RFID AND CONSUMERS´ PRIVACY PROTECTION

by

EVA FIALOVÁ*

In a competitive environment it is advantageous for various subjects to possess information about consumer's behaviour and preferences. This information can be gathered from the so called Radio Frequency Identification (RFID) technology incorporated, for example, in product packaging and in customer loyalty cards, and can refer to the consumer, purchased products or to a frequency and time of shopping. When stored in databases, this information can be a subject of profiling, data mining and data sharing. The information about the consumer and his/her private life provides an efficient tool for direct and event driven marketing and other means that directly influence consumer's choices. Furthermore, the RFID technology even allows tracking of a consumer in a specific area. For these reasons RFID represents a threat to consumers´ privacy. The aim of this paper is to discuss whether the current European legislation provides sufficient guarantees to the consumer's right to privacy in connection with the RFID usage. The paper will also sketch out possible solution of this issue in the future.

KEYWORDS:
RFID, privacy, consumer law, European law

1. INTRODUCTION

Radio Frequency Technology (RFID) is a generic name for unique identification of products or persons at a distance using radio frequencies. Data about these objects are stored on a small RFID chip which may be incorporated in objects.

* Masaryk University, evafialova@mail.muni.cz

The technology is not new. RFID has been invented in the nineteen thirties and, similarly to other technologies, its development continued rapidly during the World War II.[1]

The technology finds its application mostly in production and retail sectors. RFID appears increasingly on products or in loyalty cards. It is expected that worldwide market will grow five times over the coming decade, and in the future RFID will replace bar codes. Since RFID allows unique identification, a connection can be made between a certain consumer and products the consumer purchases.

RFID facilitates collection of data. The data may be in a form of personal data, or data about purchased goods as well as shopping habits of the consumer. This data can be subsequently linked to the personal data stored in a database. Afterwards, marketers can make a picture of a private life of an individual without his/her awareness. Therefore, consumer's privacy with regard to the use of RFID should be taken into account.

Since the consumer protection forms an important part of the European free market, the European Community attempts to harmonize this branch of law. This paper will therefore give an overview of European legal provisions that aim to protect consumer's privacy by the use of the RFID technology.

2. TECHNOLOGY

RFID technology is not represented merely by one particular type of device, but it is present in various applications. The common feature of the RFID technology is data transmission from one place to another by means of radio frequencies. The most used frequencies are 125 KHz, 13,56 MHz, 860 tot 950 MHz, and 2,45 GHz.[2] The choice of frequency depends on the planned application. The lower the frequency, the greater is the capability of penetration through various obstructions. Nevertheless, at the same time, the lower frequency means lower propagation speed.

There exist many forms of RFID. The most common are smart labels, tokens, smart cards and implants. Smart labels are suitable for object identification in logistics and retail. Tokens and smart cards serve for identifica-

[1] OECD Working Party on Information Economy DSTI/ICCP/IE(2007)13/FINAL, 18 April 2008, RFID Applications, Impacts and Country Initiatives, p. 6.

[2] Zwenne, G.-J., Schermer B. 2005, Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen (Privacy and other legal aspects of RFID: unique identification of products and persons at distance), Elsevier Juridisch, Den Haag, p. 16.

tion and authentication of persons. The smart cards form a part of loyalty cards. Tokens are used on portable objects (e.g. bracelets) for localization of persons. The implants fulfil the same function as above mentioned tokens and smart cards, but they are implanted in human or animal body.

RFID consists of three components: (i) tag equipped with a chip and antenna, (ii) stable or mobile reader and (iii) RFID middleware. The middleware is software that resides on a server between readers and ICT-infrastructure. Its function is to filter data, and to let only the useful information pass through to ICT-infrastructure.

There exist three types of tags: (i) passive tags that catch the signal emitted by the reader, (ii) battery-equipped active tags that they are able to send the data to the reader without having any previous signal and (iii) semi – passive tags that also contain the battery, but only in order to increase the memory of the chip.

3. PRIVACY

Although the international and the European law protects the private life of the individual, they do not provide any definition of privacy. However, according to the European Court of Justice (ECJ), to formulate an exhaustive definition of privacy would not be possible or even necessary.[3]

Alan Westin deemed privacy as "the claim of individuals, groups and institutions to determine for themselves, when, how, and to what extend information about them is communicated to others".[4] The protection of the information about an individual is at present often confused with the whole privacy issue in general. In contrast, information privacy, i.e. protection of the personal data, constitutes just one part of protection of private life. Undisturbed relationships with family and friends (relational privacy), and communication with other people either by (e-)mail, telephone or by VoIP (communication privacy), represent traditional domains of the private life. Together with the permeation of technology into human life, another sort of privacy should be added, namely absence of disturbance. The disturbance of private life is caused increasingly by email and mobile spam or, as adjudicated the European Court of Human Rights (ECHR), by pollution[5] or ex-

[3] ECJ 16 December 1992, no. 13710/88 (*Niemietz v.Germany*).

[4] Westin, A.F, 1967, Freedom and Privacy, The Bodley Head, Londen, p. 7.

[5] ECHR 9 December 1994, no. 16798/90 *(López Ostra v. Spain)*.

cessive noise.[6] There from follows that privacy "includes those parts of life that are so personal, that any form of interference or influence from outside should be avoided."[7] Privacy has not just an intrinsic value but it is also indispensable for promoting other aspects of human life such as e.g. personal autonomy, freedom of action or freedom of speech.

RFID technology facilitates the accumulation of a large quantity of consumer's data, which are used afterwards for profiling, data mining and data sharing in order to get more information about an individual consumer or a consumer group. Without information about their customers, the marketer would have reduced chances to succeed in the competitive environment.

The email and mobile spamming may inform the customer about products near the end of the shelf time because the marketer has knowledge about all the customers with the loyalty card purchasing such products. The mobile spamming (unsolicited mobile advertising) in RFID-enabled cell phones may disturb the user passing by the every place where the RFID reader has been installed. The RFID-enabled cell phone can be used not only for the mobile advertising, but also for tracking of the user within the reach of the RFID reader either on the street or in the shop.

The marketers may tend to exert pressure on their customers in order to profit from the aforementioned practices. For example, they could discriminate the customers who purchase a product without the RFID tag or who demand the deactivation thereof. These customers could experience disadvantages compared to those who purchase products with the (active) tag that may include, among other things, lower prices for tagged products, different product warranty, or a lack of special services bundled with the tagged product. It is not hard to imagine that such disadvantages could influence consumers´ shopping behaviour by limiting their freedom of choice.

4. PROTECTION OF PERSONAL DATA

Since the RFID facilitates the collection of consumers´ data, the technology becomes attractive to marketers. Therefore, before discussing the European consumer protection legislation, I will give a brief overview of the data protection legislation.

---

[6] ECHR 21 February 1990, no. 9310/81 *(Powell and Rayner v. United Kingdom).*

[7] Blok, P. 2002, Het recht op privacy: een onderzoek naar de betekenis van het begrip privacy in het Nederlandse en Amerikaanse recht (Right to Privacy: The Research on the Meaning of the Notion Privacy in the Dutch and American Law), Boom Juridische Uitgevers, Den Haag, p. 283.

The Directive 95/46 /EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) regulates general principles of processing of personal data. Art. 14 of the Directive covers the data processing for the purpose of direct marketing. The data subject has a right to object to the processing of personal data for such purposes and a right to be informed about the disclosure of the data to a third party for the same reason, as well as to be informed about the right to object to such disclosure. Another directive containing legal provisions referring to the data processing is the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

An increasing number of intelligent cell phones is equipped with the RFID tag. The tag catches a signal emitted by the RFID reader located in a user's environment. The transferred data may relate to a location and time-based mobile advertising (m-advertising), or may deliver a location-based services.[8] The aforementioned directive regulating an unsolicited communication (spam) and location data governs some aspects of the mobile advertising, in particular provisions concerning an unsolicited communication for the purposes of direct marketing (spam) and location data. The directive forbids in art. 13 the unsolicited communication by means of automatic calling machines, fax, email and SMS messages[9], unless the consumer express their prior consent (opt-in), or a marketer obtains electronic contact details from the customer in the context of the sale of a product or a service (opt-out).

The location-based m-advertising is a value-added service of mobile communication. The location data in the sense of the Directive can be processed only with the consent of the user for the purpose of the service. The service provider must inform the users prior to obtaining their consent, of the type of location data, other than traffic data, which will be processed, of the purposes, and duration of the processing, and whether the data will be

[8] King, N. J. 2008, 'When mobile phones are RFID-equipped – finding E.U. – U.S. solutions to protect consumer privacy facilitate mobile commerce', Michigan Telecommunications and Technology Law Review, vol. 15, no. 1, pp. 107-213, p. 117, available at http://www.mttlr.org/volfifteen/king.pdf.

[9] Recital 40 of the Directive.

transmitted to a third party in order to provide a value-added service (art. 9 par.1).

5. INFORMATION

5.1 PRODUCT SAFETY

There exists a close link between the consumer protection and the information provision.[10] In order to protect their privacy and personal data, the consumers must have knowledge about the RFID technology and the presence of the RFID tag on the product. Only with this information, the consumer is able to assess the risks connected with the technology.

In general, the consumers do not have knowledge about the RFID. In 2004, 77% of the consumers were not aware of the existence of RFID.[11] Sixty percent of respondents of the EU Public Consultation on RFID find that there is not sufficient information available about this technology.[12]

The European law does not impose an obligation to the marketers to provide any information about the presence of RFID on the products. The only exception when there is an obligation to inform the consumer is in case of any suspicion related to product's health and safety issues. The Directive 2001/95 /EC of the European Parliament and of the Council of 3 December 2001 general product safety determines that producers provide consumers with relevant information to enable them to assess the risks inherent to the product (art. 5 par. 1). The aforementioned provision would apply in case of detection of concrete risk for human health and safety incurred by RFID. Although no risk for human health is known until now, researchers consider it necessary to do further research in this field.[13] Infection of the product-embedded RFID chips by virus and malware may represent such risk, as this infection could result in the abuse of the chip-stored data by overcoming data encryption.[14] Once any health or safety risks caused by (not de-

---

[10] ECJ 7 March 1990, nr. C-362/88 (*GB-INNO-BM*).

[11] Cap Gemini, National Retail Federation Report, 2004, RFID and Customers: Understanding Their Mindset, Utrecht, New York, Washington, p. 4, available at http://www.uk.capgemini.com/insights-and-resources/by-publication/rfid_and_consumers_understanding_their_mindset/.

[12] Commission Staff Working Document SEC (2007) 312, 15 March 2007, Results of the Public Online Consultation on Future Radio Frequency Identification Technology Policy "The RFID Revolution: Your voice on the Challenges, Opportunities and Threats", p. 3.

[13] Scientific Committee on Emerging and Newly Identified Health Risks 2007, Possible effects of Electromagnetic Fields (EMF) on Human Health, p. 28.

[14] RFID Viruses and Worms, Vrije Universiteit Faculteit der exacte wetenschappen, available at http://www.rfidvirus.org/.

activated) RFID tag on any sort of product equipped with the RFID tag are detected, the producer will have the obligation to disclose information about such risks.

5.2 UNFAIR COMMERCIAL PRACTICES

Providing of information to consumers is regulated by legal rules relating to unfair commercial practices. The provision that prohibits these practices is the Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market. The reason for the prohibition of the unfair business-to-consumer commercial practices is their potential to distort the economic behaviour of the consumer. Such practices may influence the consumer to the extent that he/she takes a transactional decision that she would not have taken otherwise.

The Directive focuses on an average consumer, i.e. reasonably well-informed and reasonably observant and circumspect.[15] This raises a question whether the average consumer is able detect the presence of the RFID tag. Since most consumers do not have any knowledge about the RFID, the average consumer has no ability to notice the presence of RFID.

The unfair commercial practices occur in the form of misleading or aggressiveness. For the purpose of this analysis, the misleading action, respectively omission is particularly relevant. Misleading action is a provision of false information that deceives or is likely to deceive the average consumer (art 6 par. 1). The influence of the consumer's choice can occur by providing false information by the marketer about the presence of RFID tags, their function or information about the deactivation thereof. This false information may cause the consumer, who originally did not want to purchase a product with (deactivated) RFID tag, to take the transactional decision that he/she would not have taken if he/she had had the correct information. Given that the average consumer has little knowledge about the RFID technology, the misleading is relatively simple.

In case of misleading omissions, the marketer does not intentionally provide information that the average consumer needs in order to take an informed transactional decision (art. 7 par. 1). As misleading omission may be considered the case when the marketer knows that the consumer would not have purchased the produce if he/she had known about the presence of the

[15] ECJ 26 July 1998, no. C-210/96 (*Gut Springenheide*).

RFID tag, and the marketer does not provide such information to the consumer.

5.3 ADVERTISING

Advertising is nowadays a means through which consumers receive substantial part of information about products on offer. Advertising by the marketer is limited by a number of European rules predominantly for a particular sort of product (e.g. alcohol or tobacco). The regulation that does not apply to a specific sort of product but rather to the way of advertising is the Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising.

The Directive forbids the misleading of the consumer by advertising statements. Misleading advertisement deceives or is able to the persons to whom it is addressed or whom it reaches, and is therefore likely to affect consumers' economic behaviour. It can also injure, or may be likely to injure a competitor (art. 2 b). Misleading advertisement could thus provide the consumer with false information about the presence of RFID tags or the deactivation thereof on certain goods.

While the misleading advertisement is forbidden, comparative advertising, i.e. the advertising which explicitly or by implication identifies a competitor or goods or services offered by a competitor (art. 2 c),is permitted under certain conditions set by the Directive. The advertisement, among others, must not be misleading, it must objectively compare one or more relevant, verifiable and representative features of the goods and services in a way that does not discredit or denigrate trademarks, trade names or other distinguishing marks of a competitor (art. 4). A statement containing information about presence of RFID tags on products of another marketer providing that the marketer meets all conditions laid down by the Directive may be seen as the comparative advertising.

6. FREEDOM OF CHOICE

When concluding a contract, parties to the contract enjoy relatively broad freedom known as contractual autonomy. Theoretically, the marketer and the consumer may set down terms and conditions after mutual agreement. In reality, the marketer determinates the terms and conditions without having negotiated with the customer, who can either "take it or leave it", or who can not choose at all in case of an indispensable product. Thus, the

marketer are free to impose different pricing or warranty on their customers to differentiate those customers that purchase a product with RFID tag or let the marketer to leave tag active and those, who purchase the product without tag or require the deactivation. Providing that the principles of fair commercial practices and contract terms are not violated, these practices are legal. The aim of these practices is to influence the consumers so that they purchase products with the (active) RFID tag.

The European Community considers the consumer's choice to be an important part of the consumer´s protection. According the European Consumer Policy Strategy for the year of 2007-2013, the possibility should increase for the consumer to make a real choice.[16] The strategy does not refer to RFID technology. The principles that deal specifically with RFID are Principles for responsible deployment and operation of electronic product codes[17], adopted by the International Chamber of Commerce.[18] Art. 2.1 states that products or their packaging containing EPC tags should be labelled.

The contractual autonomy in the consumer law is limited by the Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. The contractual term is considered unfair in case that it causes a significant imbalance in the parties' rights and obligations to the detriment of the consumer if the term has not been individually negotiated (art. 3 par 1). The contracts in writing must be drafted in plain and intelligible language (art. 5). The consumer is not bound by the unfair term and the contract continues to bind the parties only if it is able to exist without this unfair term (art. 6 par. 1).

The contract term would be considered unfair if the marketer is not liable for a leak of personal data of consumers on RFID chip or software under his control. Other unfair terms in connection with the RFID technology would be those written in complicated technical language, using unintelligible abbreviations, etc.

---

[16] Communication the Commission to the Council, the European Parliament and the European Economic and Social Committee COM(2007) 99 final, 3 March 2007, EU Consumer Policy Strategy 2007 – 2013, p. 5.

[17] The electronic product code is unique identifier based on RFID, which is supposed to replace barcode.

[18] International Chamber of Commerce, Principles for responsible deployment and operation of electronic product codes, available at http://www.iccwbo.org/uploadedFiles/ICC/policy/marketing/pages/6rev8_FINAL_EPC_Principles.pdf.

7. RECOMMENDATION ON RFID

The European Union follows the rapid development and deployment of the RFID applications. Even if the EU considers the RFID development potentially jeopardizing privacy and personal data protection, this technology constitutes, according to the Union, RFID represent challenge for business opportunities, cost reduction and combating counterfeiting.[19] Therefore the EU drafts a number of proposals, which are not for the time being legally binding. One of them is the Recommendation on Implementation of Privacy and Data Protection Principles in Applications Supported Radio-Frequency Identification. The Recommendation encourages member states to oblige RFID operators to inform individuals of the presence of tags placed on or embedded in products along with raising awareness of the RFID technology among the public.

The Recommendation also contains rules for the tag deactivation and removal. Retailers should deactivate or remove tags at the point of sale, unless consumers give their consent to keep tags operational (opt-in). Deactivation or removal of tags by the retailer should be done immediately and free-of-charge. Afterwards the consumers should be able to verify the effectiveness of the deactivation or removal. Nevertheless, this should not apply if the active tags do not represent a likely threat to privacy or the protection of personal data. Likewise, in this case the retailers should deactivate or remove these tags on request of the customer (opt-out). Considering that the privacy and personal data protection is not threatened by RFID as such but rather in connection with other means and practices, the above mentioned provision seems to be problematic. The opt-in rule should be the only principle applied on the RFID tags in retail.

The Recommendation states at the same time that the deactivation or removal of tags should not entail any reduction or termination of the legal obligations of the retailer or manufacturer towards the consumer.

8. CONCLUSION

The RFID technology facilitates accumulation of the consumers´ data. In order to learn about consumers' shopping preferences and habits, the marketers use the information generated from the data. Some practices are able

[19] Recital 3 of the Recommendation on Implementation of Privacy and Data Protection Principles in Applications Supported Radio-Frequency Identification, (2009) 3200 final, 12 May 2009.

to infringe consumers' privacy. In particular, this includes manipulation with the data by profiling, data mining and data sharing, tracking RFID-enabled devices and email or mobile spamming. To get the advantages that RFID provides, the marketer may tend to influence consumers' behaviour and thus limit the consumers' freedom of choice by discriminating those who do not purchase products equipped with the RFID tag or demand its deactivation.

The European consumer law does not refer to the RFID technology. The law does not impose any obligation on the marketers to inform the consumers about the presence of the RFID tag on their products, in case these products do not pose a risk for health and safety. In case the marketer has knowledge that the presence of the RFID tag is essential for the consumer's transactional decision, and he provides false or no information about this fact, he would be liable for unfair commercial practices. When informing about the RFID technology used by the concurrent, the marketer must obey the provisions on misleading and comparative advertising. The marketers may be inclined to abuse consumer's ignorance of RFID and make a significant imbalance in rights and obligations of a contract. Such unfair contract terms would not be binding for the consumer.

The European Community attempts to protect consumers against privacy infringements caused by RFID. However, the measures taken are for the time being in the form of not binding recommendation.