Regulation models addressing data protection issues in the EU concerning RFID technology

Paper presented at the 4th Conference on Information Law and Ethics, Thessaloniki, May 20-21, 2011

Ioannis Iglezakis
Assistant Professor
Faculty of Law, Aristotle University of Thessaloniki

Abstract

Radio frequency identification (RFID) is a new technology that will boost productivity and lead to a change of paradigm, as we move into ubiquitous computing and the introduction of the so-called "Internet of things". This technology also has significant privacy implications, since processing of personal data with RFID technology takes place unnoticed and it enables identification and profiling of a person; thus, it may lead to covert monitoring of individuals, which will infringe their privacy. Issues of data protection and security with regard to RFID are addressed by various recommendations and guidelines. The provisions of Directive 2002/58 as amended by Directive 2009/136 also apply in certain cases; however, there are still issues to be tackled, and new regulatory approaches are required.

Keywords: radio frequency identification, privacy, data protection, impact assessment, privacy by design

1 Introduction

Radio frequency identification (RFID) is a new technology that is destined to change our lives in many areas, such as logistics, healthcare, public transport, the retail trade, etc., as it provides new business opportunities, cost reduction and increased efficiency (Commission, 2009). RFID uses radio waves for the automatic identification of individual items and thus, it allows the processing of data over short distances (Bannon, 2008). In more particular, RFID systems are considered as the next generation of bar codes, offering much more advantages, since they identify uniquely objects which bear a RFID tag, without line-of-sight contact, and allow for wireless transmission of data and connecting to databases and applications (A. Juels, 2006).

The main components of an RFID infrastructure are a tag and a reader. The tag on the one hand consists of an electronic circuit that stores data and an antenna which transmits the data, while the reader on the other hand has an

antenna which receives the data and a demodulator which translates the analogue information into digital data (Article 29 Working Party, 2005, p. 3). The RFID reader sends and receives back signals from the tags via one or more antennas and transmits the data to databases or software applications.

An RFID tag can be easily embedded onto various products, their packages or even be implanted beneath the skin of a human (Talidou, 2006). The size of the RFID tag, which is particularly small, about 0,4 mm^2, is an important factor for its proliferation.

A common taxonomy of RFID systems makes a distinction between passive tags, i.e. those tags that have no own power supply and receive energy from the reader antenna, and active tags, i.e. those tags that have their own power supply. Passive RFIDs are very small and inexpensive and their life span is almost unlimited and this makes them ideal for tracking materials through supply chains (R. Levary et al., 2005). Active tags are more powerful, as they can emit the stored data, rewrite those data and store new data. However, their life cycle is shorter. Since they present more possibilities of data processing they are considered more privacy intrusive (Synodinou, 2009).

The applications of RFID technology are extended in many sectors. The retail sector was one of the first to adopt this technology, which provides the retailer the possibility to control and lever the availability of products in a store and in storage. It also makes possible product traceability and recall of faulty or unsafe products, etc. It makes, therefore, no surprise that an unprecedented growth in sales of passive EPC RFID tags took place in 2010 and that the sales volume exceeded one billion units[1], while prices of tags also are decreasing.[2]

In transportation and logistics, the said systems are implemented in order to track vehicles and products, providing security during transport. Particularly, high is the importance of this technology with regard to public transportation and as far as electronic toll collection and access to public transportation (e.g., e-ticket) are concerned (Talidou, op.cit.).

Furthermore, of great importance is RFID technology in healthcare, where it is implemented to make tracking of medicines easier and prevent counterfeiting and loss derived from theft during transportation. It would also enable pharmacists or stores selling medicines to verify the origin of medicine. In hospitals such systems may be used, e.g., to eliminate the risk of leaving items inside a patient after an operation and to locate track personnel in case of emergency, while RFID tags may be attached to patients so that it would be easier for the personnel to treat them (WP, op. cit., p. 4).

[1] See RFID Journal, Sales of EPC RFID Tags, ICs Reach Record Levels, available at: http://www.rfidjournal.com/article/view/7952

[2] Notably, the price of a 96-bit EPC inlay costs from $0.07 to $0.15, whereas if the tag is embedded in a thermal transfer label on which companies can print a bar code, the price is $0.15 and more, and low- and high-frequency tags tend to cost more. RFID readers, on the other hand, cost from $500 to $2,000; see RFID Journal, FAQS, available at: http://www.rfidjournal.com/faq/20

Other applications of RFID are implemented for security and access control, e.g., to monitor valuable equipment or as components in a car immobilizer system, in aviation for baggage handling purposes, in libraries as a replacement of electro-magnetic and bar code systems of control, for the tracking animals, but also for the tracking of people. It is notable that a club in Barcelona offered its clients a RFID microchip that had to be implanted in their arms, which would gave them access to VIP lounges and could also be used for billing. Last, but not least, RFID chips are used in passports and identity cards, as they provide enhanced security as regards identification of individuals.

2 The risks to privacy

An invasion to informational privacy might occur in case personal data are being processed by automatic or traditional methods. The sole requirement for the respective data protection rules to apply is that information undergoing processing is qualified as personal data, i.e. as information relating to an identified or identifiable natural person, in the sense of the Data Protection Directive.[3] For RFID systems to underlie the provisions of a data protection act it is, thus, required that RFID information are directly or indirectly referred to a natural person (WP, op. cit., p. 8).[4]

This is the case, at first hand, where RFID systems are implemented in order to collect information directly or indirectly linked to personal data, so e.g., where products from a store are tagged with unique product codes which the retailer combines with customer names collected upon payment with credit cards and link them with the customer database. It is also the case where personal data is stored in RFID tags, so, e.g. in transport ticketing. And finally, RFID systems may be used to track individuals without a direct link to a natural person. It may happen, e.g., that a store provides cards with RFID tags to its customers and then monitor their shopping habits and make use of relevant data for marketing purposes. Even if the customer is not directly identified by means of the tagged card, he can be identified each time he visits the same shop as the holder of the card. Similarly, an individual can be tracked by shops which scan tagged products of customers. And further, third parties may use readers to detect tagged items of by passers, violating in that way their privacy (WP, op. cit., p. 6-7).

As it is obvious from the aforementioned examples, RFID technology provides the potential for tracking and profiling of individuals. Due to the fact that RFID tags can be read without line-of-sight and from a distance without being noticed, they are prone for application by retailers for customer profiling, as well as for monitoring for other purposes, e.g., for law enforcement purposes,

[3] Article 2 lit. a of Directive 95/46/EEC, L 281, 23/11/1995.

[4] See, e.g., Weinberg (2007), who points out that: 'It would be a mistake to conclude that an RFID implementation will pose no meaningful privacy threat because a tag does not directly store personally identifiable information, instead containing only a pointer to information contained in a separate database.'

etc. Such practices are infringing, however, the right to privacy of individuals, as they are not complying with basic principles of data protection legislation.

Besides that there are also security threats arising from the fact that RFID tags can be secretly read, particularly in case they are hidden inside product packaging or other items and devices, and since RFID readers can also be concealed (Ayoade, 2007, p. 558). Security issues arise for businesses, referring to espionage, unauthorized access of competitors to customers' preferences and security attacks (DoS, etc.). Personal privacy threats are more important, since individuals are exposed to the risk of their behavior being covertly monitored (Garfinkel et al., 2005).

3 Compliance with legal requirements of data protection

3.1 Directive 1995/46

The Article 29 Data Protection Working Party in working document of January 19, 2005 stresses out those data controllers which implement RFID systems must comply with the obligations of the data protection Directive (WP, op. cit., p. 5 et seq.). Accordingly, the principles related to data quality must be observed, i.e., the use limitation, data quality and conservation principles. Thus, any further processing of data, which is incompatible with the purposes of collection, is prohibited, further that irrelevant personal data must not be collected and data must be kept for no longer than it is necessary for the purpose of collection or processing.

What is more important is that data processing must be based on one of the grounds of legitimization foreseen in Article 7 of the Directive. Thus, data processing will be based in most cases on consent of the data subject, as the other requirements are not fulfilled, with the exception of the case where processing is necessary in order to protect the vital interests of the data subject, e.g. where RFID technology is used in the health sector to track items used in surgical operations or to identify and provide treatment to patients. Wherever RFID systems are implemented, e.g., by stores that offer loyalty cards to their customers should require consent from their customers to collect and process their personal data, since this would go beyond the scope of the contract.

Where RFID systems are used by corporations and stores to track products to prevent theft etc., it is appropriate to examine whether processing is necessary for the purposes of legitimate interests pursued by the controller. In our view, this requirement is not fulfilled, if tags do not incorporate privacy features, such as the "kill" command, i.e. the possibility to permanently or temporarily deactivate the tag, or the blocking of a tag (Ayoade, op. cit., p. 559). Other technical solutions that have been proposed are i) the use of encryption on tags and ii) the inclusion of a privacy bit, i.e. a logical bit

resident in the memory of an RFID tag indicating the privacy properties of the tag (Talidou, op. cit., p. 14).

The Working Party also emphasizes that data controllers that use RFID systems must fulfill the information requirements, guarantee the data subject's right of access and implement appropriate technical and organizational measures. Particularly, as regards the right of information, it is underlined that a retailer shop which employs RFID technology must provide data subjects at least with clear notice about following information: a) the presence of RFID tags on products or their package and the presence of readers, b) whether the presence of such devices enables the tags to broadcast information without individual engaging in any active action, c) the purposes for which the information is used and iv) the identity of the controller. Furthermore, data controllers must inform individuals how to discard, disable or remove tags from products and how to exercise the right of access.

However, here lies a difficulty: how can the owner of a tagged item determine what information is on the tag, who processes the stored data and for which purposes? (Flint, 2006). Due to the technical characteristics of RFID tags the right of information seems hardly realizable and only with increased cost of the tag (Garfinkel et al., 2005).

3.2 Directive 2002/58

The provisions of Directive 2002/58 on privacy in electronic communications apply also to RFID systems, particularly as this was amended by Directive 2009/136[5], which re-defined the field of application of the former Directive. It applies thus "to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices".

Consequently, data controllers must comply with those provisions of the Directive which are relevant in case of data processing in RFID systems. In accordance with Article 5 (3), the storing of information or the gaining of access to information stored in the terminal equipment of a user, i.e. in an RFID tag, is only allowed if the user has given his consent, or if it is necessary for the provision of an information society service. The latter condition is not fulfilled in the context of RFID systems and therefore, consent to write data or gain access to data in RFID tags is compulsory.

The consent of the user is also necessary condition for the use of RFID technology for the purposes of direct marketing, pursuant to Article 13 of the Directive.

[5] See Recital Nr. 56 of Directive 2009/136.

Furthermore, data stored in RFID tags can be regarded as location data, in the sense of Article 2 lit. c of the Directive, i.e. as data indicating the geographic position of the terminal equipment of a user. This is particular significant, since users can be located and their associations can be tracked (Talidou). Article 9 of the Directive provides for that users' or subscribers' consent must be given for the processing, as well as that they must be informed about the details of the processing before they provide their consent.

However, the field of application of this Directive is restricted only to processing taking place in public communications networks and thus, RFID applications which do not use such a network are exempted.

3.3 A Privacy and Data Protection Impact Assessment Framework

The European Commission issued a recommendation of May 12, 2009, in which it elaborated on self-regulation mechanisms and in particular, on the development of a framework for privacy and data protection impact assessment (Recommendation, 2009). In this recommendation it invites EU Member States to ensure that the industry in collaboration with relevant civil society develops a framework for privacy and data protection impact assessment (PIA), which would be submitted for endorsement to the Art. 29 Working Party.

It also calls Member States to identify applications posing information security threats and develop a concise, accurate and comprehensible information policy for RFID applications. It provides that operators must inform individuals of the presence of tags, using a common European sign developed by European Standardisation Organizations. And it goes even further, as it provides that retailers should deactivate or remove at the point of sale tags used in their application unless consumers give their consent to keep tags operational (Commission, op. cit., Nr. 11). This obligation may not apply, in case an impact assessment concludes that tags which used in a retail application and remain operational after the point of sale do not represent a likely threat to privacy.

Subsequently, an informal workgroup led by industry representatives delivered on March 31st 2010, a PIA of RFID applications, in cooperation with stakeholders including consumer groups, standardization bodies, and university scholars.[6] The Working Party was critical and did not endorse the proposed the proposed Framework. It laid down its objection in Opinion 5/2010, in which it invited the industry to propose a revised privacy and data protection impact assessment framework. ENISA also published an opinion,

[6] Industry Proposal on Privacy and Data Protection Impact Assessment Framework for RFID Applications of March 31 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_annex_en.pdf

making recommendations to improve the proposed PIA.[7] Next, the industry redrafted a revised PIA framework and this which was submitted for endorsement to the Article 29 Working Party on January 12, 2011.[8] The Working Party delivered an affirmative opinion, endorsing the Revised Framework.[9] In its opinion, the Working Party acknowledges that a PIA is a tool designed to promote "privacy by design", better information to individuals as well as transparency and dialogue with competent authorities.

4 Regulation vs Self-Regulation

It is indisputable that privacy issues related to RFID technology can not be solved by means of existing legislation alone and that tools other than regulation are necessary. Evidently, the provisions of the EU Data Protection Directive are too general, while the ones of the eCommunication Directive are restrictive as to their scope. In our view, there are two ways to solve this issue: one is to provide for mandatory PIA that would be made available to data protection authorities and the other alternative is to provide for mandatory technical solutions (privacy enhancing technologies) in RFID technology.

In more particular, although the existing Data Protection Directive contains rules that could be applied to data processing in RFID systems, its provisions are very general and in many cases it is unclear whether the processing includes personal data. The eCommunications Directive also contains interesting provisions, but it can only apply in processing taking place in public communications networks.

The PIA Framework that was endorsed by the Article 29 Working Party is an important instrument and its basic advantage is that it applies differently in each specific application, depending on the risk posed. It also provides for the documentation of System Protection and RFID Tag Protection, including access controls, policies on the retention and disposal of personal data, and technical measures such as encryption to ensure the confidentiality of the information, tamper resistance of the tag and deactivation or removal of the tag, if required or otherwise provided. However, the recommendation on which the PIA Framework was based is not mandatory, but it is drafted to provide guidance to EU Member States on the design and operation of RFID applications. Thus, the effects of the proposed measures remain unsure, as it is not certain whether Member States will implement this recommendation and in which way, if they will make it mandatory or introduce it as part of a code of conduct, etc.

---

[7] ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications of March 31, 2010, available at: http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia

[8] Privacy and Data Protection Impact Assessment Framework for RFID Applications of 12 January 2011, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

[9] Date Protection Working Party, Opinion 9/2011, WP 180.

To effectively address the data protection issues posed by RFID technology another regulatory approach is needed. In particular, this will require making the PIA process mandatory, providing also for the notification of its results to the competent data protection authorities, which should have the right to prior checking of RFID systems posing significant privacy risks.

Alternatively, the data protection legislation could introduce specific rules for RFID systems and more particularly, rules establishing technical solutions, since it is difficult to achieve privacy by design by self-regulation. Such rules are already foreseen in the Framework PIA as mentioned above, but they would be more effective once included in mandatory rules.

REFERENCES

Article 29 Data Protection Working Party. Working document on data protection issues related to RFID technology, WP 105, January 19, 2005, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf

Ayoade, J. 2007. Roadmap to solving security and privacy concerns in RFID systems, Computer Law & Security Report 23 (2007), pp. 555-561.

Bannon, A. (2008). RFID: Radio Frequency Identification OR Real Frailty in Data Protection?', The Journal of Information, Law and Technology (JILT), available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2008_1/bannon

Commission Recommendation (2009). On the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C (2009), 3200 final.

Flint, D., 2006. RFID tags, security and the individual, Computer Law & Security Report 22, pp. 165-168.

Garfinkel, S., Juels, A., Pappu, R. (2005). RFID Privacy: an overview of problems and proposed solutions (Computer Society). IEE Security and Privacy May-June 2005, Issue 3, pp. 34-43.

Juels, A. (2006). RFID Security and Privacy: A Research Survey, IEEE Journal on selected areas in Communications, vol. 24., No. 2, February, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.5249&rep=rep1&type=pdf

Levary, R. Thompson, Kot., K., Brother, J. 2005. Radio Frequency Identification: Legal Aspects, 12 RICH. J.L. & TECH. 6 (2005), available at: http://law.richmond.edu/jolt/v12i2/article6.pdf

Synodinou, T., 2009. RFID Technology and its Impact on Privacy: Is Society One Step before the Disappearance of Personal Data Protection, in: Politis, D., Kozyris, P., Iglezakis, I., Socioeconomic and Legal Implications of Electronic Intrusion, pp. 89-107.

Talidou, Z., 2006. Radio Frequency Identification (RFID) and Data Protection Legal Issues, in: S. Paulus, N. Pohlmann, H. Reimer (Eds.), Securing Electronic Business Processes, Vieweg, pp. 3-16.