

Chapter 5

Regulatory Framework

Standards and information for potential users are not the only prerequisites for technological growth. It is also important that the legislative framework is reliable and supports the development of a new technology. In this chapter we analyse, from a legal point of view, issues which affect RFID. These issues relate notably to privacy and security, the impact on health and environment, Intellectual Property Rights (IPRs) and RFID governance. Recommendations for regulatory actions are drawn for each topic.

5.1 Privacy

Privacy is probably the topic which receives the most attention. Unlike barcodes or magnetic stripe cards, RFID technology does not require line of sight contact, allowing the data stored in the tag to be read without any notice or previous action from the data subject. This is the reason why a number of privacy concerns have been raised over the last few years with regard to this new technology which is predicted to reach widespread implementation in the upcoming future. In most cases RFID applications do not involve the storage of personal information related to an individual (like name, address, date of birth) on a tag (Strüker et al. 2008) but only a unique identification number (like a barcode) and, therefore, do not involve privacy issues. However, some RFID applications may directly or indirectly enable the identification of an identifiable person and bring about the risk of their disclosure to unwanted parties. A case-by-case approach should therefore be adopted.

In this chapter we will provide a summary of the most relevant privacy-related legislation at the European level, and a brief analysis of the privacy principles and rules that form the basis of the data protection legal framework. From this general level we will then go into a specific analysis of the privacy impact of RFID, compiling the relevant legal documents and developing an application-specific view (illustrated by real cases) on the privacy concerns raised by RFID. The aim is to

analyse the existing legal framework alongside actual RFID applications to conclude whether or not new laws might be necessary, and which are the alternative options to address privacy concerns.

5.1.1 Legal Framework

In addition to the RFID-related EU privacy legislation (see Table 5.1 for a non-exhaustive catalogue), the “Communication on the follow-up of the Work Programme for better implementation of the Data Protection Directive” (COM(2007) 87 final) concludes that there is no need for amending it, in view of the current technological status. Furthermore, the “Communication: Promoting Data Protection by Privacy Enhancing Technologies (PETs)” (COM(2007) 228 final) sets up three main objectives in the way forward for the use of PETs: development, use availability and encouragement of consumers.

Regarding RFID in particular, in 2006 the European Commission carried out an online public consultation on the primary concerns of the citizens concerning the technology. The process ended in March 2007 with the release of the “Communication from the Commission regarding Radio Frequency Identification (RFID) in Europe: steps towards a policy framework” (COM(2007) 96 final, SEC(2007)312). According to the Commission, “further development and widespread RFID deployment could further strengthen the role of information and communication technologies (ICT) in driving innovation and promoting economic growth. Already today, Europe is a leading region in RFID-related research and development, not least thanks to the support of the European research programmes”. Additionally, the Communication identifies a number of topics for which the question of adequacy of the legal framework may be raised. This chapter has taken in account the issues proposed by the Commission in the analysis of the relation between RFID and legislation. A Recommendation on privacy and security aspects raised by the RFID technology should be further adopted by the European Commission in the second-half of 2008.

The “Working Party on the protection of individuals with regard to the processing of personal data” (so called “Article 29 Working Party”), set up under the Data Protection Directive, also adopts documents giving guidelines related to data protection (e.g. “Opinion 4/2007 on the concept of personal data”, 01248/07/EN – WP 136). On January 19th, 2005, the Article 29 Working Party published in particular a working document on data protection issues with regard to RFID technology (10107/05/EN WP 105). The working document is aimed at a) providing guidance to companies deploying RFID on the application of the basic principles set out in the directives, and b) providing guidance to manufacturers of the technology as well as RFID standardisation bodies on their responsibility towards designing privacy and compliant technology. It analyses RFID technology and its implications with regard to data protection matters, studying applications, privacy and security issues, and technical solutions.

Table 5.1 RFID-related EU privacy legislation

Name	Summary
Consolidated versions of the Treaty on European Union and of the Treaty establishing the European Community (OJ C 306 17.12.2007)	Art. 6 of the Treaty on European Union guarantees the respect of the fundamental rights laid down by the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (Art. 8), and Art. 286 deals specifically with data protection.
Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (OJ C 306 17.12.2007)	Not yet in force. It will introduce specific provisions concerning human rights and fundamental freedoms (Arts. 1.8, 2.29).
92/242/EEC: Council Decision of 31 March 1992 in the field of security of information systems (OJ L123, 8.5.1992, p.19)	Sets up the basic framework for developing a protected environment in the field of data storage and processing. It represents the starting point for the following legal texts in the field of data protection and data security.
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 of the free movement of such data (so called “Data Protection Directive”) (OJ L 281, 23.11.1995, p.31)	The directive establishes the main principles for lawful processing of personal data; it is the cornerstone of the European Data Protection legal framework.
Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and of the free movement of such data (OJ L 8, 12.1.2001, p.1)	The regulation provides rules to process personal data within the different European institutions and bodies, and establishes an independent body for supervision of their application.
Directive 2002/21/EC of the European Parliament and the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)	The directive establishes a harmonised framework for the regulation of electronic communications networks and services.
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 (so called “ePrivacy Directive”) OJ L 201, 31.7.2002, p.37 (amended by Directive 2006/24/EC)	The directive deals with a number of issues such as data retention, the use of cookies and the inclusion of personal data in public directories. Its scope is limited to “the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks.”

In order to complete the picture of applicable regulations, industry guidelines and self-regulation must also be discussed. Guidelines, in this project, are seen as implementation guidelines, i.e. “domain-specific documents assisting companies and organisations when implementing and using RFID systems with regard to possibly affected stakeholders. Such guidelines need to address specific concerns of entities within companies and organisations that implement or use RFID systems” (see Chapter 4.2.3). Self-regulation, on the other hand, is understood within the project as regulations which companies or entities impose on themselves and abide to. According to this meaning, self-regulation would be placed between guidelines, which are simply advice, and law, which must be adhered to. In any case, self-regulation and legislation are two sides of the same coin; both are intended to ensure that privacy is respected when implementing RFID. To be efficient, self-regulations need to be coherently enforced by the industry: while admitting that by their own nature they cannot be legally enforced, self-regulations would make little sense if they are not respected by their addressees. For a deeper analysis of guidelines and RFID see Gampl et al. (2008a).

5.1.2 Data Protection Principles and the Definition of Personal Data

As we have already stated, Directive 95/46 (“Data Protection Directive” hereinafter) laid down the general basis of the European data protection legal framework. Its articles (further developed or modified by other legal texts) introduced the principles and common rules that should be followed to ensure lawful processing of personal data. Furthermore, the definition of personal data contained in Art. 2 of the said directive is the key to determine which applications fall within the scope of the text. In the following paragraphs the content of the most prominent articles within the Data Protection Directive will be briefly described, in order to establish the basis for the subsequent study of RFID and privacy.

5.1.2.1 General Content

The scope of the Data Protection Directive, stipulated in Art. 3, is restrained to the processing of personal data carried out entirely or partially by automatic means, and to the non-automatic processing of personal data “which form part” or “are intended to form part” of a filing system. This means that an application dealing with data not qualified as personal falls out of the scope of the Data Protection Directive. The text is applicable to all controllers established in Member States or territories where Member State’s law is applicable (Art. 4). According to the Data Protection Directive, a controller is “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (...)” (Art. 2. (d)).

5.1.2.2 Data protection Principles

The Data Protection Directive lays down a number of principles that Member States shall determine more precisely, how the processing of personal data should be carried out in order for it to be lawful. These constitute the data protection principles and are covered by Arts. 5 to 8. The conditions, under which a processing of personal data qualifies as lawful and legitimate, break down into three different types: data quality, legitimate processing and special categories of processing.

In order to ensure the quality of the personal data (Art. 6), the controller should ensure that personal data is:

- Processed fairly and lawfully (the processing shall comply with every legal provisions concerning data protection);
- Collected for specified, explicit and legitimate purposes: when the processing proves to be incompatible with those purposes, it shall not be allowed. Exemptions can be found in historical, statistical and scientific purposes;
- Adequate, relevant and not excessive in relation to those purposes;
- Accurate and kept up to date;
- Kept in a form which permits identification of data subjects for no longer than necessary;

The processing of personal data will be considered legitimate only if one or more of the following criteria are met (Art. 7):

- The data subject has unambiguously given his or her consent. Forced, unclear or non implied consent shall not qualify;
- Processing is necessary for the performance of a contract to which the data subject is party, or at the pre-contractual level;
- Processing is necessary for compliance with a legal obligation of the controller;
- Processing is necessary in order to protect the vital interests of the data subject;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, conferred to the controller or to an authorised third party;
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed (invalid if the data subject's rights and freedoms could be harmed by such processing).

According to Art. 8 concerning special categories of processing, the processing of personal data shall be prohibited (with exceptions such as medical purposes, for example) if it reveals or concerns racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life; unless:

- the data subject has given his or her consent,
- processing is necessary to protect the vital interests of the data subject or
- data has been made public by the data subject.

5.1.2.3 Other Rules under the Data Protection Directive

- The data subject should be given certain information, such as the identity of the data controller, the purposes of the processing or the existence of certain rights (access, deletion, etc.).
- The data subject has the right to access, rectify and to block access to his or her data. They are also entitled to object at any time to the processing of data relating to them.
- No one can be legally affected by a decision taken on the basis of a pure automated processing of data.
- The controller shall make sure that the processing is secure and confidential. Furthermore, they “must implement appropriate technical and organisational measures to protect personal data” (Art. 17).

For a deeper analysis of the Data Protection Directive please refer to the extended project report on European RFID legislation (Kruse et al. 2008).

5.1.2.4 The Definition of Personal Data

Article 2 (a) of the Data Protection Directive defines personal data as follows:

Personal data shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

The concept of personal data is the key provision to determine whether a particular technology application falls within the scope of the Data Protection Directive. Only those applications which involve personal data shall comply with the above principles regarding processing.

However, *what* should be understood as personal data has been the subject of an intensive debate; in this section we will try to clarify the concept so as to establish a basis to analyse the different kinds of RFID applications, and whether they involve personal data or not.

According to the Article 29 Working Party the analysis of the definition should be focused on the first sentence of the paragraph of Art. 2(a): “any information relating to an identified or identifiable natural person” (Art. 29 Working Party, WP136, 2007).

“Any information” shall include subjective and objective information, not necessarily true or proven, made available in any form (e.g. e-mail), and including biometric data (“biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability”). The most important feature about this kind of data is that it could serve as a link between a particular individual and certain information.

For information to be classified as “relating to” someone, the information shall be about a person (e.g. name, address), or, in the cases that it is not about a person, it shall be possible to use it to take some actions over an individual or in a way that has some kind of impact on them. That information can be direct (when accessing X’s hospital records, that information is “directly” related to X), or indirect (one gets to discover X’s personal information by knowing X’s car registration number and by that gets access to the car registration record including X’s personal information).

The person shall be understood as “identified” when they are “distinguished” within a group of persons by using (a) certain characteristics to identify them, be it name, date of birth, or eye colour. The subject will be classed as “identifiable” when it is simply “possible” to identify them within a group, hence the suffix “-able” (Art. 29 Working Party, WP136, 2007).

The individual can then be identified directly (e.g. by name) or indirectly (e.g. by passport number, car registration, or a combination of records which allows an individual to be identified). As to determine whether a person is identifiable or not, Recital 26 of the Data Protection Directive states that:

“whereas to determine whether a person is identifiable, 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 accordance with Recital 26 of the Data Protection Directive, the Art. 29 WP considers that “*a mere hypothetical possibility to single out the individual is not enough to consider that person as “identifiable”*” (Art. 29 Working Party, WP136, 2007). If, taking into account “*all the means likely reasonably to be used by the controller or any other person*”, the possibility to identify an individual through the data involved with a particular technology application does not exist or is negligible, the person should not be considered as “identifiable”, and the data concerned should not be considered as “personal data” (Art. 29 Working Party, WP136, 2007).

The Art. 29 WP adopted a pragmatic approach regarding the assessment of whether a person is “identifiable” or not by stressing that “*the criterion of ‘all the means likely reasonably to be used either by the controller or by any other person’ should in particular take into account all the factors at stake. The cost of conducting identification is one factor, but not the only one. The intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, as well as the risk of organisational dysfunctions (e.g. breaches of confidentiality duties) and technical failures should all be taken into account. On the other hand, this test is a dynamic one and should consider the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed. Identification may not be possible today with all the means likely reasonably to be used today.*” (Art. 29 Working Party, WP136, 2007).

In the case where the information was collected with the purpose of identifying individuals, the person shall be considered as “identifiable”.

However, where identification of the data subject is not the purpose of the processing, the technical measures to prevent identification have to play a very important role. As explained by the Art. 29 WP, *“putting in place the appropriate state-of-the-art technical and organizational measures to protect the data against identification may make the difference to consider that the persons are not identifiable, taking account ‘of all the means likely reasonably to be used by the controller or by any other person’ to identify the individuals. In this case, the implementation of those measures is not the consequence of a legal obligation arising from Art. 17 of the Directive (which only applies if the information is personal data in the first place), but rather a condition for the information precisely not to be considered to be personal data and its processing not to be subject to the Directive.”* (Art. 29 Working Party, WP136, 2007).

As for the term “natural person”, it should be assumed that data related to dead people should not generally be considered to fall within the scope of the Data Protection Directive. Legal persons are also, in principle, excluded although there are some exemptions.

5.1.3 RFID and Data Protection Legislation: a Case Specific Approach

Having outlined the general legal provisions governing data protection, the question is now to apply those rules to RFID technology applications on a case-by-case basis.

As any technology involving data, RFID technology falls, in principle, into the scope of the Data Protection Directive. However, the provisions of the Data Protection Directive will only apply to a specific RFID application when the RFID application concerned can be considered as involving “personal data”. In this respect, we have classified below the different types of RFID applications, depending on whether or not they involve personal data as provided by Art. 2(a) of the Data Protection Directive.

5.1.3.1 RFID Tags Containing no direct, indirect or potential Identifiers

Most RFID tags only contain information (usually just a unique identification number) related to the product concerned, purely used for organisational and production effectiveness purposes within a company or throughout the supply chain. In this case, the individuals in contact with those tags are only the employees of the companies concerned and, if the application concerned would allow identification of a particular employee, the principles governing processing of personal data apply and any action challenging the employee’s privacy is prohibited (see below Chap. 5.1.3.5).

For RFID logistics and manufacturing applications, information can not therefore in principle be directly related to a specific data subject or lead indirectly to the identification of a specific data subject. For example, in the case of RFID devices used for preventing the use of counterfeited or damaged components in aeroplanes and vehicles, RFID is used for ensuring safety and security in high risk environments, and therefore identifiers are given to the components of either vehicles or aeroplanes. A tag can be placed on each part of the craft, and the tag stores a unique identification number that, when interpreted by a reader, allows the employees of the company concerned to know where the part should be placed, and if it is adequate and authentic. In this process, no data subject outside the company concerned is involved and no personal data is stored on the tag, therefore, there is no indirect or direct personal data involved. Another example can be found in the area of closed loop logistics, with companies tagging their packaging containers for control purposes. Again, no personal data is involved, since the containers are classified with numbers and only for management reasons.

As a result, it is generally agreed that the Data Protection Directive's provisions regarding the process of personal data are not applicable to logistics and manufacturing RFID applications as no personal data is involved.

Once the consumer comes into contact with the tagged product, some privacy concerns may, however, be raised due to the possible link between the unique identification number stored on the tag and some personal data of the consumer stored in a database (see Chap. 5.1.3.2). This is in particular the case for applications in the retail industry even though the tags do not store personal data of a data subject, like tags used for logistics or product maintenance and quality control purposes do.

5.1.3.2 RFID Tags which store Information that could be linked to Personal Data

This is the situation where “*indirect*” identification might take place: the tag contains a unique identification number that can be reasonably linked to a particular person and/or personal data.

In the retail sector for instance, tags can be currently placed on products in order to make the work of the staff easier and to improve the logistics of the store and customer's service. They do not have the purpose of identifying the retailer's customers.

No personal data of an individual is stored on the tags and read alone, they contain a unique identification number enabling the recognition of the product and possibly some further information regarding the product concerned (e.g. expiration date, country of origin).

If a product is tagged and read in the store (regardless if the tag is deactivated before leaving the store or not) and if the customer is not identified by means of a loyalty or credit card for instance in the store (usually at the check out point), the customer cannot then reasonably be identified through the RFID tag by the retailer or after having left the store, due to the fact that their personal data has

not been disclosed and could not be potentially linked to the unique identification number on the tag.

However, when linked to the personal data of an individual extracted from a database, related for instance to the customer's loyalty card or credit card, the unique identification number stored on the tag can, in principle, be potentially used to identify an individual. Nevertheless, in practice, identification through a credit card's database is complicated since the process is encrypted, and the data stored is secured according to applicable data protections laws to be used only for specific purposes to which a user expressly consented.

Therefore, only linking between a unique identification number on a tag with the personal information of an individual stored in a database makes a person "identifiable" (as explained above), which means that, in such a case *"taking into account all the means likely reasonably to be used by the controller or by any other person to identify the individuals"*, the RFID application concerned may be considered as involving personal data, and, thus, be subject to data protection rules. Furthermore, according to the Art. 29 WP, the RFID applications potentially enabling the identification of persons, but of which the purpose is different (such as logistics enhancement), particularly require *"appropriate state-of-the art technical and organisational measures to protect the data against identification"* (see above WP136, 2007).

In contrast, RFID application may in other sectors, like in healthcare, have the purpose of identifying persons, which makes the application of data protection rules more obvious. In the trial held in the AMC Hospital in Amsterdam for instance, patients received RFID tagged bracelets on their arrival. The tags contain a unique identification number which is linked to the hospital's database where medical records are stored. Tags were also used to identify blood transfusion instruments and respective patients in order to avoid mismatches. Therefore, those types of applications should be considered as involving information relating to identifiable individuals and the processing should be subject to the data protection rules.

According to Recital 26 of the Data protection Directive and following the recommendation of the Art. 29 WP (WP 136, 2007), due to the large number of RFID applications, the analysis of whether or not a person can reasonably be considered as identifiable by a specific RFID application should, therefore, be done on a case-by-case basis, taking into account factors such as the cost of the identification, the purpose, the expected advantage for the controller, the interests of all the parties, the security device applied etc.

In its "Working document on data protection issues related to RFID technology" (WP 105, 2005), the Art. 29 WP mentions a number of hypothetical examples with regard to the profiling of consumers and inducing malicious and unlawful processing of personal data.

However, a number of factors should reasonably prevent those kinds of situations from happening. First of all, the current level of technology does not allow such tracking. Secondly, from a practical point of view, it is hardly feasible that a company could trace a customer by obtaining only one identifier.

In addition, and assuming that the technology would be available, the profiling of individuals is already forbidden by law, and thus, any company using such techniques to track unknowing individuals would be committing a punishable criminal offence.

Furthermore, as with any other technology, RFID applications may be the object of malicious and unlawful usage from third-parties. However, an RFID application user having carried out a privacy impact assessment prior to the development of the RFID application and having installed state-of-the-art security, technical and organisational measures related to the privacy risk concerned, this user should be considered as having taken all reasonable measures to prevent all reasonable privacy risks linked to its RFID application. This user cannot be held liable for any malicious and unlawful usage of its RFID application by a third party and should not be prevented from implementing his or her RFID applications.

According to Art. 29 WP, guidelines on the compliance of the data protection requirements would help implementing RFID applications for the benefit of the industry and of the society alike.

5.1.3.3 RFID Tags which store Personal Data

In December 2004 the European Council adopted Regulation (EC) 2252/2004 introducing the so-called “European Biometric Passport” by 2005. However, due to significant delays, only some of the Member States had issued the passports containing a facial image on the tag on time, i.e. by 28 August 2006. By 28 June 2008, the Member States shall have two fingerprints added to the information contained in the chip. As already mentioned (Chap. 5.1.2.4), biometric data are considered as an additional category of personal data and are, therefore, covered by the Data Protection Directive and related legislation. Biometric passports are probably the most obvious example of an RFID application containing personal data.

RFID applications including tags storing personal data have to comply with the provisions of the Data Protection Directive and related legal instruments and are therefore covered by the existing legislation.

There are, however, limited examples where RFID applications with storage of personal data on the tag. In most of the RFID applications of today and tomorrow, the way to identify a person is by combining the unique identification number on the tag held by a person with a back-end database where personal data of the concerned individual is stored.

5.1.3.4 Applications of the Data Protection Principles to RFID

RFID technology, as any technology, principally falls into the scope of the Data Protection Directive. As explained above, however, the provisions of the Data Protection Directive will be applicable to a particular RFID application when it involves the processing of personal data according to Art. 3.1. of the Data Protection Directive. Consequently, the application of the provisions of the Data Protection

Directive should then be determined on a case-by-basis depending on whether the RFID application concerned involved personal data, making a person identifiable.

In particular, all data protection principles (see Chap. 5.1.2) imposed by the Data Protection Directive should be adhered to by the controller. In the case of RFID applications, the “controller” would be the user of the tag, who determines the purpose of that tag used in combination with the processing of the tag information to the reader and from the reader to other means, such as databases. The user is bound to the requirements of purpose limitation, proportionality and conservation principles laid down by Art. 6 of the Data Protection Directive. This means that both the controller and the manufacturer of the RFID tags shall structure the system in such a way that only the necessary data is collected and processed for specific purposes, and that their content is proportional to the purposes for which they were collected.

Concerning the legal grounds for processing, as provided by Art. 7 of the Data Protection Directive, the key element is the consent of the data subject. The processing of personal data is lawful and allowed provided that the data subject has unambiguously given his or her consent, except in some cases. Consent should be given freely, specifically and unambiguously. However, the Data protection Directive does not provide a specific method on how to grant that consent.

Besides, Art. 8.2 of the Data Protection Directive requires consent for the processing of sensitive data “explicitly”, which may suggest that not in all cases “explicit” consent of the data subject is required under the Data Protection Directive. “Explicit” and “tacit” consent could then be differentiated depending on the type of personal data concerned. Furthermore, several authors have supported the idea that a “tacit” consent shall suffice in most of the cases and therefore, that opt-out shall be the general rule (Téllez 2002, Aparicio 2000, among others). The Art. 29 WP seems also to accept that opt-out provides “practicability and flexibility” (WP 131, 2007).

For RFID applications storing personal data on the tag or having the identification of persons as their purpose, the data subjects are, in practice, generally asked to give their consent explicitly.

For RFID applications not used for the identification of persons, but where a potential may exist that information is linked to an identifiable person, supplementary consent is usually put in relation with the deactivation of the tag, in addition to the necessary consent from the data subject for processing personal data. Two scenarios with regard to the granting of the data subject’s consent could then been identified: “opt-in” (standard deactivation) and “opt-out” (deactivation on request). In the first case, the idea is that the data subject *should actively* give their consent specifically to the RFID application; this would imply, for example, that retailers using tagged items shall provide devices to deactivate all tags unless the customer gives his or her explicit consent for the tag(s) to remain active after leaving the premises. In the latter case, the tags would remain active unless the data subject expresses the desire of deactivating it. Today, the retailers having developed some RFID applications generally adopt deactivation on request by making deactivation device available to the customers before leaving the store.

On one hand, the risk and privacy impact assessment conducted by retailers has shown that adoption of an “opt-out” solution (deactivation on request) is the best option since it addresses the potential privacy risks reasonably raised by their RFID applications while ensuring their development and taking into account the current technologies available. Deactivation on request is, however, developed in combination with a good information system towards the consumer in order for them to make their cost/benefit assessment regarding tag deactivation, and then to make a choice in a fully informed way. Retailers also adopt all technical and organisation measures to ensure data security and do not illegally link RFID data with personal data.

On the other hand, the risk and privacy impact assessment performed by the retailers shows that the “opt-in” scenario (deactivation by default) would impose high technical and costly burdens on retailers and prevent the development of beneficial after-sales use cases for maintenance or food safety purposes for instance. In the case of a small or medium private retailer deploying no specific RFID application for its own use but selling tagged products (the manufacturers having tagged their products purely for logistical purposes), the generalisation of the “opt-in” scenario would oblige the private retailer to implement a RFID deactivation solution, even though it does not use RFID for its own use. Furthermore, considering that it is not possible for manufacturers to differentiate at the production level products to be sold to private retailers and to retail chains, and the state-of-the-art deactivation solutions which do not allow deactivation of all types of tags with one device, the practical and technological burdens linked to the deactivation by default seem not proportionate to the privacy risks raised by the RFID applications.

In view of the future expanded use of RFID in the retail sector, the upcoming Recommendation of the European Commission on privacy and security should especially give further guidance for the development of RFID applications by retailers, taking particularly into account the privacy of the consumers, the state-of-the-art technology, the practical circumstances of a retail environment, and the consumer benefits of after-sale RFID applications for maintenance or food safety purposes.

For all RFID applications storing personal data on the tag or enabling on purpose or not the identification of a person, two prerequisite conditions must be complied with: full information to the data subject and security of processing (i.e. taking all reasonable technical and organization measures preventing the identification of the data subject).

According to Arts. 10 and 11 of the Data Protection Directive, the data subject should be informed of a number of points, such as the identity of the data controller, the presence of RFID applications and the possibility that information could be read without any action from the subject. Information is the key when it comes to RFID and privacy. Several solutions have been proposed, from using pictograms to the handing over of notices for consumers (OECD 2008a). In cases where the applications make it impossible to provide complete information to the data sub-

jects, signs such as those used for the CCTV (Closed Circuit Television), such as “RFID used here” have been considered.

Nevertheless, in view of the lack of general knowledge of the benefits and risks of RFID technology and applications, an extensive public information campaign on the purposes, effects, advantages and disadvantages for both the industry and the society of RFID technology could, in principle, play a major role in the process of familiarising the public with it, and could also favour its widespread implementation in full respect of privacy rights.

In addition, implementation of technical and organisational measures would make the RFID application in compliance with the requirements on the security of processing provided by Art. 17 of the Data Protection Directive and would enable the data subject to exercise his/her rights of access and to object as provided in Arts. 12 and 14 of the Data Protection Directive.

In general, security of processing should be addressed by means of Privacy Impact Assessment prior to the implementation of RFID applications (OECD 2008a). There are already today some technical guidelines for implementation and utilisation of RFID-based systems, such as those currently developed by the German federal office for information security (BSI), which explain the method to follow.

Today, the retailers who have developed some RFID applications generally adopt deactivation on request by making a deactivation device available to the customers before leaving the store.

According to the Art. 29 WP, where identification of the data subject is not the purpose of the RFID application but may potentially be possible, implementing technical measures to prevent identification plays a very important role since it should avoid the information to be qualified as personal data and its processing to be subject to the Data Protection Directive (Art. 29 Working Party, WP136, 2007).

Technical measures may offer a number of options to secure RFID devices in order to protect privacy: tags could be designed in order to limit the potential privacy risks of some RFID applications. This is what has been labelled as “Privacy by Design”. Depending on the privacy risks linked to the specific applications foreseen, different designs of RFID devices would be available in order to provide the most adequate technical security. Linked with the notion of “Privacy by design” is the concept of Privacy Enhancing Technologies as provided by the European Commission (“Communication: Promoting Data Protection by Privacy Enhancing Technologies” COM(2007) 228 final). According to the PISA project (Privacy Incorporated Software Agent), PETs are *“ICT measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system”*. Some of the technical measures to implement data protection provisions are: techniques enabling visual indications of activation, data tracks to access personal data, “kill” and “sleep” commands, privacy bits (i.e. a bit placed on the memory of a RFID tag that determines whether the tag can be read by all readers or only authorised readers), clipping antennas, blocker tags or “Faraday cages” to ensure the right to erase or block the data (Kruse et al. 2008).

Information and security requirements are at the core of any RFID applications and should be treated carefully by RFID deployers in order to address privacy concerns linked to its RFID application in an adequate and proportionate manner. Implementation of any RFID application should be made only after an adequate Risk and Privacy Impact Assessment according to the applicable guidelines, if any.

5.1.3.5 RFID in Workplaces

Deploying tags in the workplace may increase privacy concerns for a number of reasons. One of them is the fact that the use of RFID is based on a non-balanced relationship, making it almost compulsory for employees to use RFID. Furthermore, even though an employee may not usually be located throughout the entire workplace, there is the possibility to trace them when passing readers (however only if specific personal data of the employee has been collected). The deployment of RFID in the workplace also means that certain indicators can be checked, i.e. levels of performance, time spent in the office or length of breaks.

Apart from the tracing of employees, the rest of the concerns already exist with current technologies (such as CCTV). In order to address the privacy concerns related to the use of RFID in the workplace, a number of options can be listed, such as the implication of Workers Councils in the implementation of technology (compulsory in Germany, for example), or the enactment of codes of conduct.

In this respect, the International Labour Organization is playing a major role in the introduction of RFID technology at work by carrying out extensive researches on the social, privacy and labour implications of the deployment of RFID. Although employees are covered (as any other person) by the extensive legal framework dealing with data protection, there are some scenarios where they might be exposed to further risks concerning their privacy more than the average citizen. In particular, the majority of cases show that the provision of personal data is somehow compulsory for the employees or even for a person to get to a job. It is considered as normal that, when working for someone, one has to give up some privacy (OPC 2008).

That is why guidelines such as “Protection of Workers’ Personal Data – An ILO code of practice” or the recommendation adopted by the Privacy Commissioner of Canada (“Radio Frequency Identification in the Workplace: Recommendation for Good Practices” of 2008) are so important in these cases. The latter document advocates “taking a proactive stance in the development and deployment of new technologies” so as to “enhance privacy by ensuring careful and appropriate design and deployment of the technologies in a manner that anticipates and respects privacy concerns”. The Privacy Commissioner of Canada is particularly concerned with the “secondary” uses that the deployment of RFID at workplaces might have, i.e. surreptitious surveillance of workers or tracking for purposes other than those accepted as “legitimate”. In order to assess the issues that might arise in the context of RFID-related privacy issues for employees, the document recommends conducting Privacy Impact Assessments (taking into ac-

count the concept of personal information and the reasonableness of personal data collection among others). The document establishes a number of good practices for employers when implementing RFID at work, such as having an accountable person within the organisation, identifying the purposes for implementation, guaranteeing the fair and informed consent of employees, limiting collection of personal data, as well as the use, the disclosure, the retention, and the updating of personal data.

As a corollary, it is important to point out that when implementing RFID technology at the workplace, employers should ensure that all labour regulations are being complied with, and proportionality applied at every level.

5.1.4 Conclusions

RFID is a technology that could place Europe in a very advantageous position if developed in the right way. It has many applications, ranging from healthcare to logistics, from public transport to libraries, which would make people's lives easier and improve efficiency in a number of industrial and service processes. Nevertheless, this potential could be harmed if potential privacy concerns raised by some RFID applications are not tackled with adequate tools. According to the OECD, "RFID technology is at a stage of development where privacy and security have been identified as challenges for its widespread adoption (...) RFID security and privacy should be an urgent priority for all stakeholders in order to prevent large scale opposition by consumers and individuals, and facilitate the successful roll-out of future RFID systems." (OECD 2008a)

RFID technology is, however, already covered, as any other technology, by the existing data protection legal framework. Given the current technological status and the current development of RFID applications, the application of the existing data protection rules adequately addresses privacy concerns which may be raised by some RFID applications.

Considering the large number of different RFID applications, the OECD recommends that firms who use RFID perform (before the implementation of the technology) a Privacy Impact Assessment in order to determine whether the concerned applications involve personal data or not (OECD, 2008a). The Privacy Impact Assessment should be based on the principle of reasonableness, i.e. it should assess the reasonable privacy risk linked with a RFID application provided that all adequate and reasonable technical security measures have been implemented.

On these grounds, the following conclusions can be stated:

Recommendation: The existing data protection legal framework is adequate for RFID technology applications

As any other technology, RFID shall comply with the Data Protection Directive and related legislation and with Member States' national data protection laws.

The privacy impact of RFID technology should be evaluated application by application. If RFID applications involve personal data, they are covered by the existing data protection legislation, guided by the principles of a) technology neutrality and b) informed consent of the individuals (OECD 2006). The current legal framework is considered as flexible enough to cope with further developments of RFID applications (Holznagel et al. 2006).

Moreover, a specific data protection and/or privacy regulation applicable only to RFID technology would hamper the development of RFID applications by the industry and especially by SMEs. This is particularly true, as item-level applications in open supply chains, that are at the core of the current privacy debate are, not in widespread use today, and would be in place only in a mid-term perspective (Strüker et al. 2008).

Recommendation: Enforcement of the current data protection legal framework is fundamental

Considering the legal requirements to comply with in order to address the privacy concerns raised by some RFID applications, the condition for securing the deployment of RFID applications in full respect of the right of privacy is to make sure that the existing data protection legislation is applied.

Continuous dialogue between the European Commission and the Member States should be encouraged in order to monitor the application of data protection legislation related to RFID applications and to avoid radical differences in the implementation among the 27 Member States. Such differences would hold back the development of EU-wide RFID applications.

In this respect, in principle, the future recommendation addressed to Member States regarding privacy and security related to RFID should adequately help to have a consistent enforcement and interpretation of the data protection principles within the EU.

Recommendation: Public information on RFID is crucial

In accordance with the rules governing data protection, when personal data is involved, complete information should be given to the individual in order to enable them to agree or not to have their personal data processed. The consent of the data subject constitutes the legal basis for processing personal data in the majority of cases. This consent should be unambiguous, freely given, specific and informed. Therefore, informing the consumer in a clear and understandable manner of the consequences of having an active RFID tag is an additional measure that can address most of the privacy concerns. In any case, it should be taken into

account that the need for information goes along with the question of whether the tag used in the given environment contains personal data or not.

If RFID is to be implemented on a broad scale, it needs to have the consumers' support, and that can only be achieved by informing them in a proper manner about the advantages and disadvantages of the technology, which is currently largely unknown by the public. Only complete information will allow the individual to understand the benefits of RFID technology and of its application in their day-to-day life, while also answering questions about the potential legitimate risks linked to their privacy.

In this respect, a European and/or nationally funded public campaign will be an efficient tool to familiarise the general public with the technology. Examples on how media coverage could be carried out can be found on TV or on the internet, with "EU Tube" hosting a complete video on the subject and web pages such as www.discoverrfid.org or www.rfidabc.de which aim at explaining how the technology works in an understandable and entertaining way. A differentiation between the diverse RFID applications and case-by-case information about their potential impact on privacy shall be provided to the general public.

Recommendation: The protection of personal data should be ensured without imposing unreasonable burdens upon the RFID users

According to the legal data protection rules, in addition to complete information to be given to the individual and to the implementation of all reasonable security measures, the data subjects must be enabled to give their consent for the processing of their personal data.

Taking into account of all the reasonable means likely to be used by the RFID user or by any other person to identify the individuals, the method applied by the RFID user to enable the data subject to agree or not with the processing of their personal data should be adequate and proportionate to the privacy risks involved but should enable freely given, specific and unambiguous consent.

The RFID user would be able to decide which method to apply for enabling the consent of the data subject by doing privacy and risk assessments prior the development of its RFID application.

If consistent public information is provided and all reasonable technical and organisational measures are applied to secure data, the "opt-out" method should be recognised as complying with all legal requirements, without hindering the development of the RFID technology.

In the field of RFID, consent from the data subject to specific RFID applications is often put in relation with deactivation of the tag. Two scenarios with regard to the granting of the data subject's consent can then be identified: "opt-in" (standard deactivation) and "opt-out" (deactivation on request).

In the retail sector for instance, privacy and risk impact assessments show that an “opt-out” policy would, on one hand, address the privacy concerns proportionally to the current risks foreseen and, on the other hand, allow the development of RFID applications, take into account of the technical and structural problems related to the deactivation of the tags by default and allow after-sale services enabled by the tags related, for instance, to recycling and anti-counterfeiting purposes.

In this respect, the future Recommendation of the European Commission regarding privacy and security related to RFID should give guidance to RFID users for applying the most adequate method for obtaining, when required, the consent of the data subject.

Recommendation: Technical measures should be used to ensure personal data security

Implementation of any RFID application should be done only after an adequate Risk and Privacy Impact Assessment according to applicable guidelines if any.

Technical and organisational measures can offer a wide range of solutions to address privacy concerns. Data security technologies (“Privacy by Design”) and Privacy Enhancing Technologies (PETs) give sound solutions to minimise the legitimate and reasonable privacy risks that a technology such as RFID might raise.

As there are, and will be, a multitude of technically different RFID applications adapted to the needs of the various economic sectors, the companies and sectors concerned should be allowed to develop and apply the adequate privacy by design and privacy enhancing technologies depending upon the legitimate and reasonable privacy risks related to the RFID application concerned.

Recommendation: Self-regulation and guidelines enacted by industry should be welcomed

In addition to the legal provisions and the technical solutions, comprehensive industry codes of conduct or guidelines shall be encouraged for spreading best practices in order to comply with data protection rules and mitigate reasonable privacy risks. Already today, there are industry guidelines indicating how to inform consumers about the use of RFID technology and about the choices available to deactivate the tags. To be efficient, self-regulation needs to be coherently enforced by the industry: while admitting that by their own nature they cannot be legally enforced, self-regulations and guidelines would make little sense if they were not respected by their addressees.

5.2 Health and Environmental Effects

5.2.1 Health Effects

The expected increase in the number of RFID tags leads to the need to evaluate whether or not the current European legislation on the protection of health pertaining to electromagnetic fields suffices for the new scenario that will be created in the following years by RFID. This section aims to briefly refer to the legislation applicable in the field of health and the consequences that it has for RFID.

The issue of electromagnetic fields and public health is not new. Since the first apparatus emitting electrical radiation was introduced, several studies have warned against the harmful effects that overexposure to radiation has on human beings, and public authorities have taken adequate legal measures to protect citizens (such as those taken on mobile phones for example). In 1999, the European Union adopted a Recommendation aiming to limit general exposure to electromagnetic fields [Council Recommendation on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) (1999/519/EC)]. This Recommendation sets up a number of restrictions and reference levels concerning the exposure to electromagnetic fields, with the purpose of ensuring a high level of protection for the general public. Furthermore, as certain workers are in daily contact with electrical and electromagnetic equipment, and are, therefore, more likely to suffer the consequences of their emissions, Directive 2004/40/EC on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) was adopted, so as to provide an adequate degree of protection at workplaces by establishing restrictions and requiring employers to take a number of measures.

In this regard, it can be considered that RFID falls within the scope of both legal texts, and that the potential effects on human health are, in consequence, covered by existing legislation. The real issue, however, will arise with the widespread development of RFID applications involving an increasing number of tags and readers.

To provide consumers with a comprehensive framework regarding health issues, they need to be reassured that RFID devices meet the requirements of all applicable EU legislation and that the applicable conformity assessment procedures have been applied. In order to give individuals confidence in RFID, the CE marking should, in principle, be used. CE stands for “Conformité Européenne” (European Conformity), and “symbolises the conformity of the product with the applicable Community requirements imposed on the manufacturer. The CE marking affixed to products is a declaration by the person responsible that the product conforms to all applicable Community provisions, and the appropriate conformity assessment procedures have been completed” (European Commission 2007).

However, using CE marking has proven to be difficult to apply when it comes to RFID. It does not seem feasible or helpful in this context, specifically due to the small size of the tags. Consequently, another solution may need to

be considered in order to inform citizens of the technical compliance of RFID systems and health legislation. From this analysis, the following recommendations can be made:

Recommendation: Monitor RFID developments to ensure compliance with EMF legal framework

As for all technologies using radio frequency, the current legal framework to protect citizens from over-exposure to electromagnetic radiation applies to RFID. The European Commission should continue to moderate a dialogue among relevant stakeholders to identify open points and engage in further legislation if deemed necessary.

Recommendation: Other means different from CE marking to inform and protect citizens should be enacted

In this respect, an independent body in charge of inspecting RFID chips might be useful, either at a European or global level.

Recommendation: Additional funds for technological research are welcome

The experience gained from first large live projects/applications of RFID is also an adequate method for addressing health concerns related to RFID.

5.2.2 Environmental Effects

As with any other technology, RFID raises a number of concerns related to its potential effects on the environment. The European Union has, however, enacted a consistent legal framework with the intention to cover all potentially harmful materials and avoid major effects on our natural surroundings. In this section we will analyse those laws and their application to RFID.

The most prominent issue with regard to environmental aspects of RFID usage is the question of recycling of transponders, products and packaging. With the widespread development of RFID applications, the components of RFID devices might cause significant problems to the environment when disposed of, since elements like silicon, nickel, copper or aluminium (all present in RFID devices) are contaminants for recyclers and manufacturers who use recycled material.

The European Union has adopted three fundamental legal texts to regulate environmental related matters of electrical and electronic equipment: Directive 2002/95/EC on the restriction of the use of certain hazardous substances in electrical and electronic equipment (so-called RoHS Directive), Directive 2002/96/EC on waste electrical and electronic equipment (so-called WEEE Directive) and Directive 94/62/EC on packaging and packaging waste. The objective of these directives is to restrict the use of certain components in the manufacturing of electronic and electrical equipment, as well as to improve the management of their disposal, trying to achieve a scheme as environmentally friendly as possible. Therefore, in principle, compliance with this legal framework ensures a high protection of the environment, and thus, all electrical and electronic equipment that are covered by the directives should not have limited effects on the natural surroundings.

It should then be established whether RFID falls into the scope of these directives. The wording of the WEEE Directive does not explicitly rule out that RFID chips could be seen as waste electrical and electronic equipment, but when the text was adopted, RFID had not yet reached its current stage of development. In the document “Frequently Asked Questions on Directive 2002/95/EC on the Restriction of the Use of certain Hazardous Substances in Electrical and Electronic Equipment (RoHS) and Directive 2002/96/EC on Waste Electrical and Electronic Equipment (WEEE)”, the European Commission established a balanced approach that makes application of the WEEE Directive dependent upon whether RFID tags are placed on the packaging or in the equipment itself. Hence, apparently RFID cannot be considered as electrical or electronic waste itself, but is rather linked to the product it is attached to. As it stands, many of the circumstances in which RFID tags will actually be deployed would result in them falling outside of the scope of the WEEE Directive. In this respect, the European Commission is currently conducting a review of both the WEEE and RoHS Directives. One of the purposes is to clarify the scope of the WEEE Directive, so as to determine the application to RFID by formalising the criteria used in the analysed FAQ document.

Thus, at the present moment, no major challenges regarding RFID and recycling exist; nevertheless, new problems may arise once the time of mass deployment will come (Gliesche et al. 2008). Therefore, it is recommended to ensure continuous assessment of the environmental impacts together with the development of the technology and to monitor this alongside the appropriate legal framework. In this respect, it is advisable to conduct an:

Recommendation: Assessment of the environmental impact of RFID

The European Commission and other stakeholders have established a coherent position on how to treat RFID under WEEE and RoHS Directives. Nevertheless, continuous monitoring of technology development is advisable to make sure that

once RFID has reached widespread item level use, the legal framework has been adapted if required. Therefore, the European Commission should support these monitoring activities carried out by academia and industry alike. Further discussion of the ongoing development of RFID technology could be required, and cooperation between industry and stakeholders would be useful in this respect (Gliesche et al. 2008). An early stage approach is considered as necessary. Examples such as the forthcoming study by the Institute for Future Studies and Technology Assessment in Berlin (commissioned by the German Federal Environment Agency) show how stakeholders (from industry to academia, from NGOs to government authorities) can join efforts in order to analyse the impact of RFID on the environment in the short- to medium-term. The study, entitled “Forecast of possible Impacts of RFID Mass Deployment on Consumer Goods for the Environment and Waste Disposal”, is intended to be published in 2008, and will be the result of a comprehensive research process, which should be then discussed at the European level.

Recommendation: Encourage research aiming at minimising environmental effects of RFID

Polymer technology could be used to produce tags without potentially harmful materials, such as copper or silicon, and energy-saving devices could be implemented.

5.3 Radio Spectrum

There is no doubt that technology plays a key role in the development of RFID. One of the essential features within the field of RFID is the availability of a harmonised frequency base throughout Europe. Although a number of instruments have been adopted in this respect, the evolving nature of the technology requires constant monitoring to ensure a coherent legal framework. This chapter aims to give a brief overview of the current European legal framework and the issues that radio spectrum might pose to RFID.

5.3.1 EC Legislation and other Policy Texts

The following table details the most prominent legislation within the field of radio spectrum:

Table 5.2 RFID-related EU radio spectrum legislation

Name	Description
Council Directive 87/372/EEC on the frequency bands to be reserved for the coordinated introduction of public pan-European cellular digital land-based mobile communications in the Community – to be repealed by Proposal COM/2007/0367 final – COD 2007/0126	Directive 87/372 required Member States to reserve a range of spectrum exclusively for GSM. Given the present situation, where a number of systems, such as RFID, have entered in operation it is necessary to repeal the directive and open those frequency bands to other devices.
Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) (OJ L 108, 24.4.2002)	This directive was enacted with the purpose of harmonising and simplifying the rules and conditions for authorisation, to facilitate the provision of electronic communication networks and services.
2002/622/EC: Commission Decision of 26 July 2002 establishing a Radio Spectrum Policy Group (OJ L 198, 27.7.2002, p. 49)	Sets up an advisory group on radio spectrum policy in order to support the Commission on radio spectrum issues.
Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision) – (OJ L 108, 24.4.2002, p. 1)	Aimed to set up a legal framework in order to manage the growing demand for frequencies, by trying to harmonise them and systematise their use.
Commission Decision of 23 November 2006 on harmonisation of the radio spectrum for radio frequency identification (RFID) devices operating in the ultra high frequency (UHF) band (OJ L 329, 25.11.2006, p. 64)	Requires Member States to make available (within the period of six months after the entry into force of the Decision) the frequency bands for Radio Frequency Identification Devices on non-exclusive, non-interference and non-protected bases.
Commission Decision of 16 May 2007 on harmonised availability of information regarding spectrum use within the Community (OJ L 129, 17.5.2007, p. 67)	Intended to harmonise the available information on the use of radio spectrum within the Community, through the unification of both the format and the content of such information and by using a common information point, called EFIS.

Name	Description
Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: A market-based approach to spectrum management in the European Union COM(2005)400	<p>As the digital dividend it is heavily fragmented, a European approach is necessary in order to fully reap the benefits from the switchover. Due to interference problems, standard digital broadcasting services and other communication services often cannot be operated in the same spectrum band. The Commission therefore suggests forming clusters of technologies using a similar type of communication network that can be clustered in closely related spectrum bands.</p>
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Reaping the full benefits of the digital dividend in Europe: A common approach to the use of the spectrum released by the digital switchover (COM(2007) 700 final)	<p>Establishes the basis for the efficient distribution of the expected freed spectrum to happen with the digital switchover, by the end of 2012. Relevant for RFID since it suggests the possibility of relocating frequencies in order to improve the current applications.</p>
European Parliament resolution: Towards a European policy on the radio spectrum 2006/2212(INI)	<p>Establishes the basis for the efficient distribution of the expected freed spectrum to happen with the digital switchover, by the end of 2012. Relevant for RFID since it suggests the possibility of relocating frequencies in order to improve the current applications.</p>

5.3.2 *Analysis*

Radio spectrum is defined as the entire spectrum of electromagnetic frequencies used for communications, with a rate of oscillation within the range of about 3 kHz to 300 GHz.

The availability of radio spectrum at adequate and affordable levels is a prerequisite for the generalisation of RFID. In Europe, there are two types of spectrum bands available to RFID. The first is exclusively reserved for it (limited number) and others are available on shared basis. At present, there are some problems concerning radio spectrum in the European Union, such as the lack of harmonisation and full availability of a “first generation” radio spectrum ranges. In addition, radio spectrum ranges are considerably smaller than the available frequency in non-EU countries, which hinders the technical development of RFID applications in the EU. In addition, there is a growing need for a pan-European program to tackle radio spectrum matters.

Although some important legal instruments have been recently adopted in order to address those issues, they are still far from the essential required organisation of the sharing of radio frequency. The Decision of 16 May 2007 which attempts to harmonise the availability of information on radio spectrum and the proposal for a directive repealing Council Directive 87/372/EEC, that intends to “free” frequency bands that are currently reserved for GSMs, might not suffice for shaping a consistent plan for the upcoming radio spectrum necessities.

With the switchover from analogue to digital communication services, additional radio spectrum will become available. This “digital dividend” is believed to offer a “public resource with an exceptional social, cultural, as well as economic potential” (Communication on a common approach to the use of the spectrum released by the digital switchover (COM(2007) 700 final). In the same document, the Commission has stated that a European approach on the switchover is needed.

Due to interference problems, standard digital broadcasting services and other communication services often cannot be operated in the same spectrum band.

The Commission therefore suggests forming clusters of technologies using a similar type of communication network that can be clustered in closely related spectrum bands. As the spectrum is fragmented, these clusters could only be formed following a common approach across the entire EU. More efficiency in spectrum management could also be achieved by establishing a common European spectrum plan.

Key requirements for the further implementation of RFID in Europe are a) the provision of suitable frequency bands and ranges and b) its efficient management. In 2005, the European Commission adopted a communication calling for a market-based approach in spectrum management. (COM(2005)400). It argued that the traditional approach in spectrum management of assigning individual spectrum rights and allocating the various bands to defined service categories “no longer seems appropriate for electronic communication services (...) Furthermore, technical development is making it less costly to enable devices to operate at various frequencies. The traditional model is not agile or responsive enough to enable society to reap the benefits of

these developments. This leads to missed opportunities in terms of competitiveness, industrial development and jobs, innovation and choice of services for citizens.”

Instead the European Commission suggested a market-based approach, planned to be established by 2010, to manage spectrum with more flexibility and efficiency. In order for the market-based mechanism to function properly, a substantial part of the spectrum should be put up for trading instead of a slow phasing in with one or several test bands. The new market based spectrum management scheme should follow the principles of technology and service neutrality.

For the European Commission, this market based approach could require further regulation in order to avoid unwanted effects such as monopoly pricing or a fragmentation into several non-useful slices of frequency spectrums.

Common to all proposals is a strong call for a better coordination of spectrum management at the community level – a position taken by the European Commission as part of its telecoms reform package in 2008.

Within this project an extensive list of the different frequency bands used for different RFID applications has been compiled (Walk et al. 2008). With regard to RFID, it has been criticised that the available spectrum for RFID in Europe is too narrow compared with other regions of the world, such as the United States of America or Japan, putting Europe at a competitive disadvantage. In addition, spectrum allocation is not consistent among the Member States.

In 2006, the Commission issued Commission Decision 2006/804/EC, according to which Member States should within six months of the publication of the decision, make available the 865–868 MHz UHF frequency sub-bands for RFID applications. It also establishes that manufacturers have to “ensure that RFID devices effectively use the radio frequency spectrum so as to avoid interference to other short-range devices” (Recital 3).

The decision has been a decisive step forward to create a level playing field for RFID applications across the Member States and begins to make up for some of the comparative disadvantages Europe has over the United States and other world regions. However, Member States have implemented this decision at different speeds, with France having been granted an exception of the decision, limiting the use of RFID application within certain distances around military installations (Commission Decision 2006/804/EC).

5.3.3 Conclusion

It is a fact that, in developed countries, there is virtually no “free” range of spectrum at the moment, although the expected digital switchover will free a wide amount. As afore mentioned, at the present time, it does not constitute a major problem for RFID, since the devices that are already working (UHF RFID) are adaptable to the existing frequencies. However, wider range of radio spectrum will be necessary to ensure massive development of RFID applications in Europe. Consequently, the following recommendation can be put forward:

Recommendation: Ensuring an appropriate radio spectrum framework

The European Commission should keep up its commitment to harmonise spectrum management and allocation across the Member States. Additional UHF spectrum should be rendered available. As RFID and other emerging technologies rely on the availability of radio spectrum, harmonised frequencies and easy application procedures are essential. As there is a strong need for harmonisation, in consequence, the efforts of the European Union should be focused on harmonising the existing technical requirements for the development of RFID, rather than creating new ones.

5.4 The Intellectual Property Rights Framework

5.4.1 Policy Approaches

The right to be granted a patent on technical innovations or a copyright on a certain work is essential to promote progress. The European Policy Outlook RFID, drafted under the German Council Presidency in 2007 states: “The patenting and licensing of innovative technologies is an everyday process, and it is one of the prerequisites for technological progress. Companies want to get a return on investment made in their R&D efforts” (BMWi 2007). However, the framework has to strike the right balance of security, flexibility and fairness for both inventors and users of RFID technology. The question to which extent industry standards should rely on patents has to be dealt with in responsible way, balancing the interests of technology developers and manufacturers as well as users and society as a whole.

The European Patent Regime

Although not directly EU legislation, the European Patent Convention is one cornerstone of the European patent regime. Signed in 1973, it aimed to harmonise European patent procedures and created the European Patent Office (EPO). The work of EPO reduces costs and makes up for some of the disadvantages compared to US companies that, with only one application at the United States Patent and Trademark Office (USPTO), can obtain protection for their IPR for a far greater market than any of the national European markets. The enforcement of the European patent is done before national courts, making it difficult and in a lot of cases expensive to effectively enforce patent rights. In addition, a patent might have to be translated into several national languages, therefore creating extra costs. It seems, however, that some issues regarding translation have been resolved, as the so called “London Agreement” will enter into force in 2008 that simplifies translation requirements for patents filed with the EPO.

Compared to the US (still the main competitor in the RFID field), the European patent regime poses advantages and disadvantages alike. The fact that there still exists no single community patent certainly puts European companies at a disadvantage. One advantage of the European patent system in comparison to the USPTO's proceedings is the first-to-file approach. To be granted a patent in Europe, it is essential to be the first to file a patent application. The patent office of Japan employs the same rule. The USPTO, on the other hand, follows a first-to-invent approach, meaning that before a patent is granted, the applicant and the USPTO have to verify in a lengthy and expensive process, whether the device has been invented somewhere else.

In another respect, the US system has a definite advantage for those who wish to be granted a patent in the area of computer software and computer implemented inventions (CII). The USPTO regularly grants patents for computer software, regardless of its function or impact. In the EPO context, software products are generally exempt from patentability, (Art. 52 (2) (c) EPC). Only if the software products in questions are "susceptible of industrial application", "new" and "involve an inventive step" (Art. 52 (1) EPC), they can be patented. Whether or not computer software can or should be patented at all has been discussed for several years. One of the main lines of arguments runs between open source proponents and those that see software patents as a way to gain revenue for innovations, especially for SME (European Commission, 2000a). Attempts by the European Commission to harmonise software patent law across Member States by a directive introduced in February of 2002 (2002/0047/COD) were halted in the European Parliament in 2005, following years of heated controversy both among software companies and open source proponents as well among the European institutions. Some refer to the TRIPS (Agreement on Trade-related Aspects of Intellectual property rights, including trade in counterfeit goods) agreement within the World Trade Organisation (WTO) which states that "patents shall be available for any inventions, whether products or processes, in all fields of technology, provided that they are new, involve an inventive step and are capable of industrial application" (Art. 27 (1) TRIPS).

The Community Patent

Initiatives for a single Community Patent date back as early as the 1970s, when in 1975 nine members of the European Economic Community signed the "Luxembourg Community Patent Convention" which never entered into force. A second attempt in 1989 also failed because not all thirteen signatory states ratified the agreement.

After publishing a Green Paper on European patent issues in 1997, in 2000 the European Commission undertook a new attempt when it proposed the creation of a Community Patent (European Commission 2000b). The proposal called for the establishment of a Community Patent granted by the EPO. Patents were to be enforced by a patent tribunal established within the European Court of Justice (ECJ). However, the proposal was turned down by the Competitiveness Council in 2004.

In 2006, the European Commission started a public consultation on the Community Patent. One of the findings was that “industry, as well as other interest groups, generally supports the Community Patent as a way of addressing problems of the patent system.” (European Commission 2006a). The same general opinion was voiced in a public hearing on July 12, 2006 (European Commission 2006b). Following the 2006 consultation, the European Commission issued a Communication on the European Patent System (COM(2007) 165) on April 3, 2007. The Communication highlights the correlation of patent activity and innovative power and calls for the creation of an internal market for patents. The Community Patent is still seen as the best overall approach, ending the current situation in which patent litigation in Europe is complicated and costly. According to a study cited in the communication (Van Pottelsberghe de la Potterie et. al. 2006), the cost for a patent application in Europe can easily be nine times higher than in Japan or the United States of America. As one of the latest developments, the Portuguese Presidency in 2007 stressed the importance of a quick solution to the patent issue as a prerequisite to fulfilling the goals of the Lisbon Strategy, and further actions in this respect have been announced by the Commission for 2008.

Related EU legal acts on Intellectual Property Rights

Directive 96/9/EC of the European Parliament and of the Council on the legal protection of databases

As RFID systems involve the creation of back-end databases, Directive 96/9/EC might in some cases also be relevant to gain legal certainty when implementing RFID. As a novel feature, the directive created a *sui generis* right for non-original databases (Art. 7 (1)). With this provision, it is intended to protect “the results of the financial and professional investment made in obtaining and collection of data and information”. The database rights do not compromise any copyright that applies to the items of the database contents (Art. 3 (2)) In the evaluation of the Database Directive, the European Commission concluded that the level of copyright protection for databases, especially for non-original databases now covered by the directives *sui generis* provisions, had increased, also in comparison to the United States of America, but that this had “no proven impact on the production of databases” in Europe (European Commission 2005).

Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs

With Directive 91/250/EEC, the Council aimed at creating a common level of copyright protection for computer programs in all Member States. According to Art. 1, the purpose of the directive is to “protect computer programs, by copyright, as literary works within the meaning of the Berne Convention of the Protection of Literary and Artistic Works” (Recitals). The Berne Convention of the Protection of Literary and Artistic Works was first signed in 1886. It is today administered by the World Intellectual Property Organisation which is part of the

United Nations. The TRIPS agreement also incorporates the terms of the Berne Convention. Art. 5 (2) of 91/250/EEC allows for the making of back-up copies, Art. 5 (3) gives software users the right to correct errors in the software product. Art. 6 also gives the possibility for reverse engineering of software to ensure interoperability with existing systems. In a report on the implementation and effects of 91/250/ECC, the Commission concluded that “the objectives of the Directive have been achieved and the effects on the software industry are satisfactory (demonstrated for example by industry growth and decrease in software piracy).”

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (EU Copyright Directive (EUCD) or Information Society Directive (Infosoc))

The major impact of the Infosoc directive was to harmonise Member States legislation to counter “circumvention of any technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective” (Art. 6 (1)). This directive has an indirect influence on RFID, as RFID can be one technical measure to improve copyright protection and counter fraud and piracy, such as counterfeit technical components or brand name products.

5.4.2 Industry approaches

RFID Patent Pool

If standards rely partly or wholly on patented technologies, competition might be at stake. However, as previously mentioned, patents are an important means to ensure innovation and creativity in the development of new technologies. Thus, a balance has to be found in order to assure that the interests of both innovators as well as manufacturers and users of standard technology solutions are met. One way to moderate the impact patents may have in that progress is to form a patent pool. Patent pools might create an environment for a fair and non-discriminating competition by providing access to key patents for all market players. Currently, the most prominent patent pool in the IT and communication industry is MPEG LA. MPEG LA is the MPEG Licensing Administration that serves as a patent pool for the MPEG-2 standard. MPEG-2 is required for the production of DVDs. Currently MPEG LA is also preparing licensing programs for the evolving standards HD DVD and Blue-Ray Disc as well as for Digital Rights Management applications. Patent pools are a means to facilitate an easy licensing of patents as companies wishing to manufacture products or offer services for which patented technologies are needed only have to turn to one institution to receive a license for all patents needed to make a certain standard work.

In the RFID industry, “The RFID Consortium” was formed in the United States in 2005. It is largely modelled after the MPEG LA example. The following US companies have finally signed the contract: Alien Technology Corporation, Applied Wireless Identification Group, Inc. (“AWID”), Avery Dennison Corporation, Moore Wallace, an RR Donnelley Company, Symbol Technologies, Inc., ThingMagic, Inc., Tyco Fire & Security, and Zebra Technologies Corporation.

In 2006, the RFID Consortium issued a call for patents, inviting companies to identify patents they have been granted that are necessary for the practice of UHF RFID standards covered by EPCglobal Class Gen1 and Gen2 as well as ISO/IEC 18000-Part 6. As stated on its website, “all patents essential to the practice of the UHF RFID standards owned by participants in the licensing arrangement will be made available to interested companies via a single license on fair, reasonable and non-discriminatory terms.” In November 2007, RFID Consortium LLC was established to facilitate RFID patent licensing following an obviously successful patent call the year before. The partners also include companies from Europe and Asia. Partners of RFID Consortium LLC are 3M Innovative Properties Co., France Telecom, Hewlett-Packard, LG Electronics, Motorola, ThingMagic, Inc., and Zebra Technologies. The program will be administered by Via Licensing, a subsidiary of Dolby Laboratories, Inc. In December 2007, RFID Consortium LLC submitted its business plan to the United States Department of Justice for a review of the legal and licensing requirements. This review also includes the list of essential patents that will be within the initial patent portfolio.

EPCglobal IPR policy

Another solution to the essential patents issue has been proposed by EPCglobal: companies wishing to participate in any of the Working Groups set up by EPC global in order to develop technical specifications for the development of RFID technology are asked to sign an IP Policy by which they engage themselves in offering the necessary patent claims royalty-free to the greatest extent. Necessary in this context means that “it is not possible to avoid infringement because there is no non-infringing alternative for implementing the Specification” (EPC global 2007). In its Intellectual Property Policy Working Group Declaration, EPCglobal states the purpose of the declaration is to “facilitate the adoption of such a set of Specifications while avoiding uncertainty to the extent possible regarding intellectual property claims in the Specifications. EPCglobal seeks to encourage the development, exploitation and competition of proprietary technology and innovative approaches to implementing such specifications, while avoiding blocking proprietary claims or monopolization of use of the Specifications”. (EPCglobal 2003)

Section 3.1 of the EPCglobal Intellectual Property Policy Working Group Declaration states that those who sign it “shall grant to the extent that it owns or has a right to grant, a non-exclusive, non-transferable, non-sub licensable, worldwide royalty-free and otherwise reasonable and non-discriminatory licence” to other EPCglobal partners. With limiting its IP policy to necessary claims, EPCglobal

hopes to encourage parties to “develop and benefit from exploiting proprietary implementations and improved systems and methods which utilise EPCglobal specifications”. EPCglobal then go on to say that they “... encourage the development and use of intellectual property which is built upon a common set of interoperable standards.” (EPCglobal 2007)

5.4.3 Open Source Approach: OpenPCD

Alongside industry-driven patent pools and royalty-free or RAND licensing schemes, the first open source solutions for RFID applications are beginning to enter the public discussion. One of the most prominent examples is OpenPCD, offering a “free hardware design for Proximity Coupling Devices (PCD) based on 13,56 MHz communication.” (<http://www.openpcd.org/>). The overall goal is to provide people with technology helping them to detect and read RFID tags embedded in ePassports or other smart cards, following a mainly critical attitude towards RFID technology. The device is able to read cards supporting the ISO 14443, ISO 15693 and Mifare Classic standards. The hardware design has been released under a Creative Commons Attribution Share-Alike license, the necessary software under the name of “librfid” is released under GNU/General Public Licence (GPL). In February 2008, a version 0.2.0 of “librfid” was made public. The OpenPCD project originated among members of the Chaos Computer Club in Berlin, Germany. It aims at reading cards using the MRTD (Machine Readable Travel Document) standard issued by the International Civil Aviation Organisation (ICAO). After free software (“librfid” and “openMRTD”) had been developed, a free hardware design was to follow – a process that has led to the OpenPCD specifications.

5.4.4 Conclusions

Patents are a normal feature in everyday business relations, and as such have positive and negative effects on technology development. A balance has to be struck in order to make patents a motor of innovation rather than a roadblock. It is also important to address the different aims of standards on the one hand and patents on the other, with standards being introduced to facilitate greater interoperability of systems across countries or industry sectors, and patents being granted to protect intellectual property rights for innovative inventions. Both are needed in order to spur further technological development and economic growth in Europe. If standards involve the use of patented technologies, then ways should be found so that the use of the standard will be possible for all those wishing to use the technology. Some methods of how this could be achieved (e.g. by patent pools) have been addressed in this section.

European companies are beginning to take an increasingly important role in industry initiatives, with Germany for instance being home to the second largest number of EPCglobal members after the USA, and with European and Asian companies now part of the RFID Consortium patent pool. The legal framework within Europe seems to be sufficient in order to promote further RFID technology development. Within the European Patent Convention, the implementation of the London Protocol as from May 2008 should make patent applications in Europe cheaper and less complicated. However, still a major impact can be expected from launching a genuine Community Patent. The latest initiatives in this respect will hopefully prove to be successful after decades of debate (Verheugen 2007). Therefore, it is recommended to:

Recommendation: Work towards a community patent

Continue collective political efforts to come closer to establishing a community patent for Europe, and take into account policy options for improving the current European patent systems (see also ETAG 2007).

Recommendation: Encourage European participation in patent pools

It is recommended to encourage and maintain European participation in patent pools and with standardisation initiatives and bodies, and also to establish regular consultations with US and Asian representatives.

Recommendation: Follow an international approach with regards to IPR

European Union should follow adopt an harmonized approach at the international level, using its weight of 27 Member States within the WTO (World Trade Organisation) and the WIPO (World Intellectual Property Organisation) to facilitate common IPR rules across the globe, as RFID even more so than other technologies, can only become successful on a global scale once the Internet of Things has become a reality.

Recommendation: Encourage an open approach to IPR

Encourage a lively and innovative IT sector by allowing for different approaches in how to manage IPR, from open source to patent pools to other industry agreements. Using RFID technology according to internationally accepted standards should be possible for as many users as possible at fair and reasonable costs.

Recommendation: Continue the discussion on IPR and standards

Support Platforms such as the Global Interoperability Forum for Standards (GRIFS) launched under the 7th Framework Programme to foster dialogue with all stakeholders on patent, IPR and standardisation issues.

5.5 RFID Governance

As the Internet of Things (i.e. a global network of objects and corresponding information, that needs to be accessed anytime anywhere across the world, which falls outside the core of the scope of this study) is still a vision, a reliable estimate of the future scope of applications and the need for exchange between different industry branches is difficult to evaluate. From today's perspective, retail and goods manufacturers as well as logistics providers (corresponding to application fields Logistical Tracking & Tracing and Production, Monitoring and Maintenance in the RFID Reference Model) are likely to be among the main branches with the need to employ systems and standards that have to be accessed by large numbers of entities around the globe.

Other issues arise when novel applications come into focus. As every individual can have their own private website and use the internet to exchange data and information with other users, one day people might also want to exchange data and information with objects. This issue raises new questions, for instance regarding the storage of data of tagged personal objects in central or decentralised databases.

5.5.1 *Observation of Current Debate on Internet Governance*

The Working Group of Internet Governance (WGIG) within the World Summit of the Information Society (WSIS) held in 2003 in Geneva and in 2005 in Tunis has comprised a definition of internet governance, stating that "internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision making-procedures, and programmes that shape the evolution and the use of the Internet. It should be made clear however, that internet governance includes more than internet names and addresses, issues dealt with by the Internet Corporation for Assigned Names and Numbers (ICANN): it also includes other significant public policy issues, such as critical internet resources, the security and safety of the internet, and developmental aspects and issues pertaining to the use of the internet" (WGIG 2005). Members of the WGIG include international representatives from research, government, industry and civil society.

In its deliberations, the WGIG has identified several policy issues that should be addressed regarding internet governance. Among these are the unilateral control of the United States over the root zone file and system administration and the lack of formal relationships of government authorities with root server operators.

Further on, the WGIG suggests a division of roles and responsibilities amongst the three stakeholder groups, i.e., governments, private sector and civil society, that they should fulfil in the debate surrounding a future Internet governance model. According to the WGIG, *governments* should create an environment that favours ICT development, should develop, if applicable, laws, regulations and standards, should foster the exchange of best practices and engage in oversight functions. The *private sector* should promote industry self-regulation and the exchange of best practices, should develop policy proposals, guidelines and tools for policymakers and participate in national law making and foster innovation through its own research and development. *Civil society* should mobilise and engage in democratic and policy processes, engage in network building and bring in other views, e.g. grass-roots initiatives in order to facilitate a bottom-up, people-centred process. As a proposal for action, the WGIG concludes that “no single government should have a pre-eminent role in relation to international internet governance” and that all relevant stakeholders should be involved in a multilateral, democratic and transparent way. This call for an enhanced cooperation has also been stressed by the European Commission (European Commission 2006).

The current criticism is focusing on the role of the United States of America within internet governance. ICANN (the Internet Corporation for Assigned Names and Numbers) is currently overseen by the US National Telecommunications and Information Administration (NTIA). ICANN was originally formed to facilitate the transition of control over the internet’s Domain Name System (DNS) from the US government to the global internet community. However, the US government’s oversight over ICANN might soon come to an end. In its response to the midterm review of the Joint Project Agreement (JPA) with the US Department of Commerce, ICANN stated that the “JPA is no longer necessary” and leads to “a misperception that the DNS is managed and overseen on a daily basis by the US government” (ICANN 2008). Other governments are currently included by way of the ICANN Governmental Advisory Committee (GAC). The European Commission has acknowledged the positive role ICANN plays in internet management.

The role of the US government in DNS administration has been at the centre of numerous discussions. As a result of the aforementioned WSIS in Tunis and Geneva, the Internet Governance Forum (IGF) has been established as a global forum for discussions about alternatives in internet governance. In a resolution debated in January 2008, the European Parliament stressed the importance of the IGF as an international forum for the exchange on internet governance issues ensuring a democratic, transparent and multi-stakeholder dialogue (European Parliament 2008). In the parliamentary debate, suggestions were made for topics to be discussed at the next Internet Governance Forum meetings. These included broadening the internet governance debate to include issues such as the Internet of Things and the necessary frameworks for global RFID applications. However, the latest

proposals for the New Delhi agenda do not explicitly mention RFID, but contain, however, several topics under which RFID-related aspects could be discussed (Internet Governance Forum 2008).

The other main point of criticism focuses on the role of the US-based company VeriSign as the main facilitator of the Internet Domain Name System and the administration of top-level domain names. Fears arise that the influence of one company might hinder Internet development as single economic interests might outweigh broader goals for an open internet environment.

5.5.2 Legal Framework and Approaches to RFID Governance

By its very nature, the internet has evolved over several years and has largely operated without a given legal framework. All over the world, lawmakers have closely followed the development of the internet in the past years and the importance it now plays in the everyday life of billions of people. Legislation has been passed in countries all over the world as well as within the European Union to ensure that the use of the internet does not conflict with national laws or international rights and conforms to norms and values predominant in the world's societies. Among the challenges tackled are, for instance, unwanted e-mails (spam), digital property rights in the internet age, restriction of certain internet content (e.g. child pornography) or enhanced consumer protection in online business transactions. However, the core of the internet, its governance structure, has not been subject to legislation, but to other forms of agreement (cf. for instance the Joint Project Agreement between the NTIA and ICANN). The same will be true for the Internet of Things. As it is still largely a vision with only some facets visible today, it has not yet been the subject of legislation, but rather of science and academia.

Current frameworks or models for RFID governance should not be mistaken to forestall Internet of Things governance models, but they might give a hint in which direction future discussions might lead. The most prominent example for a governance framework for RFID is EPCglobal. The EPC is a unique number identifier developed as a RFID data standard, mainly in retail environments. In 2003, EPCglobal was created as part of the GS1 organisation, ensuring a smooth transition from current barcode technologies and standards to future RFID application. EPCglobal is a membership-fee based non-profit organisation that, according to its own statement, is committed to open and royalty-free standards.

EPCglobal is the most prominent operator of an Object Name Service (ONS) – similar to the DNS used in the conventional internet. The ONS serves as a directory of EPC manager numbers and would be used by companies who would want to establish data with another company with whom it does not have an established relationship. It serves as a lookup service, providing a pointer to the information services provided by the manufacturer of the object. As an output the ONS produces a URL like known from the conventional internet. The URL then leads to an Electronic Product Code Information Service (EPCIS) repository that contains

information on an individual Electronic Product Code. EPCIS would be implemented on manufacturer or company level. The standards for the EPCIS are still pending. The EPCglobal ONS is hosted by VeriSign – the US company mentioned above that also plays an important role in the internet's DNS. According to EPC global Inc. President Chris Adcock, there can be more than one ONS as long as they are interoperable (Adcock 2007).

EPCglobal is governed by a Board of Governors, in which different industry sectors are represented by global corporations from Europe, North America as well as Japan and China. For public sector applications, the United States Department of Defence (DoD) is represented. This has evoked criticism as some stakeholders fear a strong influence by the US Government on EPCglobal. This issue has been the topic of several debates in Europe. In his speech at the Lisbon conference "On RFID: Next Steps towards the Internet of Things", Bernard Benhamou, Professor at the Institut d'Etudes Politiques (Institute of Political Studies) in Paris, strongly warned against, for instance, repeating decisions made in the early days of the internet, which have led to the current criticism regarding internet governance. Instead, Benhamou called for the inclusion of all relevant stakeholders across all world regions. He said that different options for different countries and regions were necessary. Calls have also been voiced for more participation of different societal groups in the governance model of the Internet of Things – a position also summarised in the Commission Communication on steps towards a RFID policy framework (Communication on RFID in Europe: Steps Towards a Policy Framework, COM(2007) 96). The Communication gives reference to the Consultation process on RFID launched by the European Commission in 2006 in which 86 % of the respondents stated that the "system for registering and naming of identities in the future "Internet of Things" should be interoperable, open and non-discriminatory. [...] It should not fall into the hands of particular interests that could use these databases and naming systems for their own ends, whether they relate to commercial, security or political aspects of governance". In addition, questions have been raised on the Security of the Object Name Service as suggested by EPCglobal (Fabian et al.).

Besides EPCglobal, other providers have begun to offer ONS services. Afilias, global provider of internet domain name registry services headquartered in Dublin, Ireland, has offered the Afilias Discovery Services (ADS) which is free of charge and compatible to EPCglobal standards. The ADS is based on the open Extensible Supply Chain Discovery Service (ESDS) protocol and ensures operability to other supply chain systems and business applications. The ADS is a first sign of an evolving market in the field of RFID governance that might lead to a fruitful competition of global information services (BRIDGE 2007). Most recently, GS1 France announced that it was planning the "nationwide implementation of the ONS root of the EPCglobal network architecture" in France, a project to become operational in spring of 2008 (GS1 France 2007). The ONS will be administered by Orange Business Services, a French company. In January 2008, first meetings took place by the EPC Network Committee that will bring together solution providers and network users to discuss the further evolvement of the French ONS

(GS1 France 2008). The French attempts could then lead to the development of an open governance mode. “Subsequently, this open governance model can be extended to incorporate various ONS systems from other parts of the world, both on technical and business aspects that would be administrated under a common set of rules. Drawing on the GS1 France project to initiate an ONS root in a European context”, specific rules, naming standards, or security tools should be discussed and developed (Pauvre 2008).

The further development of RFID and subsequently the Internet of Things will most likely not be one mainly driven by legislation within the EU or other parts of the world, but rather an issue for a continued dialogue in appropriate forums and organisations. The planned discussions at the Internet Governance Forum in 2008 might be quite conclusive to get ahead in this important debate.

5.5.3 *Conclusions*

According to the Commission’s Communication on “RFID in Europe: Steps Towards a Policy Framework” (COM(2007) 96), there are concerns about the openness and neutrality of the databases that will register the unique identifiers that lie at the heart of the RFID system, the storage and handling of the collected data, including its use by third parties. Hence, the issue of eGovernance is also perceived as a complex one: if the so-called Internet of Things is to be successfully accomplished, the data storage systems should be ethically and securely managed and the processes should remain interoperable and non-discriminatory.

As the Internet of Things is still a future vision, all stakeholders should take their time to discuss all issues properly and unbiased on the European as well as the international level. eGovernance structures should indeed be discussed in a broad scope. As a consequence of a fear of repeating decisions made when developing the internet, arguments have been brought forward to not have a centralised structure, but rather a decentralised one, also under the control of other countries or entities outside the US. The discussions should be open for all ideas and requirements. This means that the questions of how to store the data of a tagged item, how to provide the link between the item and the respective data, and how to manage the access to this data should be elaborated recognising legitimate demands for both open environments for ICT and internet development and companies’ economic interest in developing new business models. The European Commission therefore should:

Recommendation: Keep a close dialogue with all relevant stakeholders

This dialogue should include all relevant stakeholders from industry, government, civil society and academia alike, as for instance represented in the RFID

Expert Group and the High Level Group on internet governance in order to foster an open, transparent multi-stakeholder dialogue ensuring interoperability, etc., and use international forums such as the Internet Governance Forum to discuss these issues and foster transatlantic dialogue with the United States on these topics. Take opportunities for exchange and proactively approach institutions such as EPCglobal to make sure that European interests are duly recognised.

Recommendation: Encourage further scientific research in the field of RFID governance

Encourage further scientific research in this field, e.g. within the 7th Framework Programme. This research could focus on developing a decentralised structure of the EPCglobal Network with global governance participation as suggested in the European Policy Outlook RFID, which was finalised during the German EU-Presidency in June 2007, and could determine whether the EPCglobal model can serve as a pre-test for future Internet of Things structures.

<http://www.springer.com/978-3-540-71018-9>

The RFID Roadmap: The Next Steps for Europe

Wolfram, G.; Gampl, B.; Gabriel, P. (Eds.)

2008, XXIII, 201 p., Hardcover

ISBN: 978-3-540-71018-9