Transport units, animals, etc..) for RFID tags and more generic ones for the air interface (ISO 18000 series) and for item management (ISO/IEC 15963:2004).

EPCglobal Inc[14], a joint venture between EAN International and the Uniform Code Council (UCC), is governed by the EPCglobal Board of Governors which is composed of leading companies. The organization is working on the creation of 'Electronic Product Codes' ("EPC") which will identify individual items. Each product will be equipped with a tag featuring the number of the product to which it is attached. The predecessor of such a system is the 'Universal Product Code' ("UPC") or bar code system, which EPC aims to replace. The difference between the two systems is that UPC identifies a product type without each of the individual items being numbered. In addition, the EPC Global Network is creating standards to connect servers containing information related to items identified by EPC numbers. The servers, called EPC Information Services or EPCIS are accessible via the Internet and linked, authorized and accessible via a set of network services[15].

In most of the RFID standardization initiatives, it may be possible to include data protection features into technical specifications. For example, recently it was proposed[16] to modify the standard of the reader-to-tag protocol developed by ISO in order to include the Fair Information Practices developed by the OECD[17].

Recently the European Telecommunications Standards Institute (ETSI) approved a new European standard for the use of RFID systems by increasing the allowed power of the reader and the numbers of available frequencies in the UHF band, the most promising one in the retail sector for item level identification. This evolution will increase in particular the read range from the reader to the tag[18].

The interoperability of RFID systems (hardware, software and produced data) logically results from the process of standardization. From a business perspective interoperability of RFID systems is positive. Indeed, for a sustainable business model, a retailer should avoid having to implement several different tag readers in order to scan tags produced by various manufacturers. From a data protection perspective, whereas interoperability may increase the technical quality of the data and contribute to compliance with Article 6(1) (d) of the Directive, RFID interoperability may at the same time have some negative side effects for data protection unless appropriate measures are taken. For example, the principle of purpose limitation may be more difficult to apply and to control. Moreover, the management of access rights regarding privacy might also become more critical as the number of actors manipulating the data will increase.

[14] http://www.epcglobalinc.org/

[15] Until now EU concerns have been under-represented in these standardization initiatives which are mainly populated by US industry stakeholders. It is also still not sure that Chinese market will adopt one of the cited standards and will not develop its own standards.

[16] Christian Floerkemeier, Roland Schneider, Marc Langheinrich: Scanning with a Purpose - Supporting the Fair Information Principles in RFID protocols. 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), November 8-9, 2004, Tokyo, Japan.

[17] ISO 18000 Part 6 Type A

[18] The distance of the reader and its power may affect the extent to which a given RFID application is particularly privacy invasive.

5.2 Technical and organizational measures for RFID presence information, visibility and activability state

As pointed out in paragraph 4, deployers of RFID technology are required to provide data subjects with information not only on the purposes of the processing of data, but *also* on the presence of RFID devices as well as to comply with the following:

Firstly, individuals must be informed of the presence of RFID-like or activated RFID readers. In order to do so, pictograms in the direction of a world wide standard as well as other informational means towards that goal are an obvious need. The provision of this type of information is essential in order to prevent the unauthorised and surreptitious gathering of personal data through RFID technology. For example, if a store or hospital has activated readers, individuals should be informed about it.

Secondly, for the same reasons outlined above (avoid the surreptitious gathering of personal data) the identification of the *existence of RFIDs* surrounding an individual (in clothing and objects for example) is another requirement because of the RFID's size which can make it almost invisible. Methods to carry out this requirement can adopt different forms: they can be given by standard notices but also technically.

Thirdly, informing about the presence of RFID only will not suffice in practice, the activability or the *real time activation* of RFIDs is also a piece of information to be provided to individuals that derive from the data protection Directive. So, simple techniques enabling visual indications of activation or activability states are also necessary. The presence and nature of PET technology (e.g. temporal disabler, tag physical remover feature etc.) as well as organisational measures in a given environment should be part of the information easily available.

Working Party 29 stresses that there is a continuing need for further R&D on these three informational topics by all parties.

5.3 Technical and organizational measures for exercising access, rectification and deletion rights

As further described below, the way RFID technology is built may have a great impact in ensuring the effective implementation of the access, rectification and deletion rights as recognised by Article 12 of the data protection Directive.

a) Tag content access (Art. 12 a data protection Directive)

Inherently to the technology, RFID tag content access requires a reader working with the tag protocol and a display towards the individual. But for many applications, the tag contains only an Id whose semantics can only be accessed through a complete IT application environment. In our knowledge, only a small number of RFID tags bear semantic information (describing the object, the data controller identificator, the data collection finality etc.) which, too, poses the problem of the content access by individuals.

One possibility to make this information valuable is to define semantic standards using for example XML. Whatever the form they take, those semantic descriptions still pose the problem of the access by unauthorized third parties (see section 3 above).

b) Content rectification (Article 12 b data protection Directive)

Unlike content access, rectification requires a reader working with the tag protocol and an interactive IT system allowing the individual to monitor both content reading and content modification.

A particular possibility proposed is to embed a feature into the tag that will erase or scramble the item serial number and let only the item class type description completely or partially available (the contrary is also possible but with different privacy implications).

c) Content deletion (Article 12 b data protection Directive)

Whether or not tag disablers should be implemented in order to allow individuals to stop the processing of their personal data when the tag enters into the range of a reader depends on the legal grounds that legitimize the processing of personal data. For example, such implementation would not be reasonable as far as RFID tags embedded in passports is concerned whereas it would - from a data protection point of view - be necessary in RFID tags attached to consumer products. This issue was considered in the context of the Sydney conference of data protection and privacy commissioners as reflected in the Sydney declaration on RFID[19].

Various proposed solutions were published in the last few years. One approach was the introduction of a "kill" command. This means, the tag can be permanently or temporarily deactivated by sending a "kill" command. Permanent deactivation can be done by fuse effect, memory scrambling or removing the tag. Temporary deactivation could be done mechanically or by applying a software lock. A problem with this approach is that the advantage of re-using the RFID capability outside the shop is lost. So, other approaches have been proposed.

A variant of the above consists in overwriting the data stored on an RFID tag with zeros. The tag still remains active, but returns only zeros instead of a number when queried. This system this does not really "disable" RFID. The tag still responds and passes on the information that the person carries a tagged item which can have the following consequences: First, As long as RFID tags that return only zeros are not very common, the mere existence of such a tag is valuable information. It shows that the

[19] Resolution on Radio-Frequency Identification, 25th Conference of Data Protection & Privacy Commissioners, Sidney 2003, http://www.privacyconference2003.org says as follows: "...whenever RFID tags are in the possession of individuals, they should have the possibility to delete data and to disable or destroy the tags".

person has bought something from a store that tags items. A well-informed company can make an educated guess. Secondly, it appears that at first, RFID tags are going to be used on valuable items. For a few years, the mere presence of an RFID tag (even if it returns zeros or unintelligible data) will help thieves looking for items worth stealing in cloakrooms or parking garages. Finally, as RFID tags become more numerous, shops may dislike all those tags that respond to queries, but return junk data.

Another approach is physical shielding of the tag, which can be wilfully used by the user. For example, purses with shields can be used, so that tagged banknotes cannot be detected. Also aluminium sheet incorporated into the RFID passport cover could suffice for its content protection excepted when the passport is open. However, shielding is not well suited for all applications. For instance, clothes with mounted tags cannot be wrapped with shielding material while being worn. Furthermore, this approach seems to impose unduly burdens upon individuals who are ultimately and uniquely responsible for preventing the tag from disclosing information.

In defining how tag disablers should work, in addition to the above, standardization bodies, manufacturers and deployers of RFID technology should take into account that individuals selecting the removal of the tag should not be penalised in any way.

Also there, Working Party 29 stresses that is a continuing need for further R&D on these topics by all parties.

5.4. Legal grounds for processing

Tags disablers: Further to the need of tag disablers in the context of section 5.3, other provision of the data protection Directive require the presence of this function (disabling a tag). Indeed, when under the data protection Directive consent is the only legal ground to legitimise the collection of personal data through RFID technology (see section 4.2), individuals can always withdraw their consent to the processing of personal data (ex Article 7 a). If no device enabling the individual to disable the tag is available, an individual who does not wish the tag to continue providing information on him/her will be prevented from exercising this right. When personal data embedded on RFID tags has been provided collected on legal grounds other than consent, it is not always necessary for such tags to have disabler devices. For example, personal information contained in tags used in the work context for the purposes of monitoring access to work may not require having available tags disablers insofar as the data processing is based on the employment relationship.

In some RFID applications, for example when the individual has a right to withdraw his/her consent or to object to the processing (ex Article 14 a) and the subsequent right to disable the tag, both manufacturers and deployers of RFID technology should ensure that such operation of disabling the tag is easy to carry out. In other words, for the data subject the task of disabling the tag should be easy.

5.5 Data security

Use of encryption on tags and applications: When RFID tags contain personal data, pursuant to Article 17 of the data protection Directive, they must have embedded technical measures to prevent unauthorised disclosure of the data. Unless such measures are implemented, anyone with a reader could "wake up" a tag and obtain the information stored on it. Such measures are also necessary ex Art. 6.1.d of the data protection Directive to ensure the integrity of the data stored in the tag, thus avoiding unauthorised changes.

The type of technical means will depend on the nature of the data. As further illustrated below, most of the time, these tags could require the *encryption* of the data and the authentication of the reader to prevent third parties provided with readers from reading the information. If we consider the scenario where RFID labels containing the patient identity, responsible doctor and procedure to be performed by the hospital staff, it is easy to understand the hospital obligation to ensure that such information is not readable by third party readers which brings the subsequent need to use technical measures such as encryption to prevent it.

The most general and secure approach is the use of standard authentication protocols (e.g. ISO/IEC 9798). They are already widely used in networks or with smart cards. In these standardised protocols, cryptographic primitives are used. For symmetric authentication methods, which means that the keys for sender and receiver are equal, MACs (message authentication codes) or symmetric encryption algorithms (e.g. DES, AES) are used. For asymmetric methods, where each party has a private and a public key, asymmetric encryption algorithms (e.g. RSA, ECC) or signature schemes are employed.

Some cryptographic authentication methods are already implemented in car immobilizers or access control systems, but they often use proprietary algorithms, because they are often easier and less expensive to implement than standard algorithms. Nevertheless for enhanced security which may be needed to protect sensitive data, standard algorithms and protocols should be implemented. The advantage of such protocols and algorithms is that they are already widely used and therefore tested and challenged by many different parties. In that way, they are now broadly accepted as being secure.

There already exist publications that indicate that symmetric algorithms (such as AES) are suitable for RFID tags[20]. The problem of using symmetric authentication algorithms is that the key establishment and the key management is complex. Asymmetric methods avoid this problem, but are more expensive than symmetric ones.

[20] Feldhofer M., Dominikus S., Wolkerstorfer J., "Strong Authentication for RFID Systems using the AES Algorithm", In the Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004, August 11-13, 2004, Boston, USA), Lecture Notes in Computer Science (LNCS) Vol. 3156, Springer Verlag, 2004, ISBN 3-540-22666-4, pp. 357-370. http://www.iaik.tugraz.ac.at/research/publications/2004/CHES2004_AES.htm

6. Conclusion

Given the increasing use of RFID technology for a variety of purposes and applications, some of which with huge data protection implications, the Working Party felt that it was necessary at this stage to publish this Working document and contribute to the on-going discussion on RFID issues. The Working Party hopes that the content of this paper presents a useful contribution to the debate on RFID and invites stakeholders to adhere to the principles mentioned in this paper.

This Working document has been prepared on the basis of available information, considering the status of development of the technology and particularly its current application in a variety of sectors. However, the Working Party is aware that the use of RFID is in continuous evolution: developments in this field occur constantly and as more experience is gained, the greater is the knowledge of the issues at stake. For this reason, the Working Party is committed to continue monitoring the technological developments in this field in collaboration with interested parties. Several questions identified in this Working document may need to be revisited in light of the experience gained. Furthermore, depending on the evolution of RFID technology and its applications, at a later stage the Working Party may decide to focus in detail on specific areas/applications by providing additional guidance for specific applications.

ANNEX

RFID TECHNOLOGY

Wireless communication is an emerging technology and covers nowadays a wide range of applications. Among them are the setup of wireless local networks (WLAN) or low bandwidth wireless connections among various devices like laptop, PDA, mobile phone and so on (Bluetooth).

During the last few years a new technology has become more and more popular. It is called RFID, which stands for Radio Frequency Identification. The main idea behind this technology was to give every object carrying an RFID tag a unique identity which can be communicated to a reader over radio frequency. This allows various applications in the supply chain and other industrial applications. In the beginning, RFID tags were intended to be used as a replacement of barcodes. The advantages of their usage were evident: They do not require line-of-sight and therefore the registration process can be done automatically. Nowadays, as the technology advances, other more sophisticated applications can be thought of. Before discussing possible applications, an overview of the technology is given.

The simplest RFID system consists of two components: a tag, which is attached to an object, and a reader which is able to retrieve the data from the tag. These components communicate with each other via a radio link. Both tag and reader possess an antenna and a demodulator (analogue front-end). This front-end "translates" the incoming analogue information from the radio link into digital data. These data can be further processed by the digital part of the reader or the tag.

On the tag's side, digital processing can be done either by custom-designed hardware or by a microprocessor. To process the data retrieved from the tags, a host computer attached to the reader can be used. This host is required to implement special applications using the tag data. Figure shows a current RFID system.

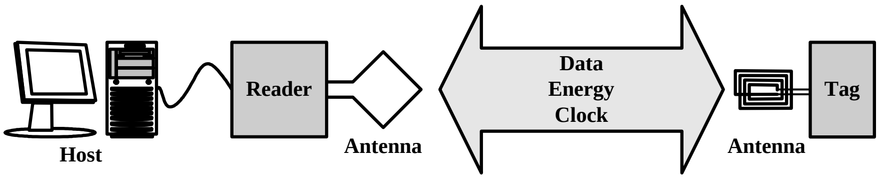

Figure: Structure of an RFID System

Various technology parameters can be used to describe a particular RFID system. Depending on these parameters, different applications are possible for RFID systems.

- *Active/Passive RFID Tags*. Basic tags working passively receive the energy and the clock signal to process and transmit data via the electromagnetic field of the reader. The intensity of this field is limited by national and international regulations. Thus, the power consumption of the tag has to be limited in order to ensure a correct functionality. The field strength diminishes with the distance to the reader, therefore smaller power consumption of the tag leads to longer reader ranges, i.e. reader and tag are capable to communicate over a longer distance. : Active tags transmit data even if there is no reader present or detected. Therefore they are equipped with a battery. To be complete in the description, some tags may incorporate a tester or a measure device recording values, such as a thermometer in order to detect ruptures in the cold chain, in that very case a battery is also needed but without direct consequence on the active/passive nature of the tag.

- *Operating Frequencies:* RFID systems can operate with different frequencies, ranges, and types of coupling. These parameters often depend strongly on each other. Frequencies vary from 135 kHz to 5.8 GHz. Here, international restrictions and physical requirements must be considered. Coupling can be electric, magnetic, or electromagnetic. The type of coupling affects the operating range, which can vary from a few millimetres to 15 m and more. More specifically, a distinction can be drawn between:

✓ Close-coupling systems, using tags with a short range of up to one centimetre. They work with frequencies between DC and 30 MHz and must be placed in or on the reader to communicate. In such systems, high energy consumption and high data transmission rates are possible.

✓ Remote-coupling systems with a range of about one meter. Most RFID systems use remote-coupling with frequencies between 135 kHz and 13.56 MHz.

✓ Long-range systems, with a range above one meter. They operate at frequencies between 868 MHz and 5.8 GHz.

RFID systems can interfere with other radio installations. Therefore it is important that they use other frequencies than audio-radio, television, or mobile radio services. The most important frequencies used for RFID systems are 0 to 135 kHz and the Industrial-Scientific-Medical (ISM) frequencies of 6.78 MHz, 13.56 MHz, 27.125 MHz, 40.68 MHz, 869.0 MHz, 2.45 GHz, 5.8 GHz, and 24.125 GHz.

- *Read/Write Capability:* The complexity of RFID systems varies. It is often limited by the capability of the tag.

✓ In low-end systems, tags are read-only. The reader can only read content from the tag, which is in general a serial number with a few bytes. Such simple tags are often used because of their low price and small chip area. They can be used to replace barcode systems where objects have to be identified, typically for storage management or routing of goods through the production process. Also animal tracking can be implemented with such kind of tags.

✓ In the middle field of RFID systems, tags may contain writable memory. Memory capacity currently varies between a few bytes up to several tens or hundreds kByte EEPROM[21] for passive tags and SRAM[22] for active ones. In this range, also sensors (temperature, pressure...) can be integrated into tags, for example to detect environmental accidents, which can be logged on the tag. Such tags can be further used for access control. Another application which has already been implemented and tested is luggage tracking at airports. The destination for the luggage can be written on the tag's memory and routing can be done automatically. Another application is in

[21] Electrically Erasable Programmable Read Only Memory

[22] Static Random Access Memory

healthcare. Such tags could be used in hospitals, to record the patients' treatment details or to monitor several parameter of a patient's condition.

- ✓ Contactless smart-cards with a microprocessor and an operating system are so-called high-end systems. They also contain a certain amount of memory, which is in general higher than for middle-field RFID tags. Complex functions can be implemented on the card. Programs can be stored in the tag's memory and then executed by the microprocessor. Due to the high power consumption of such cards, the operating range of such systems is nowadays limited to a few centimetres. More complex applications can be implemented with such cards. They are used for typical smart card applications like access control. They can also be used as identity or health insurance card. Travel documents with ICC[23] such as defined by ICAO or visa and residence permits with ICC are examples where such high-end RFID systems are under discussion.

Done in Brussels, on 19 January 2005
For the Working Party
The Chairman
Peter SCHAAR

[23] Integrated Circuit Chip