COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 12.5.2009
SEC (2009) 585

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying document to the

Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification

"RFID Privacy, Data Protection and Security Recommendation"

{C(2009) 3200 final}
{SEC(2009) 586}

TABLE OF CONTENTS

1. PROCEDURAL ISSUES AND PUBLIC CONSULTATION

1.1. Background

Since 2003 the Commission has played an active role in shaping the discussion around Radio Frequency Identification (RFID), both in research and consultation of stakeholders. In 2005 the Commission established an RFID Reflection Group to synchronise the RFID related activities of various DGs and to identify the need for Commission intervention, which was transformed into an Inter-service Coordination Group on RFID later that year. Today a total of fourteen DGs are represented in the Group's activities, including the following ones: INFSO, TREN, MARKT, JLS, JRC, SANCO, ENTR, TAXUD, EMPL, RELEX, RTD, EAC, SG, and COMP. The group convenes at meetings held on a monthly basis, at which open discussions on current topics of interest are held and compromise is sought. This Impact Assessment has been carried out with reference to the INFSO Agenda planning under the number 2007/INFSO/048.

At the CeBIT in March 2006 Commissioner Viviane Reding announced the launch of a wide public consultation on the policy issues and public concerns raised by the deployment of RFID technology and its applications. The need for an active role from the Commission was confirmed by the extensive stakeholder consultation on RFID that was performed in the second half of 2006[1]. Different thematic workshops were organised (including a workshop on RFID security, data protection and privacy, health and safety issues) and from July-September 2006 a public online consultation was put forward on “Your voice in Europe”.

This public consultation resulted in a Commission's Communication on “Radio Frequency Identification in Europe: steps towards a policy framework” that was adopted in March 2007. The Communication explicitly addressed the need for a legal and policy framework to protect privacy and security to make the technology acceptable to consumers and citizens. It foresaw possible steps both in the field of specification and adoption of design criteria and drawing up specific codes of conducts on the use of RFID technology (complementary to or in explanation of Directive 95/46/EC). To this end the Communication set out an intention to publish a Recommendation to Member States to set out the principles that public authorities should apply in respect of RFID usage. The Recommendation was at that time designed to provide a timely and appropriate answer to the serious concerns expressed by stakeholders, in particular ‘interested citizens’, in the public consultation of July-September 2006. In parallel, an RFID Expert Group was set up in June 2007 to advise the Commission on different issues related with the deployment of RFID. In 2007 the Group focused its discussions on privacy, data protection and security issues carried out at its monthly meetings. The Expert Group is composed of a balanced mix of various representatives of European RFID industry, civil society groups, standardisation bodies, as well as representatives of national and European data protection supervisory bodies. The Commission did not exclude a priori to take “other possible measures” on the basis of the input received from the RFID Expert Group, as well as the Article 29 Data Protection Working Party and other relevant initiatives. Indeed, during the period when the RFID Expert Group met to discuss the Recommendation, i.e. between June 2007 and January 2008, the idea of introducing a new specific legislation was also debated.

[1] See SEC(2007)312 "Results of the public online consultation on future radio frequency identification technology policy".

On February 21 2008 the Commission launched a public consultation on a draft Recommendation on privacy and security aspects in applications supported by RFID. Respondents to this online consultation which took place on "Your voice in Europa" website, were asked to provide their views and opinions on the draft text of the Recommendation which formed part of the consultation package. The consultation was opened for 9 weeks and ended on 25 April. The online questionnaire was answered by 637 respondents, 37% of which were interested citizens and the rest were various organisations from the private and public sectors involved in RFID. The feedback received totals up to 1000 pages printed in the A4 format. Topics that were commented most by the respondents concerned provisions on the retail settings, privacy impact assessments, and awareness raising.

1.2. Scope of the impact assessment

This Impact Assessment focuses on privacy, data protection and information security issues in applications supported by RFID. It does not cover the following policy activities that could be related to the deployment of RFID:

- Activities which fall outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on the European Union and in any case to processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law.

- RFID and radio spectrum policy, as this is a separate policy area with its own policy options. Given the scope and importance, assessment of the impacts of those options would require a specific dedicated Impact Assessment for the policy options for the spectrum policy related to RFID.

- Impact of RFID and Electromagnetic fields on health, as it was decided that Research and Technological Development are the best suited instruments to deal with the questions rising from possible health issues. The 7th Framework Programme for RTD is the Commission's main instruments to tackle these questions.

- Ethical issues that can result from the use of RFID tags, such as RFID implants.

1.3. Opinion of the impact assessment board (IAB)

This Impact Assessment Board has been consulted and formulated recommendations for improvements in its opinion of 8 September 2008: "The report should clarify to what extend the planned recommendation will interpret Community legislation already in place, and explain the use of a Recommendation rather than another form of guidance document; state whether the proposed flexibility in the application of the opt-in principle is in conformity with the opinion of the European Data Protection Supervisor; quantify the administrative burdens; and ensure a balanced presentation of the overall impact of RFID on society. The report also needs to be substantially shortened."

The recommendation is an interpretation of the current legal framework, more specifically, the Data Protection Directive 95/46/EC documented in section 2.2.4, the opinion of the European Data Protection Supervisor documented in section 2.2.5 and other relevant legislation and regulation referenced in section 2.2.6. Chapter 4 documents and explains why the recommendation is the most suitable instrument to achieve the objective. The chapter highlights that the wide public debate revealed a priority question from the citizen and those that want the deploy RFID applications for clear legal guidance. The citizen was mostly concerned that without legal protection his privacy and security would be at stake and those planning to invest in RFID application were hesitating because it was unpredictable if their applications would be compatible with future legislation. Moreover, data protection authorities have been considering to introduce local legislation if Europe would stay absent. The European Data Protection Supervisor analyses in detail the different legislative options in its opinion on RFID (2008/C 101/01) and concludes in paragraph 70 that a recommendation could force the proper implementation of the existing legal framework . If this would fail, the EDPS suggests to adopt a lex specialis vis-à-vis the general data protection framework. This last assessment will be made at the scheduled review of the recommendation 3 years after its publication in the Official Journal.

The recommendation adopts some flexibility in the application of the opt-in principle. This flexibility has been documented extensively in section 5.4. "content options related to the retail sector". Section 5.4.4. addresses the opinion of the EDPS. This opinion suggests a flexible approach to cope with the growing diversity of RFID applications and to facilitate the development of new business models and services. The EDPS was consulted several times during the preparation of the recommendation and it has largely accepted the flexible application of the opt-in principle proposed in the recommendation.

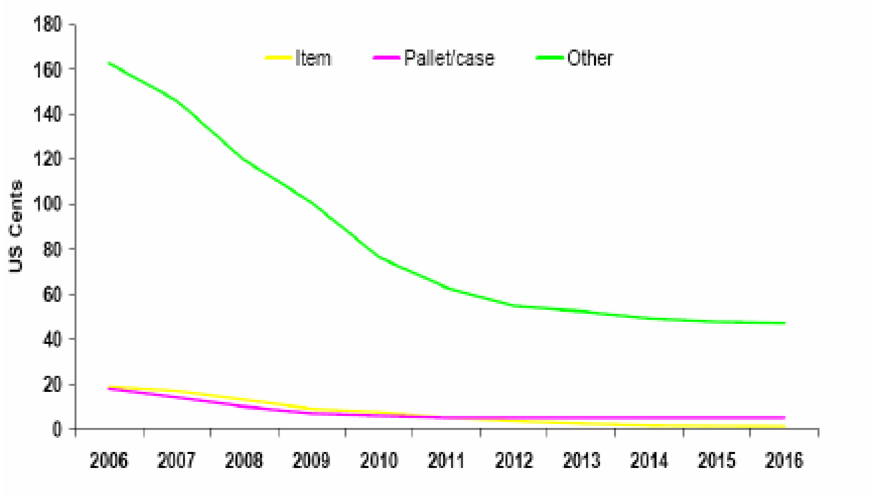
As suggested by the IAB, impacts of the recommendation have been clearly separated from the general impacts of RFID as technology. Section 5.5 and Annex 4 have been reworked and complemented in order to provide a more balanced assessment of RFID impacts, in particular as regards impact on employment.

2. PROBLEM DEFINITION

2.1. Introduction

Radio Frequency Identification (RFID) is the designation for a microchip technology that uses radio signals to automatically identify objects, such as goods, vehicles, animals and people. The basic components of an RFID system are a tag (a transponder), which is attached to an object, a reader (sometimes called an interrogator) which is able to retrieve data from the tag and middleware to link RFID data with the ICT infrastructure and application tools of the company using RFID. Besides retrieving data, it is also possible in some specific RFID systems to modify the information on the tag (write to it) using the reader. The tag and the RFID receiver communicate with each other via a radio link. Annex 1 presents more characteristics of RFID technology.

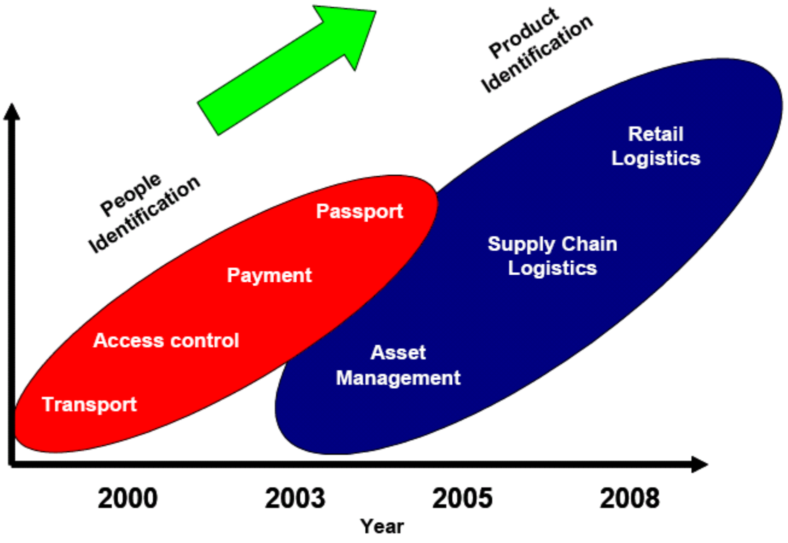
Figure 2.1. Expected average price tag per application (2006-2016)



Source: IDTechEx

RFID technology itself is not new, however advancing technology developments (e.g., miniaturisation) and costs reductions have led to an increased uptake by the market over the last decades and to a situation in which we stand at the verge of large scale introduction of RFID. At present the price for the cheapest tags hovers around 0.14-0.18 EUR[2] per tag. Further cost reductions are foreseen with tag prices expected to drop to 0.04 EUR within a few years (see Figure 2.1).

Figure 2.2. Market and application perspectives for use of RFID



Source: JRC, 2007.

In general, tags can be attached to individual items (e.g., products in a retail store, access cards), or can be used to identify packages or containers which include multiple individual items. In this sense, most of current RFID applications use tags at a container or palette level (see Figure 2.2). Further tag price decrease is expected to drive a massive introduction of item level tagging in the supply chain and thereby boost the market. This is expected to precede the introduction in other sectors, such as healthcare, ticketing services, etc.

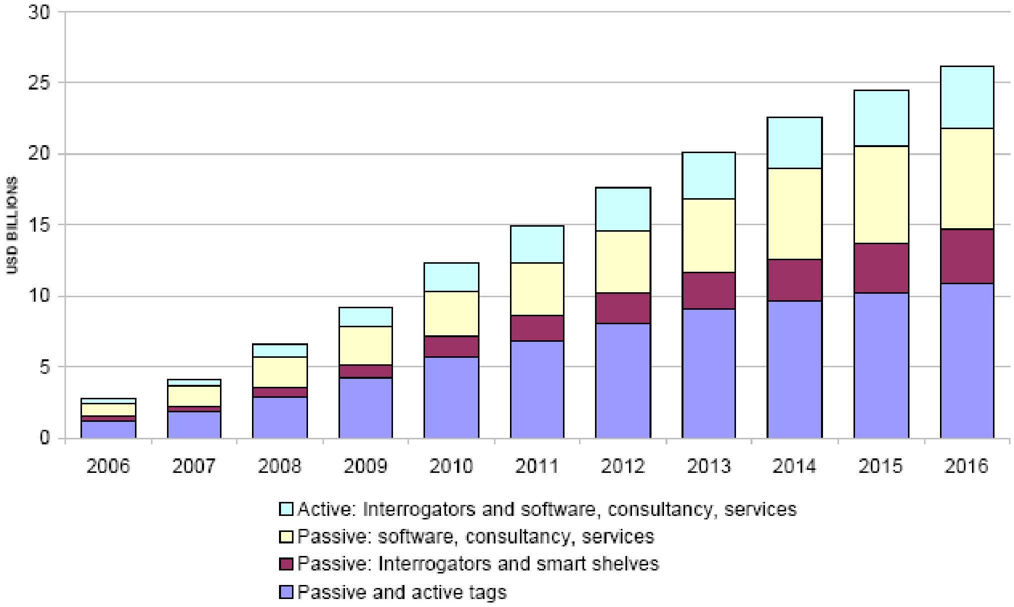
[2] Exchange rate: 1 USD =0.70 EUR.

The overall market for RFID is estimated to grow from €1.75 billion to €8.4 billion in 2010[3] worldwide, further increasing to over €17.5 billion in 2016 (see Figure 2.3). About half of the market is accounted for by the market for tags.

Nowadays the largest geographical market for RFID is found in the US. The size of the European market is about half as large[4].

Market growth and deployment of RFID also correlates with employment that can be found in RFID. At present, North America is the world's leading region in terms of RFID employment, with Europe coming third after Asia (see figure 2.4)[5]. However, it is likely that Asian countries will adopt RFID technology faster (49% share) and that Europe's share in the global RFID workforce will decrease to 16%.

Figure 2.3. Total RFID Market forecast 2006-2016



Source: IDTechEx

Given the relatively big application potential of RFID, the market for RFID is expected to become a highly significant market in the coming decades. For Europe alone, the number of passive tags sold in 2012 is forecasted to be 21 times higher than the number of tags sold in 2007. By 2022 the market volume of this type of tags is expected to increase 600-fold.

At present, RFID cards account to most of the business turnover. For example in 2007, China supplied a peak number of RFID cards for their national scheme[6]. Consequently, Chinese companies are expected to take the leading position on the worldwide market. With regards to other components of the RFID application, the position of the US is dominant with Europe in the second place (58% USA versus 33% Europe).

[3] Frost & Sullivan (2004), IDTechEx (2006).

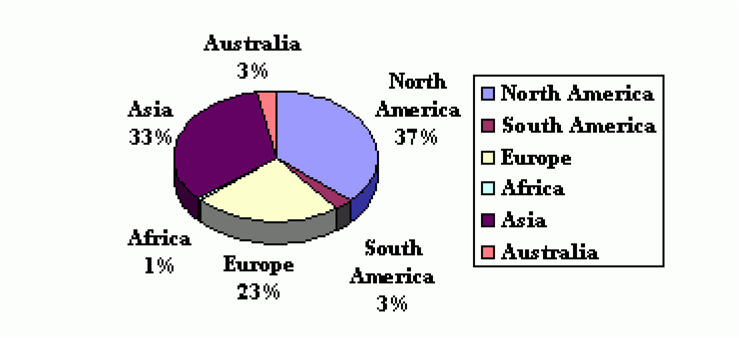
[4] IDTechEx 2005.

[5] Source: The RFID Tribe (2006), The RFID Workforce Report 2006.

[6] China has issued the world's largest order for RFID - a $6 billion order for a national ID card scheme. These are contactless cards, operating at HF. By the end of 2005, China had issued 110 million national ID cards. The target is to issue 900 million ID cards by the end of 2008.

Today, EU manufacturers of RFID tags and consulting services hold a reasonably strong position in the market. The competitive position in the markets for components, developers and resellers, system integrators and RFID software providers, however, is quite weak[7]. In the field of research and development Europe is seen as one of the leading regions in the world, although it should be noted that the number of RFID patents which are allocated to European companies is limited[8]. Also the rate of growth in the market of RFID systems appears to lag behind.[9]

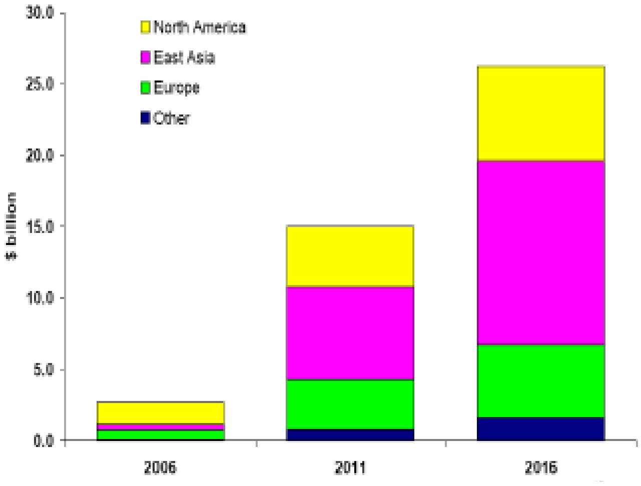
Figure 2.4. RFID Workforce 2006



Source: RFID Tribe (2006)

Given the predicted size of the market, it is important that Europe tries to strengthen its position on this market. Regulatory uncertainty and higher costs of deployment in Europe can make the competitive position of Europe weaker.

Figure 2.5. Total spend on RFID systems, service and tags by region



Source: IDTechEx

[7] JRC 2007.

[8] According to a study made by RFID Journal in 2005 some 150 patents were judged to be relevant to RFID. Almost all of them are rewarded to US companies, with the top 3 companies having a share of 43% of all 150 patents (i.e. Intermec, Checkpoint, Motorola). Reference to this study is made in JRC (2007) p99-100.

[9] 45% per annum compared to 60% worldwide (source "RFID chips: Future technology on everyone's lips", Deutsche Bank Research, February 20, 2006, cited in COM(2007)96.

RFID also holds the promise to become one of the key technologies for the "Internet of Things"[10] where smart objects communicate with each other (ambient intelligence) and new services and applications can be offered by linking the RFID information to databases and communication networks. It offers the potential to become a powerful catalyst for innovating the European economy and our daily lives.

2.2. Challenges for RFID deployment

RFID is a powerful technology which has the potential to boost the EU economy and to increase convenience of citizen's everyday life. It can create new services and jobs and increase efficiency of production, trade and services. The above mentioned figures show that implementation of RFID technology lags behind the US and certain Asian markets (especially South Korea and Japan) and this gap could further widen in the future. As a consequence, European companies will not be able to grasp full benefits of mass deployment of RFID.

The public debate on RFID and consultations with experts and stakeholders revealed that there are certain challenges to faster and wider deployment of RFID technology in the EU market. Consumers are sensitive to privacy, security and data protection related issues and there appears to be uncertainty among the industry players as to whether and when the data protection legal framework is applicable in the case of RFID. The four key challenges – privacy concerns, security risks, awareness and interpretation of data protection law – are discussed below in more detail.

2.2.1. Privacy and data protection related risks and concerns

Notwithstanding the expected benefits of the widespread deployment of RFID technologies, it also leads to public concerns especially regarding privacy, data protection and security[11]. The possibility that the collected information can relate to an identified or identifiable individual who based on that information could be identified either directly or indirectly is one of the main areas of concern, especially with respect to item level tagging at the consumer level and workplace performance monitoring.

In itself the collection of data, in many cases personal data and risk of its use by third parties or the possibility of combining data for profiling consumers and/or for marketing purposes are not new or specific to RFID technology. However, the expected scale of deployment and the rapidly evolving and interconnected digital technologies pose significant new challenges.

The **potential privacy and data protection related risks** are due to the assumption that RFID offers the possibility to establish profiles (e.g. on purchasing behaviour), track and trace people's movements, or misuse personal data stored on the RFID tags or in the database which is part of a backend system. Although these data do not have to be personal data, it

[10] The "Internet of things" predicts a world wherein billions of everyday objects are linked in a network and are intercommunicating. This idea has grown from advanced concepts from the last twenty years, such as ubiquitous communications, pervasive computing and ambient intelligence. In a world of "Internet of things", computing is enabled to melt invisibly into the fabric of our business, personal and social environments, supporting our economic, health, community and private life (EC, 2006).

[11] See e.g. EC (2004) Consultation report on *'Smart wireless tags research needs'*, CapGemini (2005), *RFID and consumers,* Spiekermann, Ziekow (2006), *A systematic analysis of privacy threats,* JRC (2007), *RFID Technologies: emerging issues, challenges and policy options,* OECD (2006), RFID: *Drivers, challenges and public policy considerations,* EC (2007) *Results of public online consultation on future RFID technology policy (SEC(2007)312,* STOA (2007), *RFID & Identity Management in Everyday Life,* Rathenau Insitute et.al. (2007), *RFID awareness of consumers.*

does lead to new possibilities of combining data, which eventually may be related to individuals. When data are transferred from one data controller to another this risk increases. Also, RFID uses wireless communication which allows for data retrieval without the line-of-sight, which could increase the risk of unwanted tag reading. This practice however would depend on the reading distances incurred by the used RFID technology. Although other technologies also use wireless communication (e.g. mobile phones, WiFi, Bluetooth) and could pose similar risks, the key difference is that RFID tags are in general hard to "turn off".

Especially with respect to **item level tagging in consumer environments** (such as retail) the risk of unwanted tag reading may occur. This is caused by a number of factors including the expected mass deployment, the limited level of security on small, cheap tags, and the possibility to link product data to individuals/consumers. The privacy and data protection related risks do not always occur as result of the introduction of RFIDs alone (which do not always contain personal ID data itself), but can arise through combining several information sources.

Table 2.7. Consumer concerns related to RFID

Issues of concern	EU (%)	USA (%)
Consumer data used by third parties	59	69
Tracking of consumers via product purchases	55	65
Tags could be read from a distance	52	42
Targeted, more direct marketing	52	67

CapGemini (2005)

Privacy and protection of personal data are therefore seen as one of the key concerns about RFID technology. Recent surveys tend to indicate that this concern is shared by approximately two-thirds of respondents[12]. Various consumer surveys, and the EU Commission's own consultation on RFID, indicate that this is a headline issue. According to a recent study by CapGemini[13], privacy is seen by European consumers as one of the main concerns related to RFID technology, albeit at a slightly lower level than by US consumers. The use of consumer data by third parties and tracking of consumers via product purchases are particularly major concerns (see Table 2.7).

One of the consequences of the privacy and data protection related concerns described above is that the resulting **distrust can impact the deployment of RFID**. In this context, many hold the view that privacy and security is a fundamental enabler or a showstopper of smart wireless tag technology[14]. A recent OECD report states that "*without addressing privacy related issues carefully and transparently … backlash by consumers and citizens is a potential risk that could limit long-term benefits and development.*"[15]. Well-known public campaigns such as

[12] For example see CapGemini 2005. Consumer surveys carried out by CAP (2004, and BIGResearch & Artifact (2004) reveal similar results in this respect (these surveys are cited in JRC (2007)). The Commission's own consultation in 2006 shows also comparable results.

[13] CapGemini (2005).

[14] See EC (2004) Consultation report on Smart wireless tags research needs.

[15] OECD (2006), Radio-frequency Identification (RFID): Drivers, challenges and public considerations. Cited in JRC (2007).

those against Benetton, Gillette and TESCO were effective in halting the companies' RFID trials[16] and illustrate how privacy concerns can have an impact on deployment of RFID.

Table 2.8. Factors contributing to trust and perceived risk

Factors contributing to trust	Factors contributing to perceived risk
Ability to trust[17]	Risk Perception Bias
Experience (personal or via other people)	Uncertainty
Predictable performance	Personal details (more details result in higher risk)
Comprehensive information	Alternatives (level of choice)
Shared values	Specificity (sole or multiple supplier of system)
Communication	Autonomy of the system
Interface design	

ECORYS, based on JRC (2007).

According to recent literature[18], trust and risk affect the success of a new technology. The risk in this respect is the perceived risk by the consumer, which may or may not be related to the actual risk. If the perceived risk is high and no sufficient trust is available to offset this risk, the acceptance of RFID technology may become problematic. Table 2.8 gives an overview of factors which influence trust and perceived risk levels.

2.2.2. Awareness of RFID technology

Existing consumer surveys provide clear evidence that a large amount of people are still unaware of RFID[19]. For instance, a survey in 2005 showed that only 18% of European respondents had heard of RFID[20].

There is a common agreement among experts that lack of experience with RFID technology and a low level of public awareness directly affect both trust and risk levels towards an RFID application. Awareness will also have a direct impact on the speed of deployment through the business community, and especially SMEs, which are still unaware of RFID and its potential. In this respect, dissemination of information is an important factor to enhance overall public awareness. This is relevant both for increasing the level of awareness on the economic potential and technical possibilities of RFID, and on the rights of consumers and all individuals, which stem from the existing data protection legislation.

[16] See http://www.nap.edu/books/0309095433/html/21.html.

[17] All people possess a basic level of trust, but people do not have the same baseline level of trust.

[18] See e.g. A. Patrick (2002), Privacy, trust, agents and users: a review of human-factors issues associated with building trustworthy software agents. A more extensive review of this issue is presented in JRC (2007), RFID Technologies – Emerging Issues, Challenges and Policy Options.

[19] See also JRC (2007).

[20] CapGemini (2005).

2.2.3. Security related issues

An RFID system is prone to a number of **security threats**. Reasons for attack can be eavesdropping, espionage, fraud/deceit, and putting the system out of order. Obviously threats are higher if the value of the information (or the value of the result of the security attack) is higher to the attacker, and the security level (the threshold) is lower. For example high value goods will in general represent a higher threat profile than low value goods. As a result, items which are prone to a higher threat level might merit more stringent security safeguards. Whatever countermeasure is used, the RFID system is as strong as its weakest link. Therefore, the system should be analysed to determine the most appropriate security level, in order to decide which countermeasure is most adequate. Although in principle most privacy risks can be overcome by using so called privacy enhancing technologies (PETs)[21], the need for small and cheap tags, especially in item level tagging, will limit the application of these measures.

Information security has a direct link to the privacy risks perception of citizens as one of people's fears is that tags can be read from a distance[22]. As indicated earlier, the possibilities of monitoring tag information from a distance is strongly dependent on the technical specifications of the RFID technology that is used. However, not only tag information may pose a risk. Illicit use of data stored in a back-end system can pose a threat. Also in a business environment security of information may be an issue (e.g. industrial spying, theft, re-coding of tags, etc.).

2.2.4. Regulatory framework: Directive 95/46/EC - Data Protection Directive

2.2.4.1. The Data Protection Directive

The objective of the **Data Protection Directive** is to protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of personal data. The Directive sets the general rules on the lawfulness of the processing of personal data, including criteria for making data processing legitimate and provisions related to the confidentiality and security of processing. The Directive applies regardless of the technology used for the processing of personal data.

Article 29 of this Directive sets up an independent advisory body so called Article 29 Data Protection Working Party that shall, among other issues examine questions covering the application of the Directive in order to contribute to its uniform application across Member States, advise the Commission on issues related to the protection of personal data or issue recommendations on all matters relating to the protection of personal data. Furthermore, Article 27 of this Directive supports the development of specific **codes of conduct** to take account of the specific features of the various sectors. According to this Directive, these codes of conduct can be either drawn up at a national level[23] or at Community level[24].

[21] COM (2007)228 final.

[22] The results of the consumer survey quoted in table 2.2 indicates that 52% of EU consumers fear that tags can be read from a distance.

[23] The German Federal Office for Information Security (BSI) is working on a set of guidelines for the use of RFID technology in various application domains (e-Ticketing for events, NFC-based mobile ticketing, e-Ticketing for public transport, and logistics and retail), which are expected to be published towards the beginning of 2008 (http://www.bsi.de/veranst/rfid/index.htm).

[24] The first Community code of conduct on the use of personal data in direct marketing was approved in 2003.

2.2.4.2. The concept of personal data

An important aspect regarding the applicability of this Directive to RFID is the definition of personal data. In Article 2(a) of the Directive, personal data is defined as *"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".*

In case of an RFID application, a test whether personal data will be processed could be quite challenging, since a stand alone piece of information can be non-personal, but "as a person can be linked to a RFID serial number, the distinction between personal data and non-personal data could be blurred"[25]. An important issue here is, according to Recital 26 of the Data Protection Directive to determine whether a person is identifiable while taking into account all the means likely reasonably to be used either by the controller or by any other person to identify the said person.

This difficulty has been identified by the Commission which has stated that "RFID devices raise fundamental issues on the scope of the data protection rules and the concept of personal data."[26] This is one of the main causes of **regulatory uncertainty with respect to RFID application**, especially in cases of item level tagging. This uncertainty has a direct impact on investor behaviour, as confirmed by the 2006 public consultation which showed that "regulatory certainty is sought by industries that wish to deploy RFID and by users."[27]

The definition of "personal data" can also give rise to **different interpretations in the practices of the Member States**[28]. This partly results from the fact that the relevant provisions leave Member States with a "margin of appreciation" in adopting national legislation. The European Court of Justice has made it clear that nothing prevents Member States from extending the scope of national legislation implementing the provisions of the Directive, to areas not included within the scope - provided that no other provision of community law precludes it[29].

In January 2005 the Working Party 29 published a working paper[30] which aimed to provide guidance to RFID users on the application of the basic principles set out in the EC Directives, in particular the Data Protection Directive and Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive). It also provided guidance on designing privacy compliant technology. Furthermore, the Working Party analysed in details the notion

[25] EC (2006) RFID Consultation Workshop summary. This difficulty is noted by various other authors including OECD and WP Article 29.

[26] Commission of the European Communities, *Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive*. Brussels, 7.3.2007, COM(2007) 87 final, p. 7.

[27] SEC(2007)312, Results of the online consultation on future RFID technology policy.

[28] This discussion began when the European Commission considered to start an art. 226 EC infringement procedure against the United Kingdom for incorrect transposition of Directive 95/46/EC. This was caused by the case known as the *Durant case*. Court of Appeal (civil division) 8 December 2003, *Michael John Durant. Financial Services Authority*, [2003] EWCA Civ 1746.

[29] Judgment of the European Court of Justice C-101/2001 of 06.11.2003 (Lindqvist), § 98. Cited in WP Art 29 (June 2007), Opinion 4/2007.

[30] WP Art 29 (2005) Working Paper 105, Working Document on Data Protection Issues related to RFID Technology.

of "personal data" in its recent Opinion on the concept of personal data[31] that serves as practical guidance what is and what is not considered as personal data.

2.2.5. The European Data Protection Supervisor (EDPS)

More recently, in December 2007 the **European Data Protection Supervisor (EDPS) published its opinion** in reaction to the Commission's Communication on RFID (COM(2007)96). In his opinion, the EDPS agrees with the view that RFID systems could play a key role in the development of the Information Society. Further, the EDPS states that RFID may have a fundamental impact on our society and on the protection of fundamental rights in our society, such as privacy and data protection.

The opinion indicates that for a number of reasons possible consequences of RFID on data protection are uncertain at the moment, but it recognizes that data protection safeguards are important for the acceptance of RFID. The EDPS considers it justified to focus first on item level tagging in consumer products, because of the expected mass deployment of RFID systems in retail environments and the potential risks of surveillance and automated large scale data processing in a future information society. This risk is also influenced by the life cycle of a product.

A number of specific data protection risks are identified:

– RFID systems may potentially lead to the identification of an individual,

– data controllers of RFID systems may change throughout the chain,

– wireless nature of tag communication,

– small and cheap tags limit security measures that are applied,

– lack of transparency in data processing.

As a result of these risks, the EDPS considers that self-regulatory measures in the form of codes of conduct or best practices, as indicated in Article 27 of the General Data Protection Directive, are appropriate. The EDPS does point to the obligation of the regulatory framework when handling personal data and recommends guidance by the Commission on the application of the current regulatory framework to the RFID environment, including the promotion of privacy by design measures. The EDPS favours an opt-in principle at the point of sale with respect to de-activation of tags as a precautionary approach, although flexibility of this approach is at the same time recommended. This also allows erasing tag information from the database, in case of short life products, instead of tag de-activation. In case of failure of self-regulation binding legislative measures may still be needed.

2.2.6. Regulatory framework: Other relevant legislation and regulation

2.2.6.1. The ePrivacy Directive

A second directive of relevance is the Privacy and Electronic Communication Directive 2002/58/EC (ePrivacy Directive), which is sector specific and complementary to the Data Protection Directive. It applies its principles to the processing of personal data in connection

[31] WP 136, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

with the provision of publicly available electronic communications services in public communication networks. This Directive concerns RFID applications when they are connected or make use of public communication networks.

2.2.6.2. The R&TTE Directive

Of further relevance is the Radio & Telecommunications Terminal Equipment Directive (1999/5/EC) - **R&TTE Directive**. Article 3.3 of this directive contains provisions to assure the privacy of identity. It stipulates that "… the Commission may decide that apparatus within certain equipment classes or apparatus of particular types shall be so constructed that it incorporates safeguards to ensure that the personal data and privacy of the consumer and of the subscriber are protected; and/or that it supports certain features ensuring avoidance of fraud". This directive thus reflects the conditions stated in Directive 95/46/EC.

At a more aggregate and fundamental level, also related to the issue of data protection is the recent EC Communication on promoting data protection by **Privacy Enhancing Technologies** (PET)[32].

2.2.6.3. Health aspects

The potential **health** effects under RFID fall under the Council Recommendation 1999/519/EC of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) and on Directive 2004/40/EC of the European Parliament and of the Council of 29 April 2004 on minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields).

2.2.6.4. Environmental aspects

On the environmental side, there is a relation with the Electrical and Electronic Equipment Directive to the extent that RFID may be considered as **electronic waste**.

2.2.6.5. Self Regulation

Besides the EU Directives on Data Protection, ePrivacy and R&TTE, there are examples of **self-regulation**. The most noticeable examples of self-regulation are the International Chamber of Commerce principles on EPC deployment and operation[33] and the EPCglobal guidelines[34]. The latter state that in order to unlock the potential of RFID and the EPC, it is important to address privacy concerns regarding the use of the technology. EPCglobal has proposed a set of privacy guidelines that companies deploying RFID can follow to complement existing national and international legislation and regulation dealing with consumer protection, consumer privacy, and other issues. Key tenets of the guidelines incorporate principles of industry responsibility, providing accurate information to consumers, and ensuring consumer choice. The guidelines encompass practices for consumer notice, consumer choice, consumer education, as well as record use, retention, and security. EPCglobal also suggests that companies provide consumers with notice and choice when tags are used, including options to disable tags after the point-of-sale.

[32] COM(2007)228.

[33] Available at: http://www.iccwbo.org/id600/index.html.

[34] Available at: http://www.epcglobalinc.org/public/ppsc_guide/.

In general, the most important aspects of the existing self-regulatory acts are:

- inform the consumer (e.g. about the presence and/or the consequences);
- offer the consumer a choice (e.g. RFID tag or not);
- abide the law that is applicable;
- secure the data that is controlled by the technology.

In addition, there are countries that have specific RFID regulations. The U.S.[35], Canada and Japan[36] for example have RFID guidelines.

With respect to **data protection of workers**, International Labour Organization (ILO) drafted a code of practice on the protection of workers' personal data[37]. It covers general principles of protection of workers' personal data and specific provisions regarding the collection, security, storage, use and communication of such data. While this code of practice does not replace national laws, regulations, international labour standards or other accepted norms, it can be used in the development of legislation, regulations, collective agreements, work rules, policies and practical measures at enterprise level. The ILO code of practice follows similar principles as the Council of Europe Recommendation on the protection of personal data used for employment purposes[38].

2.2.6.6. SWOT Analysis

The table below presents an overview of strengths, weaknesses, opportunities and threats (SWOT) of EU-wide implementation of RFID. It suggests that given the currently premature stage of deployment of RFID technology, especially in the supply chain and consumer-oriented applications, there is actually a need to increase Europe-wide legal certainty for both investors and consumers/citizens in order to realise the full potential of RFID while still addressing in the most relevant, efficient and effective way the issues of privacy, data protection and information security.

Table 5.1 Strengths, weaknesses, opportunities and threats of EU-wide implementation of RFID

Strengths	**Weaknesses**
– Europe houses part of the big RFID suppliers – Leading countries worldwide with focused attention on RFID (UK, France, Germany, The Netherlands, Italy) – Interesting public domain applications – Focus of attention comparable to USA	– Many European countries with only marginal attention for RFID – Vulnerable image of RFID – No level-playing field for RFID across countries – No harmonised frequency policy in all European countries

[35] http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf.

[36] http://ubiks.net/local/blog/jmt/archives3/001114.html.

[37] ILO (1997) Code of Practice on protection of workers' personal data.

[38] Council of Europe Recommendation R(89)2.

Opportunities	Threats
– Sharing of experiences in non-competitive markets (public transport, health, …) – Creation of European market of RFID applications (health, public transport, identity cards) – High market potential – Considerable potential efficiency gains – Creation of shared research agenda (security issues of passive RFID, novel technologies – chipless tags, SAW,etc.) – Organisation of societal dialogue on RFID implementation in societal domains	– Hidden costs (societal and organisational) may be high – Lack of skilled workforce – Negative experiences in one domain may influence commitment in other domains – Growth in complexity of RFID systems may counteract possible positive uses – Legislation may hinder wide-spread deployment (privacy) – High initial costs – Job losses

Source: based on TNO report No. 035.30374.

2.3. Justification for EU intervention

The cross-border nature of RFID applications, the risk of diverging responses in Member States combined with the high importance of RFID both from the viewpoint of privacy and security and economies of scale are the core arguments justifying an intervention at EU level. Strictly speaking, an intervention has its legal base in the Treaty establishing the European Community, in particular in Article 211.

When the expected mass deployment of the technology takes place at item level, RFID will potentially affect all individuals in the EU. RFID applications are **borderless**. Although there will be applications that are developed in a closed environment within one country, a large number of applications involve activities that cross borders both within the EU but also outside the EU (e.g. RFID in supply chain management and item level tagging in products).

EU-wide benefits of RFID can be found especially in areas where European integration, cooperation and coordination have progressed most – fighting against terrorism, recognising and combating animal diseases, coordinating European research. In these domains of an economic, social and/or political nature, RFID may contribute to realising tangible benefits for Europe. The effort in achieving European synergies and benefits, however, is not trivial: collecting personal data with RFID to enhance security raises privacy issues; enforcing the use of RFID in the tagging of animals is not easy to realise in many countries; the creation of a European research agenda on RFID requires cooperation between different stakeholders in the value chain.

The issues of privacy, data protection and security related to RFID have recently gained significant attention not only at the EU level but also in Member States. Although the existing EU data protection legislation covers privacy and data protection issues a further interpretation of its application in a specific situation can improve legal certainty ex ante on privacy, data protection and security issues. If no action is taken at the EU level at this particular moment in time, Member States could take action individually with the risk of creating **different interpretations of the existing legal framework and divergence in**

RFID policy. This in turn could result in the distortion in functioning of the internal market and would have detrimental impact on the speed and level of RFID deployment across Europe. A harmonised or at least co-ordinated approach is therefore necessary to prevent fragmented solutions and creation of additional obstacles for companies and consumers.

EU should take action since the objectives can be better reached by the Union than by individual initiatives launched by the Member States. More importantly, Member States alone will not be sufficient to achieve the set objectives. Consequently, there is a clear added value in intervening now at an EU level.

Finally, RFID industry has a big growth potential and the EU can become one of the world leading forces in this development. With clear legal requirements and guidance on their application at the EU level, it will be much easier for both RFID manufacturers and application providers to realise **economies of scale** and EU wide deployment of this technology.

2.4. What if EU takes no action?

It can be expected that in case EU does not take any action at a Community level the development of a common approach towards RFID applications across Europe could be hampered. It should be stressed that the risk of fragmented, un-harmonised approaches across Member States is considered one of the main arguments for an intervention at an EU level. Adverse impacts of an un-harmonised approach can be expected. The existing lack of clarity and corresponding uncertainty for potential RFID application users is likely to slow down the investment and uptake of RFID in different sectors, especially in those sectors where privacy concerns are highest. Initiatives will show a more fragmented, pilot character and mass scale deployment could be delayed. A similar lack of clarity and uncertainty will remain for citizens thus feeding their privacy concerns. Triggered by the privacy and data protection related concerns of individuals, Member States will start taking measures towards potential RFID applications. Their responses are likely to differ in time and scope as no explicit co-ordination will exist at a European scale and the sensitivity of Member State governments to these privacy and data protection related concerns will differ. The differentiated treatment of RFID applications at a European scale and the continued uncertainty could have negative consequences for deployment of RFID. As a result, not only the potential benefits of RFID applications will be postponed, but also the competitive position of the EU RFID industry will worsen in comparison to countries which are applying RFID technology at a faster pace.

All these arguments suggest that an EU level action will provide an added value because Member States cannot tackle the above mentioned issues satisfactorily by themselves and the objectives of wider deployment of RFID and mitigation of privacy, data protection and security can be achieved more efficiently and effectively through a co-ordinated EU level action.

3. OBJECTIVES

3.1. Objectives for a future RFID policy on privacy, data protection and security

The principal objective of the intended Commission intervention is to address the privacy, data protection and security problems associated with RFID use. As noted in the problem definition, these problems create challenges to wider and faster RFID deployment in Europe for the benefit of the economy and of all stakeholders concerned by RFID, including individuals (citizens, consumers, travellers, patients, etc), as well as companies. The objectives of "guaranteeing privacy and security" and "promoting a fast and comprehensive deployment of RFID across the EU" are intertwined – on one hand, the unresolved privacy and security issues generate a lack of trust and consumer acceptance that hinders the further deployment of RFID technology and applications; on the other hand, the fact that Europe trails behind other countries in the world in accomplishing the implementation of large scale pilots and trials makes it relatively difficult to draw concrete lessons from experience with respect to the potential privacy and security issues in actual settings (sectors/applications).

The **specific objectives** are more immediate objectives of the intervention that contribute to achieving the overall objectives. The following specific objectives have been identified to be achieved in the medium term:

– to mitigate security, data protection and privacy related risks related to RFID use, especially in business-to-consumer (B2C) environments, and in particular

    (a) to minimise the number of complaints and court cases from consumers on infringement of privacy and data protection law,

    (b) to reduce the percentage of consumers who state their concerns and to increase the percentage of consumers who state higher levels of trust (in surveys),

– to avoid uncertainty among investors as to the applicability of the existing privacy and data protection legislation to RFID applications, and in particular

    (a) to increase the number of large-scale pan-European RFID pilots,

    (b) to increase the investment in secure and privacy aware RFID applications by companies in the EU,

    (c) to decrease the number of requests for information to Data Protection authorities,

– to stimulate innovation through a wider adoption of RFID applications, and in particular

    (a) to increase the take-up and adoption of RFID in various application sectors,

    (b) to increase the number of European RFID patents,

    (c) to improve productivity in RFID-related sectors, such as logistics, retail,

– to facilitate development of harmonised, interoperable use of RFID in Europe and similar privacy & security conduct in the different Member States of the EU, in particular,

    (a) to stimulate the creation of Community codes of conduct,

    (b) to intensify cross-border investment in RFID,

– to improve awareness among citizens and companies (including SMEs) of benefits, potential threats, as well as rights and obligations related to RFID applications, in particular

(a) to increase percentage of consumers and citizens who are aware of RFID,

(b) to accelerate the adoption of RFID by SMEs.

3.2. Relevant EU policy background and objectives

The general and specific objectives of the planned RFID initiative correspond to the overall wider EU policy goals and strategies. Of direct relevance to RFID is the Lisbon Strategy which aims at transforming Europe into a competitive, dynamic, knowledge-based economy. In the area of information society, the i2010 policy framework supports the realisation of the Lisbon Strategy. Objectives of the RFID initiative are fully in line with the general i2010 policy framework.

Recently adopted under the i2010 strategy, the Communication "A strategy for a Secure Information Society"[39] emphasises the positive virtue of technological diversity, as an integral component of security and highlights the strategic importance that European industry has both as a demanding user, and as a competitive supplier of network and information security products and services. It encourages stakeholders to pursue regular dialogue and tackle the information and network security problems in a co-ordinated manner. The overall strategy outlined in this Communication has a direct relevance for the RFID-related security issues.

4. POLICY OPTIONS CONCERNING THE CHOICE OF THE LEGAL INSTRUMENT

4.1. Introduction

This impact assessment examines policy options at two different levels. First, the available options concerning the choice of a suitable policy instrument are discussed and assessed (Section 4). Second, specific measures within the most suitable policy instrument identified at the first level (i.e. content of a policy instrument) are presented and assessed (Section 5). As noted above, the Commission Communication reporting on the results of the public consultation already expressed a certain preference for the policy instrument, mentioning explicitly a Commission Recommendation as the "preferred option" insofar as it constituted a timely and effective response to the immediate concerns expressed by European stakeholders, notably interested citizens, during the public consultation of summer 2006. It is nevertheless important to explain what other options are available and why a specific instrument is preferred. This assessment is carried out at a more general, essentially qualitative level, whereas the assessment of content options in Section 5 goes into more detail on specific measures and assesses some of the costs quantitatively.

It must be stressed that the time dimension is critical in this discussion. In this respect, the impact assessment specifies, at a given point in time, the advantages and disadvantages of the various options.

4.2. Policy options concerning the instrument

The following three policy options concerning the instrument should be analysed in more detail:

1. No change (a baseline option),

[39] COM(2006)251.

2. Introduce a comprehensive set of ‘soft’ law instruments including Commission Recommendation,

3. Introduce ‘hard’ legislative instruments.

Option 0 is a baseline option against which the two remaining options are assessed. It does not propose any additional measures above those that are already in place. In this option, any additional policy decisions and initiatives will be left largely to Member States and stakeholders. The EU will continue to finance projects and networks, support research, facilitate exchange of best practice, and collect and disseminate information on RFID application and impact. At the same time, not coordinated activities across policy domains will be pursued.

Option 1 encompasses a set of "soft" policy instruments across all relevant policy domains, including:

– ‘soft’ legislation (a Commission Recommendation),

– self-regulation (codes of conduct),

– information and education campaigns.

A recommendation would allow the Commission to suggest a line of action without imposing a direct legal obligation on those to whom it is addressed (the Member States, other institutions, industry or in certain cases the citizens of the Union). It would provide strong guidance with respect to interpretation of existing data protection legislation and proposed lines of action to be taken. It would also encourage further development of codes of conduct for specific RFID applications, as the recommendation itself cannot cover all potential RFID applications that exist or are being developed. In addition, an **awareness raising** campaign can form part of this set of instruments, as RFID technologies are widely unknown to both the public and many enterprises.

Option 2 would mean that privacy, data protection and security issues related to RFID would be subject to new specific legislation. Among the available legislative instruments, and given the problem definition as described in Section 2, a directive would be the most suitable legal instrument.

The content of a directive could be for some measures similar to the content of a recommendation but measures imposed by a directive would be binding. They would have to be transposed into national legislations and enforced by relevant public authorities. Specific RFID legislation would be in a position of *lex specialis* with respect to the Data Protection Directive. A RFID directive could also introduce additional requirements, e.g. codes of conducts could be made obligatory for all or certain RFID applications.

4.3. Assessment of the impacts of the policy instrument options

The assessment focuses on the main differences between the instruments applied to the specific case of RFID policy. As such, impacts can be assessed only at a general level using the following criteria:

- the cost-effectiveness of the intervention (administrative and compliance costs in relation to effectiveness) for business (RFID industry, RFID applications providers) and public authorities,
- flexibility of the instrument,
- regulatory certainty and consumer trust, and
- time-to-implement.

Administrative and compliance costs

It is clear that "no change" option will not lead to any additional administrative and compliance costs. The policy options 1 and 2 will result in additional costs in comparison with the "no change" option.

Compliance costs depend on the content of an instrument rather than on its nature, and the degree to which it is followed (see Section 5 for an analysis of costs of the content options). It can be reasonably assumed that the level of compliance would be similar for Option 1 and Option 2 because the proposed Recommendation in Option 1 is based on a wide consensus among stakeholders. The Recommendation is largely acceptable for most stakeholders across the board which provides a reasonable assurance of significant compliance based on actual commitments of the industry and Member States. Under voluntary schemes of self-regulation, verification of adherence to codes of conduct, processing of complaints and dispute resolution would need to be implemented by the private entities (associations, etc.) managing the self-regulation instruments. These mechanisms would be financed directly by the association members and signatories to self regulation, i.e. the industry partners, and could therefore result in principle in higher costs for the private sector.

All in all, in the short term the compliance costs of option 1 and option 2 would be similar but in the longer term the compliance costs of option 1 would be lower due to a likely change of behaviour within the private sector towards self regulation and adhered industry-specific codes of conduct and the gradual amortization of the initial high costs.

As concerns administrative costs, option 2 will lead to higher budgetary and administrative costs for public authorities and the Commission than option 1 given that new legislation would require monitoring and enforcement.

Effectiveness

With respect to effectiveness of the different policy instruments, both Options 1 and 2 are expected to bring more positive results than the “no change” scenario. As noted in the assessment of the baseline scenario (Section 2.4) no intervention could lead to a more fragmented patchwork of solutions where achievement of the general and specific objectives will become increasingly difficult and consumers’ trust in RFID technology could be further undermined.

Effectiveness of a recommendation combined with self-regulatory measures will essentially depend on the level of industry commitment and willingness to implement the recommended measures and to agree on and implement codes of conduct in different sectors. Already today, more and more industry-driven initiatives to develop sector specific guidelines on respecting privacy (eg., EPCglobal Guidelines on EPC for Consumer Products) are emerging.

Option 2 could be effective in terms of mitigating privacy and security risks and providing higher level of trust for consumers. However, the risk of imposing high costs and unnecessary burden on the industry is relatively high as RFID is still in the initial phase of deployment. Imposing any RFID-specific regulatory measures now in this fast developing and changing market would bear the risk of a regulatory failure with significant consequences on hindering the speed and level of deployment of RFID applications that could bring many benefits to society in general.

Cost-effectiveness

From the above analysis on the compliance costs and the effectiveness, it can be concluded that the option 1 should be more efficient than option 2.

Flexibility

In terms of flexibility of different options, Option 1 provides a more flexible solution than Option 2. Given the fact that RFID market is still not sufficiently developed and mature, flexibility and a possibility of a quick public policy response to new developments is particularly important. While legislation should not be excluded from possible options in the future, it is not suitable for rapidly changing and relatively new markets and technologies such as RFID at this point in time. A specific legal measure in a rapidly evolving area like RFID runs the risk of some issues being not covered while other issues may no longer be relevant or up to date by the time the measure is adopted.

Regulatory certainty and consumer trust

Option 2 has the highest impact on regulatory certainty and consumer trust, as it would clearly define the rights and responsibilities of RFID application providers and regulate the modalities of use of RFID technology including appropriate sanctions for non-compliance. An intervention is expected to have a direct influence on the **regulatory uncertainty** of investors as it further clarifies the interpretation of the existing regulatory framework (in particular on data protection) regarding RFID applications. By offering a framework for a common European approach it also reduces the risk of additional national regulation for RFID applications. Both option 1 and 2 are expected to have a significant positive impact on this issue in comparison with the baseline scenario, and are not assessed to present major differences as the content of both options would be comparable.

The other aspect of influence on the uncertainty of investors is the **risk and trust of the public,** particularly in environments where there is a direct interaction with consumers or citizens (e.g. retail, health). According to the risk-trust model (see Table 2.8) the perceived risk can be positively influenced by limiting uncertainty, limiting the amount of personal details provided to the system, creating alternatives for consumers (freedom of choice), and the degree of autonomy of the system. Through its higher attention on information exchange to the public and awareness raising activities, option 1 is expected to address the perception of RFID at a general level and overcome some basic fears and potential myths.

The risk and trust of the public is also influenced by the effectiveness of the type of intervention as perceived by consumers and citizens. In the public consultation on RFID in 2006 it was shown that respondents, of whom 70% were 'interested citizens', have only limited confidence in self-regulation (approximately 15%) and that they have a higher belief in additional hard legislation (66%). As such, the impact on trust and acceptance could be expected on these grounds to be higher for policy option 2 than for policy option 1, especially because policy option 2 “hard legislation” has a strong possibility for enforcement. However, it should be noted that this does not necessarily lead to the conclusion that the current intervention's objectives of privacy and security would be better achieved through "hard" legislation.

Higher consumer trust in "hard" legislation can be counteracted by an actual pro-active behaviour of (especially consumer-oriented) sectors and industry in the development of specific codes of conduct which prove their good will. A priori, there seems to be a mutual interest in safeguarding the privacy and security risks in certain sectors, as citizens’ concerns will also affect their economic performance. Fear among consumers and negative publicity campaigns could seriously harm the economic performance of (retail) enterprises. There thus exists an incentive to adopt soft measures, as long as the costs are not too high. Soft measures do not fully exclude hard legislation, as hard legislation can be used as a “stick” when soft regulation proves not to be effective. This is the traditional approach surrounding e.g. industry covenants. The existence of this threat alone can stimulate pro-active industry behaviour.

Introducing hard legislation now would be premature also because the industry does demonstrate now its good will by launching initiatives aiming to self-regulate the market in terms of consumer privacy protection and security. As described in Section 2.2.5, one of the most known examples of a **voluntary code of conduct** are the guidelines developed by ECPglobal.

Time-to-implement

The recommendation under policy option 1 follows a relatively light decision-making process and can be quickly adopted, in other words the **time-to-implementation** is low. Policy option 2 first has to be adopted by the Council and the European Parliament and then it requires a number of years to be fully transposed into national legislation of the Member States. This longer preparation period can be important as it will be difficult to develop a “one-size-fits-all” for all RFID applications, given the wide scope of application that are, or might be, developed. This does require a continuous updating of the existing legislation in line with new developments, which makes it a relatively cumbersome process and may even hamper the development of new applications (as it is not clear from the beginning which requirements should be legally met).

4.4. Conclusions

A summary of the considerations made in the previous section is presented in Table 4.1.

Table 4.1. Comparison of options on policy instruments

Impacts (factors)	Option 0 No change	Option 1 Soft legislation	Option 2 Hard legislation
Administrative and compliance costs	0: No additional costs	- Moderate administrative and compliance costs.	-- Additional administrative and compliance cost.

Impacts (factors)	Option 0 No change	Option 1 Soft legislation	Option 2 Hard legislation
		Costs of maintaining self regulation instruments	Monitoring and enforcement cost for PAs
Effectiveness	0 not relevant	+ Effective	+ Effective
Cost-effectiveness	0	++ Most cost-effective	+ Effective but at the expense of higher costs
Flexibility	0 not relevant	++ Flexible	- High effort for adaptation
Regulatory certainty and consumer trust	0 Remains low. Potential risk of fragmented approach across member States. Consumer trust not affected.	+ Positive effect through guidance on applicability of regulatory framework for RFID.	++ Offers further guidance on applicability of regulatory framework for RFID.
Time to implement	0 Not relevant	- Relatively fast legislative process	-- Longer approval process and time needed to transpose regulation in national laws

In conclusion it can be stated that the policy option 1 involving "soft" law instruments, such as a recommendation, is the preferred option. Given that RFID is yet in the early stage of its deployment, the time dimension of any Commission intervention is crucial. Imposing any RFID-specific legislation as of now on privacy, data protection and security would bear the risk of playing against proper use of RFID technologies, i.e. hindering the adoption and further development of RFID applications that could bring many benefits to society in general. A recommendation offers in this respect more flexibility, is faster to implement and is much more cost-effective than any other policy option that could be considered at this stage. It must be noted also that the resulting current preference for a recommendation does not exclude any further legislative measures in due time in the future. A recommendation constitutes now a preferred policy instrument option on the assumption that if the implementation of the recommendation fail to achieve its goals within the next few years, the Commission might amend it or submit any other proposal deemed necessary, including binding measures. Consequently, in the next section and in the remainder we analyze options that form the concrete contents of the selected policy instrument, i.e. a recommendation.

5. CONTENT OPTIONS

5.1. Introduction

The content options (sub-options) are related to requirements that are either specific interpretations of the general data protection directive or are additional. In accordance with Section 1.2, unless otherwise stated, these sub-options apply for all potential RFID applications (note that some are specific to the retail sector).

Based on the problem definition detailed in Section 2, the following sub-options under three main areas of analysis can be identified:

I. Assessment of privacy and security risks. This includes:

(a) No change on prior assessment requirements,

(b) *Privacy impact assessments* to be conducted and systematic security risk management (combined or conducted separately) for RFID application operators before any implementation,

(c) Certification by authorised third party organisations and/or public authorities.

II. Information to be provided to individuals and awareness-raising. This includes:

(a) No change on requirements related to information and communication,

(b) The development and dissemination of a *written information policy* for each RFID application that describes its intended use,

(c) Same as (b) + indication of RFID presence through images and logos.

III. Retail specific provisions. This includes:

(a) Implementation of the opt-in principle with no additional requirement in retail environments beyond existing legal requirements,

(b) Implementation of the opt-in principle for all situations, including those not covered by the existing legal framework,

(c) Implementation of the opt-in principle with some level of flexibility.

The assessment of the sub-options follows the following process:

(a) For each sub-option, an assessment of the associated compliance costs,

(b) For each sub-option, an assessment of the following direct economic and social benefits is provided:

- citizen trust and risk perception,

- regulatory certainty & harmonisation,
- awareness (of both consumers and enterprises) and information about RFID,

Where applicable, the impact on third countries of the sub-option is assessed.

(c) For each sub-option, most relevant direct economic impacts, in particular on competitiveness, innovation, jobs, and SMEs are assessed in case they can be observed.

(d) For each sub-option, (a), (b) and (c) are combined to assess the overall impact of each sub-option on the speed of RFID deployment.

(e) A summary of broader economic, social and environmental impacts of RFID technology as such is provided in Section 5.5, indicating what benefits and disadvantages a faster speed of deployment would bring for Europe as a whole. The impacts of RFID technology include:

- *economic impacts:* competitiveness of EU industry, internal market and competition, sector benefits,
- *social impacts:* employment impacts, privacy and security, public health,
- *environmental impacts:* waste production, recycling, …

As far as possible the assessment attempts to provide quantitative data. However, in some cases concrete figures are difficult to obtain as RFID is evolving very rapidly, both in technology and costs terms, and because B2C applications are still mostly in a trial phase (i.e. uncertainties as to the actual cost of wide scale deployment exist).

5.2. Assessment of impacts of the content options on prior assessment requirements

5.2.1. Option I.a – no change on prior assessment requirements

5.2.1.1. Description

Under this option, RFID application providers are not requested to conduct any type of privacy or security assessment prior to the deployment of an application. Experience in information security shows that generally, businesses tend to mitigate the risks and assume the related associated cost that have a direct impact on them but not the indirect ones (the so-called externalities). The former will be addressed but the later will be transferred to the user of the product or service who will then assume the risk and the cost alone.

Businesses will continue implementing currently ongoing initiatives. Sectorial associations are likely to create codes of conduct which will include some best practices and guidelines to follow on privacy and data protection. However, a risk exists under this option that the industry in different Member States will set own rules which will differ from each other.

5.2.1.2. Costs

Seen from a narrow view, immediate costs are nil to the RFID application providers as they do not need to conduct any assessment. However, any costs resulting from the use of the application where this will have had an impact on privacy, data protection or information security will have to be incurred by the user.

Under the economic concept of a "cheapest cost avoider", when the cost to mitigate the risks faced by customers is lower to businesses than the cumulative cost to customers, businesses should be responsible to implement those measures.

5.2.1.3. Benefits

Trust. As experienced in earlier trials of RFID technology[40], it cannot be excluded that privacy and/or security breaches due to non-assessed risks (or simply the fear of them) drive affected individuals away from the technology and affect in return the uptake of the technology.

Harmonisation. A lack of harmonisation at EU level can be expected as some MS will likely head towards tighter requirements that might as well affect the proper functioning of the internal market. By not encouraging privacy/security assessment, the private sector itself is likely to adopt different approaches when addressing those questions.

Awareness. Not conducting any type of assessment would contribute negatively to rising awareness on the technology among SMEs as those would loose the occasion of learning the lessons from the larger players.

5.2.1.4. Direct economic impacts

As indicated above, the lack of consumer acceptance towards the RFID technology, which is likely to occur under this scenario, might hinder the innovation and take up of the technology.

5.2.1.5. Overall speed of deployment

The speed of deployment is likely to remain, at best, the same as of today. In the worse scenarios, a few poorly thought applications (in privacy, data protection or security terms) might negatively impact the perception of the technology among the citizens and slow down the use of RFID in B2C applications.

5.2.2. Option I.b – Privacy and data protection impact assessments and security assessments

5.2.2.1. Description

The same way organisations typically evaluate a series of factors before deploying a new application (financial or technical feasibility), this option would include the recommendation for organisations to run a privacy, data protection and a security assessment (PIA) before deploying their RFID application. While security assessment is nowadays well integrated in an overall risk management approach, privacy implications tend to be more disregarded.

[40] See 'RFID & Identity Management in everyday life' – European Parliament's Scientific Technology Options Assessment entity (STOA)

The privacy, data protection and security implications of RFID applications are not always evident and preparing an impact assessment prior to their development is generally seen as an effective way to understand those implications[41] and proactively act on them.

In practical terms:

- because security, privacy and data protection are closely connected, the respective assessments should be at least carried out in a coordinated manner, and preferably done at once;
- while all RFID applications are affected by security, not all are affected the same way by privacy and data protection. A PIA should therefore be flexible so that any type of application is assessed with the appropriate depth. For example, a stepwise approach should be envisaged, where a sort of high-level impact assessment determines the level of depth of the actual assessment. This would limit the costs associated with the exercise;
- PIA could form an input for future codes of conduct;
- it is important to note that the option would apply to all applications, regardless of the sector or the type of affected individual (worker, consumer, etc).

Privacy, data protection and security assessments are prerequisites for determining the most appropriate measures to counter the assessed risks. Guidelines that contain technical and organisational measures throughout a given sector/application could be considered as a supporting instrument to ensure privacy and security by design. They could also form the basis to demonstrate that an appropriate level of privacy and security is established. The existing early experience with PIAs seems to confirm this statement[42].

5.2.2.2. Costs

For security assessments, the cost of including them in the recommendation is close to zero as this type of assessments is usually conducted anyway as part of good business practice.

For privacy and data protection assessments, they can either be included as part of the security assessment, provided it is conceived as such, or can be done as a separate assessment. Unfortunately, the information on their costs is scarce. However, domain experts generally agree that they bear close similarities with an Environmental Impact Assessment (EIA)[43] in terms of methodology as this type of assessment also identifies the potential risks ex-ante and proposes the most appropriate mitigating measures.

According to a study on the costs and benefits of EIA[44], most represent a cost inferior to 0.5% of the total project costs and tend to be lower as capital costs are higher. It should be noted here that EIA are regularly performed for (large) infrastructure projects which can have a significant capital cost outlay. EIA costs ranged from €80.000 to over 1.5 million € for very large projects. In the case of PIAs for RFID applications, the expected cost will certainly be

[41] Additional information on existing use of PIAs and security is provided in Annex 3.

[42] See Loughborough University et. al. (2007) *Privacy Impact Assessments: International study on their applications and effects.*

[43] See Directive 85/337/EEC as amended by Directive 97/11/EC and Article 3 of Directive 2003/35/EC.

[44] EIA – A study on costs and benefits (1996) IISBN 92-828-3572-3. See http://ec.europa.eu/environment/eia/eia-studies-and-reports/eia-costs-benefit-en.htm.

lower than that but the range is foreseen to be very wide, ranging from small amounts for off-the-shelve applications where RFID are not handed to individuals (e.g. tags monitoring the pipe temperatures of an air conditioning system) to larger amounts for large first-time deployments that include individuals receiving tags that contain personal data (e.g. smartcards that contain health records). While the upper limit is hard to evaluate, costs for a PIA could be as low as 50€ for simple applications.

It should be emphasised that the EU standard cost model for calculation of administrative burdens cannot be applied as relevant data on the cost of privacy impact assessments are not available at this early stage of RFID deployment. The Recommendation could envisage the establishment of an appropriate 'framework' for PIAs (within the first 24 months), which will be done together with the industry and relevant authorities. The cost of an individual PIA will therefore also depend on how this framework is ultimately defined, what kind of RFID applications will be used, etc. Such data will be collected in the process of the future monitoring and evaluation (see section 6) when more reliable cost data are available.

5.2.2.3. Benefits

Trust. By showing that privacy and security risks are considered prior to deploying an application supported by RFID, RFID operators will contribute to higher perceived consumer trust in the application in focus and in the technology at large.

Harmonisation. Privacy, data protection and security assessments are expected to be welcomed by Member States as this measure is easy for organisations to adopt, presents benefits for the affected individuals and is flexible in its approach.

PIAs will have, in the longer run, a positive impact by promoting the development of codes of conduct. When the same specific application is deployed many times, PIAs are likely to be highly similar. It is therefore likely that the concerned industrial sector and/or the RFID industry will see an interest in harmonising and expediting the individual PIAs by developing a code of conduct that would serve as an umbrella for the deployment of the application, therefore reducing the work related to the development of PIAs.

This will create additional regulatory certainty, which in turn will have a positive impact on the speed of deployment for RFID applications that fall under the code of conduct.

Awareness. By disseminating the results of the privacy aspects of such assessments, operators will contribute to raise awareness among citizens and SMEs. In particular, SMEs will benefit from the knowledge and experience generated by large companies which are expected to deploy their applications first.

5.2.2.4. Direct economic impacts

Obliging RFID application operators to carry out PIAs prior to deploying an RFID application could be seen as a barrier that would delay market entry for RFID applications having thus a negative impact on competitiveness. Similarly, there is a risk that putting extra burden on operators innovation could be affected in the negative sense. This could have an impact in particular on SMEs.

As indicated in the section 5.2.2.2 on direct costs, this option would also increase costs, and in the result prices, of services and products to consumers.

Depending on the size of the project and the complexity of the application, this option could contribute as well to the creation of high quality jobs for workers with expertise in privacy and data protection law.

5.2.2.5. Overall speed of deployment

Despite some initial time investment in developing the framework, the assessments, enforcing PIAs and promoting existing security assessments should become quickly beneficial for all: 1) individuals because they will gain trust in the technology, and 2) businesses, because their applications are secure and perceived as such by consumers.

5.2.3. Option I.c - Certification by authorised third party organisations and/or public authorities

5.2.3.1. Description

Under this option, RFID applications would have to be third party certified against some privacy and security criteria. This option implies the creation of a new or the designation of existing third parties to provide such certifications. For example, certifying the information security management system of the RFID application provider (according to ISO/IEC 27001) could be seen as one possibility; while National Data Protection Authorities (NDPA) have their mandate extended to include being notified of new RFID applications (privacy aspects).

As another example, the German BSI[45] is developing several Technical Guidelines for RFID applications that contain technical advice on how to implement a system in a secure, functional and economically viable way and deals with issues such as privacy, information security and (system) safety. In the future, BSI (and probably other accredited facilities) will offer a **certification service** for implementations that follow the guidelines.

5.2.3.2. Costs

Evaluating the costs of this option includes:

- The cost to establish those guidelines. In the BSI example, the costs of developing a single guideline for a specific RFID application varied from 50.000 to 100.000 €.

- The costs for companies to be certified. Those are strongly related to the complexity of the certification process and whether it includes mainly an organisational audit or also technical tests. Assuming a certification is comparable to an ISO 9000 certification, a single audit may costs some 1500-2000 €.

As in the previous case of PIAs, more detailed data on the specific costs of Option I.c are not available and cannot be collected as such certifications are currently not in place and RFID is still in the early stage of deployment. It can be however safely assumed that the cost of the certification process would be higher than the cost of PIAs.

[45] The Federal Office for Information Security in Germany.

5.2.3.3. Benefits

Trust. Having independent third party organisations or authorities certifying RFID applications for security and/or privacy friendliness, like done for environment or quality, has the potential to improve trust and acceptance from citizens.

Harmonisation. One of the barriers for RFID adoption is the lack of knowledge of the technology and the different approach adopted by different vendors when tackling a given business case. Certifications should contribute to harmonising the approach, create more competition among vendors and offer an easier approach to SMEs.

Awareness. The establishment of guidelines for certification would contribute to the dissemination of the knowledge of the RFID technology, particularly to SMEs.

5.2.3.4. Direct economic impacts

As is the case with option I.b, this option would create additional barriers and impose costs on companies willing to provide on the market new applications. These costs would have been assumed by consumers in prices of goods and services.

5.2.3.5. Overall speed of deployment

While the development of those certifications might take initially some time, development of guidelines should in the medium term support a faster deployment of the technology. They would serve in two directions: firstly to guide RFID application providers in particular SMEs to implement appropriate privacy and security measures; secondly to serve as a baseline for demonstrating that an appropriate level of privacy and security is established either through self-declaration or independent certification.

At this stage of the development of the technology, enforcing this measure for all type of RFID applications seems to be too early as such certification services are not available on the market so far. It is likely to significantly delay the uptake of the RFID technology in Europe until such certification procedures are put in place. However, certifications bring some benefits, for example stronger harmonisation or a citizen trust perception, and could be encouraged (but not enforced) for those sectors where a critical mass of applications exists (e.g. e-ticketing, access control).

5.2.4. Comparison of sub-options I.a, I.b & I.c.

		Sub-Option I.a	**Sub-Option I.b**	**Sub-Option I.c**
Costs	Cost of implementation	0 Immediate costs would be negligible	- Establishing guidelines to create PIA and have them executed has a certain cost	-- Establishing third party certifications has a higher cost than a PIA
Benefits	Citizen trust and risk perception	- - No benefits, but citizen trust would be heavily affected should a major privacy or security breach occur	+ + By showing that privacy and security risks have been taken into account, operators will create trust among citizens	+ + An independent authority certifying risks should create trust among citizens
	Regulatory certainty,	-	+	+ +

	harmonisation	No benefits – but there is a risk that Member States establish their own requirements	PIAs are expected to be welcomed by Member States who would not add further rules	Independent authorities, provided they work together, should be able to secure a good level of harmonisation
	Awareness (both citizen and SMEs) and information about RFID	- / 0 No impact is expected on this aspect (provided no major privacy breach occurs)	+ + By making public the result of their PIA, operators would greatly contribute to the technology awareness raising	+ The existence of a trusted certifying body would contribute to disseminating technology awareness.
Direct economic impacts		0 No immediate impacts on competitiveness, innovation, jobs SMEs	+ Creation of specialist jobs	0/- Potential negative impacts on SMEs through high costs of certification
Speed of deployment of RFID		- - / 0 Speed of deployment would depend on how much it would be affected by the lack of harmonisation and by eventual privacy/security breaches	+ The time spent in establishing Impact Assessments would be balanced by the improvements in the deployment quality of applications.	0/+ Establishing third party certifications and disseminating them across the industry would take several years but will ease deployment of applications.

Conclusions:

- **<u>I.b > I.a.</u>** Based on the above table, it appears that I.b, despite some additional costs, is overall more beneficial than I.a and should therefore be recommended.
- **<u>I.c is still valid.</u>** I.c which can coexist with I.b, is as well interesting but presents some delays and cost related drawbacks if made mandatory and should therefore only be encouraged.

5.3. Content options on requirements related to information and communication

5.3.1. Option II.a – no change on requirements related to information and communication

5.3.1.1. Description

Under this option, no recommendation related to information to be provided to individuals is included. The Data Protection Directive would still oblige data controllers to provide certain information to data subject if their personal data is processed. RFID application providers would decide on a case-by-case situation which information, if any, they will disclose to consumers on the purposefulness of the use of RFID tags in their applications, and to what extent they aim to process personal data.

5.3.1.2. Costs

As with option I.a, this option bears no costs for the industry but this apparent freedom might turn to be counter-productive if companies fail to demonstrate their good will so that a minimum level of citizen trust in the technology is not reached and/or it is done at the expense of the internal market.

5.3.1.3. Benefits

Trust and awareness. One recurrent theme coming from individuals and civil society organisations, such as privacy groups, workers' unions, consumer organisations, is the fear of the existence of some 'secret databases' that carry out 'hidden' operations with data about individuals. Not providing information on how RFID is used at all, or providing such information in an unorganised way, is likely to have an adverse effect on trust and awareness.

Harmonisation. In the absence of any requirement beyond the Data Protection Direction, there is a risk that RFID application providers will not inform individuals or will inform in different manners: sometimes along sector-specific non-binding guidelines (such as EPCglobal ones in the retails sector) and sometimes in an uncoordinated manner.

5.3.1.4. Direct economic impacts

Under this baseline option, direct impact on jobs, innovation, and competitiveness seem to be negligible.

5.3.1.5. Overall speed of deployment

Under this sub-option, the overall speed of deployment is expected to be stable as long as an eventual lack of harmonisation does not cause any problem and as no major trust breach happens.

5.3.2. Option II.b - A written information policy

Under this option, RFID application operators would be recommended to develop and disseminate a written information policy governing the use of their RFID application. This measure is without prejudice to obligations resulting from the Data Protection Directive.

The recommendation would state the following minimum information to be provided to the public:

– the identity and address of the RFID operator;

– the purpose of the RFID application and intended data processing,

– which data are collected and if the location of tags is monitored,

– which link, if any, is made to personal data,

– a summary of the impact assessment including the likely privacy risks, if any.

A related question is whether this requirement should apply to all RFID applications or be limited in scope, for example only to those applications deployed in public areas (public transports, museums, supermarkets, etc). By doing so, this information requirement would be lifted for most intra-company applications where the public has no access (e.g. a logistic warehouse that uses RFID to track its parcels). In this example, the only individuals in contact with the RFID technology would be employees of the company. While such information might sound legitimate, one can as well assume that such a requirement is already part of the information/training that employers need to provide to employees to perform their work.

Another possible limitation in scope would be to limit application of this measure to those that process personal data. In this case however, it must be noted that if the data is considered personal, information requirements already exist under the Data Protection Directive and that, by doing so, the underlying objective of informing and re-assuring individuals would be largely jeopardised.

5.3.2.1. Costs

The **cost impacts** of this information provision are mainly related to the design and dissemination of the information material. This is mainly a non-recurring expense for application providers, though it may require regular adjustments/updates. Depending on the size of the organisation this may range from € 500 to several thousand euro per location.

For small scale RFID operators, such as small retail outlets, these costs may still be relatively high. For these actors it is sensible to develop standard information brochures, either by their suppliers or by SME associations in Member States.

In addition to the information material, RFID operator's staff who are in contact with individuals, would have to be trained to answer related questions. This cost could be estimated at a few hundred Euro per person to be trained.

To enhance the effectiveness of information, it would be advisable to carry out a wider **awareness and information raising campaign** on RFID, organised by a public authority or a large private initiative. A specific element could be to develop a neutral reference website at a European or Member State level.[46] The Commission could play a clear role in this respect[47]. The costs involved in such an information campaign depend very much on the scope and depth. For example, the highly intensive information campaign on the introduction of the Euro cost € 80 million[48]. A more light footed information campaign in all Member States including the establishment of a central website and the central publication of information material should be possible with a budget of several million euro.

5.3.2.2. Benefits

Trust and awareness. The provision of concise, adequate information can be an important factor to increase trust and awareness. This will take place only if the information is considered to be trustworthy, factual and not misleading.

Harmonisation. The written policy would state minimum requirements on which Member States could add additional information should they feel the need. This is a common way of specifying requirements, and Member States are not expected to add that many requirements that would make the written policy too different from country to country.

5.3.2.3. Direct economic impacts

Companies might not be willing to provide information concerning which data are collected by means of readers and the purpose of the RFID application and how their applications

[46] This could for example be a joint initiative of CEN (the European Committee for Standardisation)/ETSI and Working Party 29 to be able to give both factual technical background information and information of privacy rights and obligations.

[47] e.g. cf. the role of the Commission with respect to the Denied Boarding Regulation in the aviation sector.

[48] www.ecb.int.

process data collected as this is part of their business know-how. Once revealed to the public, this knowledge could be used by competitors. A risk exists that this could have a detrimental effect on innovation. A balance must be thus sought between publishing such an information policy to enhance consumers trust while avoiding disclosing sensitive, application-specific information that can be misused by other parties.

Direct impacts in terms of workforce can be negligible for this sub-option.

5.3.2.4. Overall speed of deployment

The promotion of individuals trust, especially in combination with an increased level of awareness of both citizens and businesses, is expected to have a positive impact on the speed and level of RFID deployment, which subsequently leads to increased economic, environmental and social impacts associated with RFID (see next chapter).

5.3.3. Option IIc – Option IIb + the use of logos and identifiers to indicate the presence of RFID

5.3.3.1. Description

In addition to a written policy (described in the previous section), RFID operators could be requested to indicate the presence of RFID technology itself through the use of logos. Those can be used to indicate:

– the location of tags,

– the location of readers,

– the area in which RFID technology is used to collect and process data.

Tag level. The main rationale for placing logos on RFID tagged objects is to make individuals, including consumers and citizens, aware of the presence of the tag in the labelled object so that they could behave accordingly. However, a question is whether using a unique logo for any type of RFID tag (therefore easy to understand/remember by individuals) and using different logos to represent the different reasons for which a tag can be attached (a tag tracking a bottle of water along company internal supply chain processes and a tag carrying biometric information in a passport serve different purposes, are different technologically, etc).

For this reason, using a logo on all tags seems to be counter-productive, and, hence, this option would entail only placing logos on retail products as technology and purpose are usually very similar. Furthermore, it is worth noticing that labelling of tagged items is already endorsed by the retail sector and is therefore already commonly applied[49]. Another question is what type of labels should be applied as these can be different: adhesive (a sticker on the product itself,) or printed on the package (e.g., carton).

Reader/zone level. Placing logos on readers seems most appropriate at first sight but presents problems that lead to discard this solution:

[49] See Guidelines on EPC for Consumer Products at http://www.epcglobalinc.org/public/ppsc_guide/.

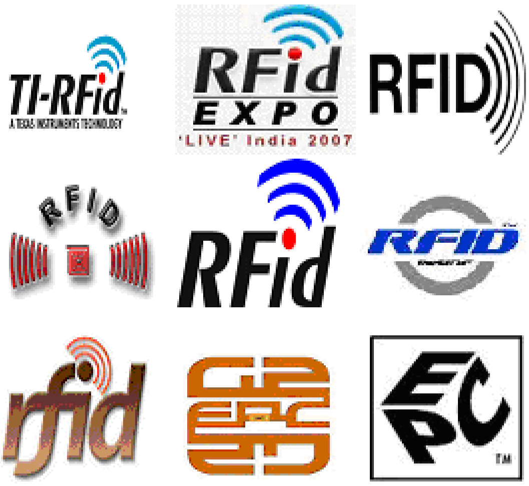
– Readers are not always visible (they can be hidden behind a soft-wall) or are embedded in other items (e.g. cell-phone).

– The objective of putting a logo on readers is not clear: what matters for individuals is to be aware that they are entering a 'RFID-read' zone rather than knowing where readers are individually placed.

For those reasons, it seems that the logos indicating the presence of RFID readers in a 'zone' (e.g. stickers at the entrance of a sub-way station) is the best suited solution, addressing the 'information' question while avoiding proliferation. This would operate the same way as CCTV presence is indicated at the entrance of the concerned area but not all cameras are then labelled.

In order to enhance harmonisation and avoid confusion, a standard logo should be applied. At ISO level, a proposal for such a logo is currently being evaluated. Alternatively, the European industry seems willing to endorse its own logo or a European Standardisation mandate could be used. Figure 5.1 shows a sample of logos developed to date by the RFID industry.

Figure 5.1. Examples of RFID logos already in use.



5.3.3.2. Costs

Tag level. The costs of tag labelling can appear to be high at first sight as they represent a change in product label. These costs will vary according to the label type which can be either adhesive or on-pack For example, previous policies regarding changes in product labelling reveal that the mandatory nutrition labelling in the EU is estimated to be between 2k€ and 9k€per product line[50]. This cost is however to be put in perspective when considering that 1- the cost of the tags themselves is largely higher (re-labelling is a one-time cost, while the tag is a recurrent cost) 2- the marginal cost for such a change in label is close to zero for existing tagged products as a vast majority of retail products that are currently tagged are already labelled.

Zone level. The cost of logos for RFID zones is relatively modest and can be compared to the cost of disseminating information (see previous section), particularly if logos are harmonised. The Commission will monitor the actual cost of implementation of logos and written

[50] See EAS (2004), Impact Assessment on the Introduction of Mandatory Nutrition Labelling in the EU (commissioned by DG SANCO).

information policy and will provide a more detailed assessment of these costs at the next review of the recommendation (see Section 6 Evaluation and monitoring)

5.3.3.3. Benefits

Trust and awareness. As with the written information policy, the use of images and logos to indicate to individuals that they are entering a RFID area and to consumers that they are purchasing a tagged product will support the transparency and communication of RFID to the public. Both measures complement each other, aim for the same goal and address the information need if used in combination.

Trust in the technology and its development work as a virtuous cycle: creating trust allows further RFID deployment; deploying while addressing individual fears creates trust in return.

Harmonisation. When introducing identification signs, there's a potential risk of seeing the development of different logos. However, in the RFID case, a proposal for such a standard is already being examined at ISO level and, alternatively the European industry is willing to develop a unique logo (or set of logos).

5.3.3.4. Impact on third countries

Companies of third countries that export retail products to the EU would be subject to the same type of obligations as companies within Europe and would have to indicate the presence of tags in their products. This will increase the cost of production and labelling for the European market, unless similar obligations are introduced also in third countries.

5.3.3.5. Direct economic impacts

On top of the direct economic impacts of the option II.b, this option puts additional non-negligible costs on producers of all kinds of RFID-tagged products that are intended for the retail market.

5.3.3.6. Overall speed of deployment

This combined sub-option (policy + logo) is by nature complete and coherent. The speed of deployment should even be improved compared to option II.b as endorsing logos on retail products is only confirming the industry initial guidance on this respect and adding signs to indicate RFID 'zones' does not constitute a time factor.

5.3.4. Comparison of sub-options II.a, II.b & II.c.

		Sub-Option II.a	**Sub-Option II.b**	**Sub-Option II.c**
Costs	Cost of implementation	0 Immediate costs would be negligible	- Costs are limited as a written policy is a one-time limited cost	- Cost for item-labelling are limited and already planned by the industry while zone-labelling is a limited one-time cost

Benefits	Citizen trust and risk perception	- - No benefits expected. Citizen trust would be heavily affected should a major privacy or security breach occur	+ By adopting an open and transparent attitude, operators will create trust among citizens	+ + On top of the written policy, indicating the presence of tags in retail products would be additionally beneficial from a trust point of view. The signs at the entrance of a RFID zone complement this mechanism adequately.
	Regulatory certainty, harmonisation	- - No benefits. There is a risk that Member States establish their own requirements	+ The written policy would state minimum requirements on which MS could add additional information should they feel the need	+ + On top of the written policy, using an existing logo or designing one at EU level seems is feasible.
	Awareness (both citizen and SMEs) and information about RFID	- / 0 No impact is expected on this aspect (provided no major privacy breach occurs)	+ Awareness, especially among individuals, would be very large	+ + Awareness, provided the logos are well introduced, would be large and immediate, and once again complements the written policy very well
Direct economic impacts		0 No effects.	- Potential negative impacts on competitiveness	-- Further negative impacts on competition through extra costs for product labelling
Speed of deployment of RFID		- / 0 Speed of deployment would depend on how much it would be affected by the lack of harmonisation	+ By improving trust among individuals, the deployment speed of RFIDs could be enhanced	+ + By reaching higher levels of trust and acceptance among individuals, the deployment speed of RFIDs could be further enhanced

Conclusions:

- **II.a is not favoured.** This option has major drawbacks that neither the industry, nor the civil society is willing to accept and the former have already started implementing the other solutions.

- **II.b** constitutes a first step in terms of information to be provided to individuals. While the overall impact of this measure is positive, it is lower than II.c.

- **II.c**, by combining the written policy and the use of logos, is likely to have the best impact in terms of deployment speed for a cost that would only be slightly higher than II.b. Furthermore, this approach has already endorsed by the industry, although not harmoniously (different logos, etc).

5.4. Content options related to the retail sector

5.4.1. Introduction

Retail is, by large, the sector on which the RFID debate has focussed the most. In particular consumer organisations have been echoing concerns, partly based on unsuccessful trials from the industry[51].

Item level tagging is the tagging of the smallest unit of things that can be tagged – the piece of apparel, library book, jewellery, engineering parts, and laundry are examples. The item level RFID business is expected to rise from $250 Million in 2008 to more than $8200 Million in ten years. Currently, item level tagging only exists on high value goods with a fast turnover, such as DVDs, retail apparel or computer video games.

The essentials for any successful retailer are: buy at the best price, promote and merchandise to expectations, lower costs in the store, and quick and efficient check-out for the customers. RFID technology enables retailers to synchronise all the basic essentials and automate critical store functions – control inventory flow, combine in-store and back-office virtually to enhance productivity, track customer purchases, control back-office and retail floor simultaneously, inventory and price checks on floor. Some of the recognised retail chains (e.g. Wal-Mart and Albertsons in the U.S., METRO Group in Germany, Carrefour in France) have been testing RFID technology since 2003-2004 with pilot projects now starting to show tangible benefits across the supply chain – labour efficiency, Out-of-Stock management, inventory management, receiving shipping accurately, reduced claims, product recall management, and reduced shrinkage, improved dock and truck utilisation, improved product traceability, precise recall capability. More and more retailers consider that RFID technology can be a catalyst for change. Automated and enhanced store processes supported by a common store infrastructure solution can help them transform their stores into *sense-and-respond* environments. Data gathered from tag/reader interactions can be integrated into store applications and processes to allow dynamic changes. They can access a real-time view of product, operational and customer-profile data across your operations — from the warehouse to the point of purchase and beyond.

5.4.2. Statement of the issue

The central issue in the retail sector is what to do with RFID tags when a product is sold. Item level tagging has the potential to become a mass market application and therefore will affect a huge number of individuals whose *personal data*[52] are possibly going to be processed each time they acquire a product to which a RFID tag is affixed. To understand this issue, it is important to define the following:

- **Deactivation** is the physical process or software command that causes the cessation of any functionality from a tag[53].

[51] 'RFID & Identity Management in everyday life' – a report of the European Parliament's Scientific Technology Options Assessment entity (STOA). Available at: http://www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf.

[52] On the concept of "personal data", see Opinion 4/2007 of the Article 29 Data Protection Working Party, adopted on June 20th 2007 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[53] CEN TC225 RFID Ad Hoc.

- **'Opt-in'** refers to the default deactivation of tags unless the consumer provides the RFID operator with a freely given, specific and informed consent that s/he wants to keep them active. This will be applicable in many cases; however there are further criteria for making data processing legitimate under the Data Protection Directive. Because this option includes a conscious decision by the consumer, it is usually referred as 'Opt-in'.

- **'Opt-out'** refers to maintaining the tag active by default unless the consumer wants to deactivate it.

Therefore, in an ‘opt in’ regime the explicit consent of the involved subject is an indispensable prerequisite for the collection of individual-related data and the linkage with other data sources. More concretely, it means that the retailer has to deactivate the RFID tag at the point of sale unless consumers that so desire, expressly ask for tags to remain operational.

In the case of an 'opt-in' regime, putting a system at a retail company's checkout to disable the RFID tags has the following main consequences:

- buy the hardware equipment to be installed at each checkout;

- buy and/or develop a software application to disable the tag;

- install the new solution in each store and every checkout;

- handle the physical integration of RFID readers, antennae and controllers in the existing checkout, which can be a complex process because space is limited;

- train the cashier;

- include maintenance services on new hardware and software equipments;

- administrate the solution to monitor the good health of the RFID infrastructure, have people able to support store (helpdesk, remote access, on-site assistance...) with new and appropriate tools;

- adapt the interaction and relationship with other applications (like loyalty, payment).

On the contrary, in an opt-out scenario, the consumer has to ask for the tag to be deactivated – individuals are included in RFID data collection by default, but offered the option of removing themselves. In this case, the roll out of the "deactivators" includes the main following tasks:

- buy the equipment, both hardware and software;

- develop the application;

- install and integrate the solution in the stores;

- train staff;

- include maintenance services on the equipments;

- administrate the solution to monitor the good health of the RFID infrastructure and have people able to support store (helpdesk, remote access, on-site assistance…) with new and appropriate tools.

5.4.3. Views of major stakeholders on deactivation of tags

The public consultation which the European Commission launched in February-April 2008 resulted in 637 valid responses including 403 (63%) from non-citizen stakeholders (RFID systems industry, RFID using industry, Telecommunications, RFID consulting industry, academic organisations, governmental organisations, labour organisations, non-governmental organisations, international organisations).

As regards the issue of the use of RFID in Retail, and more specifically the impact of mandatory deactivation of tags at point-of-sale (POS), international retail organisations have responded to the public consultation and provided their detailed analyses.

5.4.4. Opinion of the European Data Protection Supervisor (EDPS)

The European Data Protection Supervisor[54] (EDPS) indicated in its Opinion of December 20th 2007 that maintaining tags active if personal data is being processed[55] would be unlawful unless the data controller has the appropriate legal grounds to do so (usually consent of the data subject, or based on other criteria that makes data processing legitimate as enshrined in Article 7 of the Data Protection Directive).

> *"For all relevant RFID applications, <u>solutions should respect and implement</u> as a prerequisite, an opt-in principle at the point of sale. Enabling the RFID tags to continue transmitting information after the point of sale would be unlawful unless the data controller had appropriate legal grounds. Appropriate legal grounds would normally only be (a) the consent of the data subject or (b) if such disclosure was necessary in order to deliver a service, a specific and free request by the said individual. Both legal grounds would then qualify as 'opt-in' (…)*
>
> *In order to cope with the growing diversity of RFID applications and to facilitate the development of new innovative business models, the EDPS stresses the importance of a flexible approach. Flexibility has to be provided as to the implementation of the opt-in principle (…)*
>
> *To conclude, although the EDPS argues that <u>the 'opt-in-principle' at the point of sale is a legal obligation that already exists under the Data Protection Directive in most situations</u>, there are good reasons to specify this obligation in self-regulatory instruments, also in order to ensure that the principle will be implemented in the most appropriate way."*

Furthermore, several industrial stakeholders argue that deactivation or removal of an RFID tag should only take place where personal data is <u>in the tag</u> itself, the EDPS puts forward a more sophisticated approach:

[54] See Opinion of 20th December 2007, paragraphs 46 to 50.

[55] A privacy impact assessment discussed in option I.b should provide more guidance as to whether personal data is processed by the specific RFID application or not.

- RFID tagging has consequences for the owners of items (e.g. consumers) who should not be subject to the process of adverse automated decisions;

- the data stored in or produced by an RFID tag can be 'personal data' as defined in Article 2 of the Data Protection Directive;

- even if the information stored in the RFID tag would not include names of individuals, RFID tags contain unique IDs attached to consumer products, and such identification can be used for surveillance purposes (e.g. of someone wearing a watch that carries an RFID tag); in this context, it is necessary to ensure that RFID applications are deployed with the necessary technological measures to minimise the risk of unwilling disclosure of information;

- the analysis of the impact on privacy of RFID systems offering the possibility to track products after the point of sale should take into account (1) how personal the item is considered to be, (2) the mobility of the item, and (3) the life cycle of an object.

5.4.5. By way of conclusion

The costs of physical removal or destruction depend on who executes the action: if the consumer does the operation (e.g. if the RFID tag is embedded in the price tag of a cloth), costs are close to zero for the retailer. If the retailer does it, the costs are proportional to the time it takes the check-out operator to remove/destroy the tag himself.

As can be derived from the information provided by the large retail companies, the costs of software deactivation originate from:

> 1- The cost of equipping the shop with the adequate readers to perform the deactivation. The number of such equipment would depend on the number of products to deactivate. It can be one for an entire supermarket if the number of concerned products is limited and goes up to one per cashier. The cost of single deactivation equipment varies largely from source to source. While the actual figure of the equipment seems to be in the range of 500€ to 1000€, the costs of integrating it with the back-office IT systems and physically at the cashier desk bring the cost up to 5-7k€/cashier.
>
> 2- The extra time readers need to perform such operation. Typically, a writing interaction would take very little time (<0.1s) and several tags can be deactivated in parallel. However, deactivating a full trolley is more difficult as tags could interfere in between them.

Several deactivation mechanisms exist but they can be grouped in two groups: the ones that physically destroy or remove the tag (e.g. like shredding the tag) and the ones that deactivate the tag through a specific tag/reader writing interaction (sometimes referred as a software deactivation or, abusively, as a kill command)[56].

5.4.6. What are the options?

The public consultation launched in 2008 plus the numerous contacts the European Commission had with key stakeholders covering the technological, economic, social, and

[56] For more information on modalities of deactivation, refer to Annex 5.

legal perspectives have shown that the fundamental options for the deactivation of RFID tags in retail stores in Europe are not 'opt-in' and 'opt-out'. Since the 'opt-in' principle has been set by the EDPS as "a legal obligation in most situations", the available options for its implementation actually depend on the scope of the "flexible approach" which the EDPS invokes in paragraph 48 of its Opinion.

It is essential to acknowledge that the protection of the rights to privacy and data protection within the European Union is guaranteed by a legislative framework consisting of:

- the Data protection Directive 95/46/EC, and
- the ePrivacy Directive 2002/58/EC.

The Data Protection Directive applies to RFID as far as data processed by RFID systems fall within the definition of 'personal data'.

The ePrivacy Directive is limited to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks. When devices such as Radio Frequency Identification Devices (RFID) using radio frequencies to capture data from uniquely identified tags, are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC, including those on security, traffic and location data and on confidentiality, should apply.

The options for the use of RFID in the retail sector are therefore the following:

- implementation of the 'opt-in principle' with no additional requirement in retail environments beyond existing legal requirements,
- implementation of the 'opt-in principle' for all situations, including those not covered by the existing legal framework,
- implementation of the opt-in principle' with some level of flexibility.

5.4.7. Option III.a – Implementation of the opt-in principle with no additional requirement in retail environments beyond existing legal requirements

5.4.7.1. Description

Under this sub-option, no additional measures to the retail sector would be included in the Recommendation and the existing legal framework would apply. The recommendation would simply limit itself to provide a legal interpretation in case that personal data is processed (i.e. opt-in solution is recommended). If a retailer does not process personal data, he would have no obligation, not even to deactivate the tag upon request of the consumer. If the consumer wants to deactivate the tags, he would then have to choose in between: buying an untagged product elsewhere or deactivating it by its own means.

5.4.7.2. Costs

Cost impacts are hard to assess under this scenario. On one hand, it places no new requirements on the industry (implying zero marginal costs) but, on the other hand, it disregards the benefits that would originate from the higher consumer trust. Some consumer/privacy organisations are very vocal about deactivation and have, in the past, been up to block the entrance to supermarkets. In this case, the cost analysis should include the damage made to the brand, etc. Also, as the applicability of the data protection framework may sometimes be difficult to assess ex ante, (successful) legal challenges of certain practices being in breach of data protection legislation could add further costs.

5.4.7.3. Benefits

Trust. Not including further provisions would fail to address the concerns that consumer organisations have been voicing since several years and a potential major back-lash of the technology as a whole cannot be excluded.

Harmonisation. Furthermore, early signs show that several Member States could adopt conflicting measures justified by consumer protection that would hamper the Internal Market. For example, one MS could decide to force deactivation at the point of sale, others to make it optional and others to prohibit the presence of tags in retail products. In a European Community where retail products are often manufactured in one country and then distributed across MS, this would imply manufacturing different versions of the same product which is direct contradiction of the Internal Market.

Awareness. Awareness would obviously be at best neutral but could possibly be high, although carrying a negative message.

5.4.7.4. Direct economic impacts

Little or no direct impacts are expected from the implementation of this option as it will not increase legal certainty nor directly address the concerns of consumers. Therefore, controversy between industry and consumers' organisations will continue regarding the interpretation of the Data Protection Directive – e.g. is there an issue only when personal data is in the tag or, more broadly, where a link can be established between the information in the tag and the identity of the consumer – and retailers, both large companies and SMEs, would hesitate to invest in the technology.

5.4.7.5. Overall speed of deployment

The overall effect on the speed of deployment would depend how far the consumers would complain. However, when not even an opt-out mechanism is proposed, only a very little minority can become very vocal and create a lot of bad press for the technology as a whole. Based on anecdotic evidence, it seems that this minority does exist and that choosing this solution would largely undermine the technology in people's mind, possibly for long.

Additionally, it must be stressed that some retailers had chosen III.a several years ago but, due to communication problems with their clients, are now favouring option III.b. Should the EC choose III.a, it cannot be excluded that retailers interpret it as an incentive to be more permissive with consumer's privacy.

5.4.8. *Option III.b – Implementation of the opt-in principle for all situations, including those not covered by the existing legal framework*

5.4.8.1. Description

Under this sub-option, the opt-in principle would be extended beyond the existing legal requirement to RFID applications that do not process personal data.

5.4.8.2. Costs

For some type of products (such as cloth) which are usually protected against theft with apparent devices, tags would likely be removed manually. The process of removing both could be simultaneous and cost marginally zero.

However, as embedded tags become more common, deactivation will be software-based and imply additional costs to, in a first stage equip shops with a single deactivation booth and progressively all check-outs. In brief, the retail industry claims that a full opt-in scenario would modify the business case for tagging products at item level and would therefore stop this specific RFID use until either the requirement is lifted or technology is developed that will ease the process of deactivation (which is a 3 year perspective).

It must be noted that standard deactivation might lead to the slower development of new services after the point of sale. At this moment this mainly refers to reverse logistics and recycling, but other services might be developed in future.

5.4.8.3. Benefits

Trust. An extended opt-in approach is expected to have a higher positive impact on privacy, data protection and information security risks associated with the use of RFID in item level tagging as it can be expected that more tags will be deactivated. It also addresses a stated concern of consumers, thus it can be expected to increase **consumer confidence** in RFID. The public consultation by the Commission on RFID revealed that two-thirds of respondents were of the opinion that tags should be automatically de-activated at the point-of-sale. Also a recent consumer survey carried out in the Netherlands[57] showed a strong preference for an opt-in scheme, with 37% opting for an opt-in approach for all products and 25% preferring an opt-in system depending on the product involved.

De-activation is expected to increase consumer trust levels, which in turn can be expected to have a positive impact on the speed and level of RFID deployment, which subsequently leads to increased economic, environmental and social impacts associated with RFID (see Section 4).

Harmonisation. As such, the measure is expected to contribute to harmonisation. However, the measure can be perceived as very demanding by the retail sector and the possibility exists that some retailers, eventually backed by Member States, decide to go against it.

Awareness. Logically, the level awareness induced by this measure would be very high.

[57] Rathenau Institute, Consumentenbond, ECP.NL (2007), RFID awareness of consumers. How Dutch people think about RFID (in Dutch).

5.4.8.4. Direct economic impacts

According to information provided by all retailers, industry associations, the implementation of a full opt-in principle would imply very high investment and maintenance costs and neutralise any expected efficiency gains. Therefore, it is most likely at the present time that given the lack of innovative technology enabling consumers to deactivate and reactivate RFID tags, as they find it appropriate, the retailers will freeze, at least for some years, any plans to use and deploy the technology. The immediate impact on corporate profitability and on jobs should be marginal but in the longer-term (2-5 years) the impacts should be negative due to a loss of market opportunities and competitiveness compared to global non-European retailers.

5.4.8.5. Overall speed of deployment

The costs assumptions of the retail industry are hard to verify given the lack of transparency but the limited deployment of the technology at the moment and the technical difficulty to mass-deactivate tags at a checkout indicate that this approach would likely freeze for some time the item-level tagging of retail products (but would normally have no impact on applications that do not have privacy or data protection implications).

5.4.9. Option III.c – Implementation of the opt-in principle with some level of flexibility

5.4.9.1. Description

Under this sub-option, the opt-in principle would be applied to RFID applications, whether they process or not personal data, with some level of flexibility and due safeguards.

Against this background, the elements of flexibility that have been identified are the following:

- 'Useful' tags after the point of sale should remain operational. The problem is that the notion of 'usefulness' is largely subjective, hence hard to specify. The tag may have a primary role in the functioning of a product, i.e. "no tag = no product", for instance electronic car keys. The tag may have an important role in the functioning of a product, for instance RFID tags embedded in car tires to enable them to be tracked electronically or RFID tags to monitor the 'freshness' of a dairy product and help identify the source of contaminants. Finally, the tag may have a role beyond the initial functionality of a product, for instance faster after-sales service or improved product recycling. The solution is to assume that the consumer will, subject to receiving relevant and clear information beforehand, make by himself the appropriate choice, for example leave the tag operational if it is indeed useful for him.

- Following the completion of a privacy impact assessment, the tags that don't present any privacy risk, or no more than a negligible privacy risk (e.g. short life cycle of a product, RFID tags attached to 'swing tags' rather than directly to the item, use of a protective covering to the tag to prevent it from being scanned), would be deactivated only if the consumer requests it. In this case, however, information on the use of RFID will still need to be provided.

- In the case of a retailer not developing and/or using any specific RFID application but selling tagged products (the manufacturers having tagged their products for purely logistical purposes), the implementation of the opt-in principle obliges the private retailer either to implement a RFID deactivation system – even though he does not make use of RFID – or to depend on RFID application operators up the supply chain (e.g. the transport delivery companies or the distribution centres) to deactivate the tags before passing the goods to him or to provide him with the means to deactivate the tags. Such requirements are expected to be (a) particularly rigorous for small- and medium-sized private retailers having to deactivate the tags themselves and (b) impossible to implement for RFID application operators up the supply chain having to do the deactivation on behalf of the small- and medium-sized retailer – it is indeed not possible for the former to differentiate at the production level products to be sold to private retailers and to retail chains. Furthermore, the state-of-the-art deactivation technology does not allow to deactivate all types of tags with one device. The solution here is to consider that the retailer who is not an application operator should not be requested to take action (i.e. the tag remains attached to the product), provided that the privacy impact assessment will have beforehand detailed any potential risks for privacy and data protection. This element of flexibility implies that consumers willing to deactivate the tags have to do it by themselves. An alternative solution is to request that deactivation is done by the 'last active operator', thus providing maximum safeguard to the consumer, but the question remains open as to whether the implementation of this scenario is at all feasible.

5.4.9.2. Costs

While stating its clear preference for the implementation of an ‘opt-out’ approach implying the existence of a limited number of deactivation booths (likely located in between check-out and exit), the retail industry would respond favourably to the introduction of elements of flexibility in the implementation of an opt-in principle. Of course, the opt-in principle means the integration over-time of deactivation devices in every check-out, but the consideration of the ‘usefulness’ of the tag after the point of sale, the level of privacy threats as established by the privacy impact assessment, and the special treatment granted to those retailers that are not RFID application operators would still meet the essential privacy requirements while minimising the costs for industry. In conclusion, it should be stressed that the flexible opt-in scheme incurs lower costs for retailers than a full opt-in scheme.

5.4.9.3. Benefits

Trust. In immediate opposition to a strict implementation of the opt-in principle detailed before, it is likely that consumer trust will be lower under this scenario despite the possibility to request deactivation. Note that, while a full opt-in mechanism is expected to soon drive retailers to equip all checkouts with readers, under a flexible opt-in mechanism retailers that are also application operators are expected, at least for some time, to only make available one ‘deactivation booth’ likely located at the level of the checkouts. The level of trust among consumers is likely to be proportional to how smooth they can actually request such deactivation.

Harmonisation. The measure is expected to offer a compromise between, on one hand those Member States which view the opt-out principle as too permissive (consumer protection habits in Europe tend to be based on the opt-in principle) and could decide to implement a full opt-in mechanism anyway and, on the other hand, the other Member States which either view the opt-in principle as too costly for the retail industry or consider that it is premature to choose a mechanism at such an early stage of RFID implementations.

Awareness. Provided retailers fulfil the recommendation in good faith, i.e. by offering a good level of information and an efficient deactivation to those requesting it, the level of awareness should be similar to the opt-in approach.

5.4.9.4. Direct economic impacts

On one hand, the confirmation of the opt-in principle as a legal obligation deriving from the Data Protection Directive will lead active retailers in the European market to reconsider their early RFID deployment plans. On the other hand, the improved legal certainty combined with the flexibility provided in the actual implementation of the principle may encourage retailers to proceed further with their initial plans. The expected overall direct impact in the retail sector points at a limited slowdown, if any, in the implementation of new pilots. Increased legal certainty and consumer confidence may lead large retailers to be engaged into full-scale RFID implementations with some positive impact on market performance and jobs.

5.4.9.5. Overall speed of deployment

Should the technology exist to equip all checkouts with smooth deactivation functionality at an affordable price, option III.b would certainly be the preferred one. However, under current technical possibilities, option III.c is arguably the only one which is cost-effective, despite not offering the same level of benefits. For this reason, at this stage, the best compromise is to:

- Remind the legal obligation of opt-in when personal data is involved,
- Indicate a preference for an overall opt-in mechanism,
- Permit a flexible implementation of the opt-in mechanism for the time being,
- Follow-up the evolution of the technology and its deployment in real situations and, should it be necessary, revise the flexible opt-in mechanism in the upcoming years.

5.4.10. Side questions: verification of and responsibility for de-activation

Verification of tag deactivation (under the opt-in scenario) is a side question under consideration. It implies that consumers have the possibility to verify that tags have been properly deactivated by the retailer. In principle, this would require an additional reader, which would allow consumers to check whether the tag is still operational. For large shops and supermarkets, which have already many readers available, this cost would be marginal, but this would not be the case for small retailers.

A final question is the **responsibility for de-activation** of the tag. This is especially relevant for situations in which a retailer does not make use of the RFID technology (such as a small corner shop that does not have an interest for using RFID for item flow control in processes or inventory audit), but is faced with items which have an embedded tag.

In the current situation of today, in most pilot projects, item level tagging is done by the retailer himself for his own needs. The next phase is for large retailers to require their suppliers to tag the products themselves. Over time, those requests becoming more common, suppliers are likely to tag all of their products, regardless of whether the retailer has requested it or not.

In determining who is responsible for tag de-activation there are two choices:

- The retailer is responsible for tag deactivation, whether or not he is a user of the technology (i.e. an RFID application operator),

- The 'last active user of the technology' (or 'last active application operator') up the supply chain is responsible for tag de-activation, either by deactivating himself or by passing downwards the supply chain the required information and means to have the tag deactivated.

In the first situation all retailers need to possess deactivation equipment. This may not pose a large problem in the future situation when item level tagging is widespread, but will be a significant issue for its introduction, especially for **small retailers**, who are not using RFID themselves but would have to face the costs. Note that, in some particular situations to be assessed case by case (such as tags attached to a cloth the same way as a price tag) it could be tolerated that the responsibility for the removal of the tag is left up to the consumer.

In the second situation, the 'last active user' in a supply chain, in most cases a transport company, would need to deactivate the tags at delivery, or provide the retailer the information and means to carry out de-activation.

5.4.11. Comparison of sub-options III.a, III.b & III.c.

		Sub-Option III.a	**Sub-Option III.b**	**Sub-Option III.c**
Costs	Cost of implementation	- / 0 Immediate costs would be negligible but eventually costs might be high as most items are expected to have tags affixed to or embedded in them.	- - Costs of implementation are high as a large number of checkouts would have to be re-constructed.	- / 0 While this option incurs some costs, those have already been considered to some extent by those retailers who have normally integrated the opt-out scenario in their initial deployments.
Benefits	Citizen trust and risk perception	- - No benefits as citizen trust would be heavily affected to the extent that civil protests could happen.	+ + By adopting an open and transparent attitude, operators will create trust among citizens.	+ If playing the game in good faith, level of consumer confidence and trust should be high but retailers would have to remain careful on how they approach the question.
	Regulatory certainty, harmonisation	- - No benefits as there is a high risk that Member States establish their own requirements (either full opt-in or opt-out).	+ + The certainty of the regulation would be very high.	+ + The certainty of the regulation would be very high.
	Awareness (both citizen and SMEs) and information about RFID	- / 0 No impact is expected on this aspect.	+ + Awareness among consumers would be very high.	+ Awareness among consumers would be high.
Direct economic impacts		0 Little impact expected, if any, due to lack of clarification.	- - High risk of European retailers suspending their early deployment pilots with negative impact on their competitiveness and on jobs.	0/+ Limited overall impact as incentives and disincentives to further deploy the technology are likely to neutralise each other. Existing plans for RFID deployment are likely to be maintained with potential gains

			in terms of efficiencies and hence competitiveness.
Speed of deployment of RFID	- Speed of deployment would depend on how much it would be affected by the lack of harmonisation and the response from the civil society.	- - The business case for many retailers to tag their products at item-level would be modified and likely imply a freeze, at least temporarily, of this specific deployment.	+ This option seems to be the best compromise in between what is affordable in terms of deactivation and what consumers seem ready to accept. Because not optimal, it would have to be followed-up and eventually revised.

In conclusion, it should be noticed that:

- **IIIa would not work.** This option suffers major flaws and should be discarded. Through early trials a few years ago, the industry is aware of it and is avoiding proceeding this way in their new deployments.

- **III.b is the favoured solution** when only looking at the benefits. It is however costly to implement to the extent that it would risk to seriously slow down, if not stop, the use of the technology for retail item-level tagging.

- **III.c is the best compromise** under current technical situation. The recommendation should therefore permit this solution.

5.5. Economic, Social and Environmental Impacts of RFID technology

The previous sections analysed the direct impacts of various policy options for a recommendation. It showed that the policy intervention must find a difficult balance between the benefits in terms of increased public awareness, reduced privacy and security risks and regulatory certainty on one hand and additional compliance costs for companies on the other hand. Both direct costs and benefits will influence the speed of deployment of RFID.

It is important to note that while some policy options can contribute to higher deployment of RFID in Europe (mainly deployment of item level tagging in retail environment), there are also other factors, such as costs of RFID tags and equipment, which influence deployment of RFID but cannot be directly influenced by the EU intervention. RFID tags are already used in many business-to-business (B2B) applications where privacy and security risks for consumers are not of direct concern. It can therefore be concluded that the Recommendation by itself will not play a decisive role in mass deployment of RFID in general but it can contribute to wider deployment of RFID technologies, particularly in B2C applications.

This section summarizes the key economic, social and environmental impacts of RFID technology as such. Summarized statements in the table below are supported by evidence and analysis in Annex 4. The table considers two distinct scenarios: low speed of RFID deployment in Europe and high speed of deployment. It is clear that while RFID technology has the potential to bring many benefits, particularly higher economic efficiency and productivity, mass RFID deployment can also have negative consequences, such as loss of routine jobs in the retail sector. The increased automation that is made possible by the introduction of RFID technology will reduce the need for administrative staff and jobs that involve bar code scanning such as cashiers in supermarkets or jobs in distribution centres, as one example. A report from the US Yankee Group (2004) [58] forecasted that efficiency advantages of RFID could affect 4 million employees in the retail sector in the US[59]. Nevertheless, it is likely that introduction of the RFID technology in the retail sector in Europe will happen gradually and some retail companies have already signalled that they plan to re-train workers and transfer them to other positions (such as customer service) rather than fire them[60]. Nevertheless, it cannot be excluded that in the short term, some routine jobs in the retail sector will be lost while demand for highly qualified RFID-related jobs will increase. It is worth noting that the telecom industry, with the introduction of mobile telephone had to undergo a similar transition.

Table 5.2. Summary of indirect impacts of RFID deployment in Europe

Speed of deployment	Low	High
Economic impacts		
Competitiveness of the EU RFID industry	Competitive position of the EU RFID industry will worsen in the medium to long term as other regions (US, Asia) deploy RFID at a faster pace.	Improved competitive position of the EU RFID industry, new opportunities for innovation and expansion of EU businesses, stronger position in international markets (e.g. in terms of international standards).
Economic performance of sectors	Lost opportunities in terms of possible benefits and cost savings for industry and services. Absence of RFID tags in products can constitute a barrier to export in third countries.	Efficiency gains, improved logistics, cost reductions, error minimisation and other benefits in many sectors (see Annex 4).
Economic impact on third countries	EU companies not ready to export to third countries using RFID technologies (US, Japan, Korea). Main RFID producers located outside the EU.	Third countries would be obliged to use RFID technologies and respect privacy and security rules when entering the EU market.
Impact on SMEs	Limited opportunities for growth in the RFID sector, limited use of RFID applications in business processes .	New growth opportunities for SMEs in the RFID industry and cost reductions for SMEs using RFID applications.
Social impacts		
Employment	Job losses not as big as for high speed of RFID deployment, and limited creation of high value-added jobs.	Loss of routine jobs (cashiers in supermarkets, jobs in distribution centers, etc.) and increase in high quality jobs (information processing, new services, etc). Higher demands for workers with RFID related skills (RFID engineering, etc.).

[58] Yankee Group (2004), *Sers and vendors are beginning to explorer the utility of RFID technology In the supply chain.* Cite In JRC (2007).

[59] The report does not state that all these jobs will be lost. According to report some of the workers will lose their jobs, but most will see them migrate from mundane to 'more value-added' positions.

[60] For more details on employment impacts, refer to Annex 5.

Public health	More research needed to determine the impact of electromagnetic field on human health.	More research needed to determine the impact of electromagnetic field on human health. Benefits in the health sector (patient tracking, effective management of information within hospitals, etc.) Positive contribution to food safety, animal identification and animal health.
Environmental impacts		
Waste implications	Low amount of RFID-related electronic waste.	Increase in electronic waste in case of mass deployment of RFID. Negative impacts can be mitigated through innovation (e.g. lead-free tags) and recycle programmes.
Reverse logistics and recycling Animal health and food safety	Limited application of RFID in reverse logistics and recycling. Low impact on animal health and food safety	Mass deployment of RFID can enable more efficient lifecycle information management systems. Increased food safety and animal health thanks to more efficient animal livestock identification and tracing applications.

5.6. Risks and uncertainties of the assessment

Any policy assessment in the domain of RFID is necessarily characterised by uncertainties and risks. The RFID market is not mature yet, development of the technology is hard to predict and consumer perception of RFID is also likely to change in time. The aim of this section is therefore to identify the main uncertainties in the assessment of options and impacts and possible ways of mitigating them.

Table 5.3. Uncertainties and risks in the assessment

Uncertainties/risks	How to mitigate them
The assessment of content options assumes that all entities will implement the Recommendation – risk of low compliance	The Commission must remain an active partner for the industry stakeholders and Member States, facilitating dialogue and encouraging implementation of the Recommendation. An effective monitoring system will also encourage compliance. If compliance is not ensured, the Commission can consider revising the Recommendation or taking regulatory measures.
Despite the privacy and security measures in the Recommendation, consumers will be still reluctant to accept RFID	Pubic bodies must ensure that information provided to general public is well targeted and easy to understand. Public awareness campaigns both at the EU level and in Member States are very important for gaining public trust and explaining benefits of the policy framework.
Some Member States will not play an active role in implementation of the Recommendation	In order to achieve a harmonised outcome, the Commission must ensure commitment of all MS and national data protection authorities. MS will be requested to report on implementation of the Recommendation.
Industry will not develop Community codes of	The Commission together with Member States can act as

conduct to facilitate the use of RFID application in different sectors	a facilitator and "honest broker" in developing industry codes of conduct.
Use of RFID will take off more rapidly in third countries because of less strict privacy and security framework	The level of privacy and security protection in a country depends also on societal demand. Evidence shows that countries where RFID is being used in B2C environment (e.g. Japan, US, Korea) put in place guidelines or self-/co-regulatory measures to safeguard privacy and security of consumers. The EU could promote its policy framework in third countries, explaining its benefits.

6. EVALUATION AND MONITORING

6.1. Specific evaluation and monitoring requirements

In view of the fast moving developments in the field of RFID, it is necessary to introduce periodic reviews of the Recommendation to judge its effectiveness and to adjust or expand the Recommendation with new RFID application areas. In this way, the Recommendation will remain up-to-date in view of the most recent market and technological developments. It also allows the Commission to judge whether it is appropriate to replace the "soft" Recommendation with hard legislation if its objectives are not fulfilled.

The Commission will monitor closely the key market and technology developments through studies and RFID-related research projects. With respect to monitoring of the efficiency and effectiveness of the proposed measures, Member States will be required to inform the Commission of actions taken in response to the Recommendation. Data protection authorities in each Member State will be involved in monitoring of the implementation. In particular, national data protection authorities will gather information about the existing codes of conduct in their Member State (Article 29 Working Party will monitor the Community codes of conduct). Member States will also provide information about the level of compliance with the provisions of the Recommendation. Additional data on economic impacts of the measures on different groups of stakeholders can be collected through ad hoc evaluation studies. The Commission will also collect data on administrative costs of implementing privacy impact assessments, introducing logos on products and implementing the flexible opt-in solution in retail stores. This data will provide evidence for the review of the recommendation.

The monitoring data collected from Member States and the economic data from research projects and studies will be used to evaluate the effectiveness and efficiency of the Recommendation. The Commission will provide a report on the implementation of the Recommendation and its impact on economic operators and consumers. On the basis of the results published in this report, the Commission will decide whether to amend the Recommendation, extend it in time or scope or whether any additional binding measures will be necessary in the future.

6.2. Objectives and evaluation indicators

Indicators are meant to concretise the objectives. This step is important since it will allow the measurement and assessment of the various policy measures and enable adequate monitoring and evaluation of the policy intervention. The table below outlines the core indicators for the key policy objectives of the RFID initiative. Other, more detailed performance indicators will be formulated at a later stage when the concrete policy measures are adopted.

Table 6.1. Objectives and indicators (initial, non-exhaustive list)

Objective	Indicators
Overall policy objectives	
Address privacy and security concerns related to RFID use	• Percentage of consumers expressing privacy and security concerns related to RFID • Number of RFID stories covered by public press and other media
Specific policy objectives	
Avoid uncertainty among investors in RFID technology as to the interpretation of the general data protection legislation	• Investment in RFID applications by companies in the EU • Stated uncertainty (in surveys); number of requests for information at DPAs
Mitigate security and privacy risks and concerns related to RFID use, especially in B2C environments	• Adoption of codes of conducts with appropriate countermeasures for the application at all risk levels • Number of infringement cases on personal privacy legislation in relation to RFID • Reduced % of people that state their concerns and improved trust levels (surveys) • Number of persons working in RFID industry
Stimulate innovation through a wider adoption of RFID applications	• Share of EU RFID industry in the global RFID market • Improved service levels (ease of processes, improved information, additional services) resulting from RFID applications • Level of investment done by companies
Facilitate development of harmonised, interoperable use of RFID in Europe and similar privacy & security conduct in the different Member States of the EU	• Cross-border investment in RFID • Number of Community codes of conduct • Size of RFID market (tags, middleware, back-end systems, supporting services etc.) in EU
Improve awareness among citizens and companies (including SMEs) of rights and obligations related to RFID	• Availability of information to consumers/citizens • Awareness of consumers/citizens (% of people) • Share of companies that are aware (survey information)

ANNEX 1. RFID: KEY CHARACTERISTICS

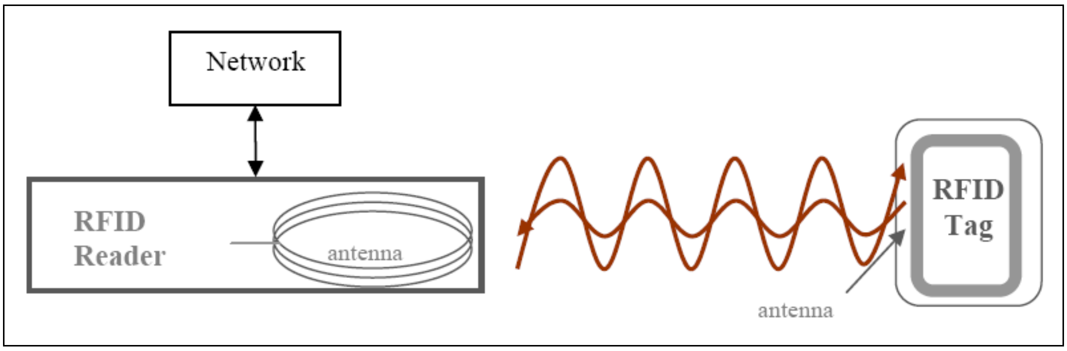
As with all other IT systems, RFID systems can vary in terms of complexity and implementation. The following common subsystem building-blocks can be distinguished:

1. The RF subsystem (front end-system). This subsystem consists of the RFID tag and the RFID reader and is the part that performs identification and related transactions over a wireless interface.

2. The enterprise subsystem. This subsystem comprises the computers and software necessary to process and store data acquired from the RF subsystem.

3. The inter-enterprise subsystem. This subsystem is used to connect different enterprise subsystems to each other if information needs to be shared between organisations.

Figure A1. Basic components of an RFID system



Source: JRC 2007

RFID tags can be **passive or active** tags. Passive tags do not have an own power source and are powered by the reader's field which charges the tag. This typically requires a stronger field and makes this type of tag more suitable for short read-range applications. This type of tags is mostly cheap, light and compact.

Active tags are powered by their own battery and can emit a detectable signal. Their lifetime is determined by the lifetime of their battery. Often these tags have read/write capacities over greater distances and increased memory capabilities. These tags are relatively larger and more expensive.

Around the world, different parts of the **frequency spectrum** are assigned to different purposes by government regulation. This results in a multitude of frequency bands in use for RFID, divided into four groups: Low Frequency (LF), High Frequency (HF), Ultra-High Frequency (UHF), and Microwave. The table below contains the frequency ranges together with their areas of application.

Table A1. Frequency bands and application

	LF	HF	UHF	Microwave
Frequency Range	< 135 KHz	10 – 13.56 MHz	860 – 960 MHz	2.4 – 5.8 GHz
Read Range	~10 cm	~1 m	2 ~ 5 m	~100 m
Coupling	Magnetic, Electric	Magnetic, Electric	Electromagnetic	Electromagnetic
Application	Smart Card, Ticketing, Anti-Theft, Animal Tagging	Small Item Management, Anti-Theft, Supply Chain	Transportation, Vehicle ID, Access/Security, Large Item Management, Supply Chain	Transportation, Vehicle ID, Access/Security, UWB Localisation

The relation between applications and frequencies stems from the fact that lower frequencies penetrate deeper into materials and liquids, but have a shorter reading range. Whereas higher frequencies have typically a longer range, but are more sensitive to the environment.

Sometimes RFID is considered as the replacement of the barcode. However, one of the major differences with barcodes is the **numbering** used for RFID. Barcodes typically have the same number for a particular product type (i.e. two bottles of water of the same brand have the same number) where RFID typically identifies each product with a unique number (i.e., these two bottles have different numbers).

As for other technologies, **standardisation** constitutes a main driver for interoperability, which in turn is important for its successful adoption. In particular this is valid for applications that operate in an open system (e.g. integrated logistics, asset management, e-payment etcetera). There are two official standards institutes that play a relevant role in RFID standardisation: the International Organisation for Standardisation (ISO) and the European Telecommunications Standards Institute (ETSI). Also the EPCglobal organisation is an important player. Though not an official standardisation body, EPCglobal main aim is to lead the drive to standardise and promote the Electronic Product Code (EPC). The existence of standards does not mean that all tags are equal. Some features are optional or proprietary.

ANNEX 2. EXAMPLES OF PIA HANDBOOK , PIA REPORT AND BSI SECURITY ASSESSMENT

This Annex gives additional information on a number of existing PIA methodologies in the UK and Canada. It also provides an example of the concept of the combined privacy/security assessment that is carried out by BSI in the establishment of technical guidelines for specific RFID applications.

1) PIA in the UK

Table of content of the UK PIA Handbook[61]

Part I – How to Determine whether an Assessment is Needed

Preparing for the PIA Screening Process

The PIA screening Process

Part II – Full-Scale Privacy Impact Assessment

Introduction

Framework

Overview of full scale PIA

Planning the PIA Process

Conducting the PIA Process

Part III – Small-Scale Privacy Impact Assessment

Overview of small scale PIA

Background information

The process

Part IV– Privacy Law Compliance Checking

Privacy Law Compliance Check

Part V– Data Protection Act Compliance Checking

Data Protection Act Compliance Check

Part VI – Additional Information

General resources

Publications

Glossary

Service-Provision, Quality, Access and Equity

The Allocation of Effort, Costs and Risks

Data Protection Act Compliance Check

Privacy and Electronic Communications Regulations Direct Marketing Compliance Check

[61] Available at http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/foreword.html.

Persons at Risk, and Vulnerable Populations

The UK PIA Handbook gives a detailed overview of the PIA process and consists of six parts. In the first part it can -by answering some questions- be determined if a PIA is needed and if this PIA should be full-scale or small-scale. When it's clear what kind of PIA is needed, it can be conducted through a 5-phase process.

1. Preliminary phase: ensure that a firm basis is established for the PIA to be conducted effectively and efficiently

2. Preparatory phase: make the arrangements needed to enable the critical Phase 3 to run smoothly. In this phase, organisations may undertake a stakeholder analysis, development of a consultation strategy and plan, and establishment of a PIA Consultative Group (PCG).

3. Consultation and analysis phase(s): this phase includes consultations with stakeholders, risk analysis, the articulation of problems, and the search for constructive solutions.

4. Documentation phase: document the process and the outcomes. The deliverable is a PIA Report, which must contain some key-elements. There is no template available like for the Canadian PIA (see box).

5. Review and audit phase: that the design features arising from the PIA are implemented, and are effective. The deliverable is a Review Report.

The main reasons for documenting the outcomes of a PIA is that it's a way to demonstrate that the PIA process was performed properly and the report is a basis for audit and for post-implementation review. In the UK PIA Handbook, the key elements of this report are described. These key-elements are:

- *Description of the project*
- *An analysis of the privacy issues arising from it*
- *The business case justifying privacy intrusion and its implications*
- *Discussion of alternatives considered and the rationale for the decisions made*
- *A description of the privacy design features adopted to reduce and avoid privacy intrusion and their implications of these design features*
- *An analysis of the public acceptability of the scheme and its applications*.

2) PIA in Canada

In Canada (and the US) there is a template available for writing a PIA report. In Canada, the following structure must be followed:

Table of contents Canadian PIA Report

1. Executive Summary

2. Introduction

2.1 Report Objectives

2.2 Scope of PIA

2.3 Reference Documentation

2.4 Participants

2.5 Legislation and Policies

2.6 Abbreviations Used in this Report

3. Project Proposal

4. Data Flow Analysis

4.1 Business Flow Diagram and Description

4.2 Data Flow Table

5. Privacy Analysis

6. Privacy Risk Management Plan

6.1 Privacy Risk Mitigation

6.2 Summary Table

7. Communications Strategy

Source: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2_e.asp#AnnexA

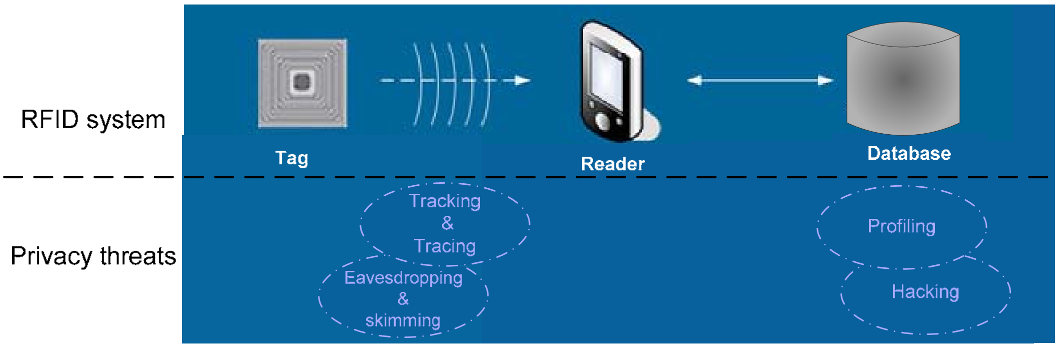
3) BSI Concept of the Security Assessment

Error! Objects cannot be created from editing field codes.

ANNEX 3: COUNTERACTING SECURITY AND PRIVACY THREATS

The strongest privacy and security concerns of the public are twofold. On the one hand there is fear that consumers can be tracked and traced through tags that can be read from a distance. On the other hand, the fear is that data collected can be used by third parties (including profiling, targeted direct marketing)[62].

Fig. Security and privacy threats in the RFID data chain



De-activation at the point-of-sale or other security measures mainly refer to the first point, which in fact illustrates a security risk. The latter issue is more related to the data management policy that is followed and the extent that data is shared (and becomes part of the ubiquitous world of the Internet of Things).

Possible measures to counter security and privacy threats

De-activation is one of the possible information security countermeasures that can be taken. It does answer to a specific privacy concern of consumers. To provide a good contextual understanding of potential other countermeasures an overview is presented of the most obvious countermeasures that can be applied at different components of the RFID system. The eventual choice of the most appropriate countermeasure should be defined in a combined privacy impact/security assessment.

Table below gives an overview of possible countermeasures, the RFID system component in which they interact, and effectiveness and cost level. With respect to the cost level it should be noted that these are strongly subject to change, as RFID is still in its infant stages of development and prices are likely change in the coming decades.

The measures as listed in the table are not all equally effective and the costs of different measures may vary significantly. Moreover, there are some drawbacks identified regarding some of the countermeasures and some can only be effectively used when combined with other measures.

Table. Effectiveness and costs of countermeasures for privacy threats

RFID component	Countermeasure	Effectiveness	Costs
Tag	Recoding & pseudonym	Very effective	€€/€€€

[62] See CapGemini (2005).

RFID component	Countermeasure	Effectiveness	Costs
Tag	Reduce information on the tag	Very effective	€€
Tag	Kill command/sleep command	Very effective[63]	€/€€[64]
Tag	Destroy tag	Very effective	€€[65]
Tag	Tear off antenna	Very effective	€€/€€€
Tag	Removing the tag	Very effective	€
Reader (signal)	Shielding	Effective	€
Reader (signal)	Verify tag data	Very effective	€ (initially €€€)
Reader (signal)	Encryption	Effective	€€€
Reader (signal)	Detect the presence of readers	Effective	€€€
Reader (signal)	Reader authentication	Effective	€€
Back office	Permissions are issued sparingly	Very effective	€
Back office	Screen servers and shield different groups of users	Very effective	€€
Back office	Procedures	Effective	€€
Back office	Software is checked before installation	Effective	€€
Back office	Possible content of parameters is restricted	Effective	€
Back office	Ensure proper format of	Not very effective	€

[63] Although the EPC standard allows a kill command for EPC Class 1 Gen 1 (8 bit password) and Gen 2 (32-bit password), not all tags may be equipped with sufficient memory to allow the application of this command.

[64] Readers with kill command possibilities will not be significantly more expensive than readers without this option; in principle costs to kill a tag are low, if tags are of the same type and possess the same password; if different passwords are used (e.g. tags from different tag suppliers) or different types of tags, more complicated readers will be required. In addition password management becomes more complicated. It should be noted that large retailers may cause further standardisation. Another view, defended by industry is the following: the secure password handling infrastructure that is required at each point of sale does require a solution that not yet exists. In addition it is expected to require new, additional POS systems to ensure that the deactivation does not interfere with the read-out process for potential payment uses or EAS (Electronic Article Surveillance). This would be the case even if a suitable password-handling infrastructure would be in place. Both reasons render technical deactivation (as opposed to mechanical deactivation) prohibitively expensive for the time being.

[65] It is reported that tag zappers (or RFID zappers) are available that generate a strong electromagnetic field at a cost of €50-100. An alternative is the physical destruction of tags (punch a hole in the tag).

RFID component	Countermeasure	Effectiveness	Costs
	data		

Below some further considerations are presented with respect to the use of countermeasures:

- *Recoding and use of pseudonyms*: using a recoding protocol is a very effective measure; however it should be combined with other countermeasures.

- *Having a tag use pseudonyms:* This means a tag does not always respond with the same identification number, but has a number of IDs. The back-office of the system will have no difficulty matching the different tag IDs to the same item, but for a party making illegal readings this will be much more difficult. This requires a slightly more expensive tag.

- *Reducing information on the tag*: this essentially means that one shifts the information from the tag to the back office. This is considered to be very effective because the information that is not stored on the tag cannot be read from the tag. However, as a result, there is more data stored in the database and it will be important to set up appropriate security measures for the protection of the database.

- *Encryption:* although the costs are high (encryption-enabled tags are approximately 50% more expensive than non-cryptographic tags), this is a very effective countermeasure. Depending on the strength of the encryption algorithm, the encryption could be broken or the encryption key could be stolen, but this is unlikely and in many cases not worth the effort.

- *Reader authentication:* Authentication-only capable tags are roughly ~20% more expensive than non-cryptographic tags, but this is an effective measure since the tags can no longer be read by unauthorised readers. Similar to the previous measure, depending on the strength of the authentication algorithm the authentication could be broken, but this is usually unlikely and not worth the effort.

- *Ensure proper format of data being written to the tag:* By means of software, it is ensured that proper data is written on the tag. This helps prevent wrong or malicious (virus) data entering the system. However, it does not prevent malicious changes to the tag contents (thus reading it as well) by outsiders. Hence the effectiveness is low.

- *Verify tag data:* This requires the use of proper software engineering practices combined with the use of the appropriate tools, together with a suitable level of quality control. If these practices and tools are being followed already, the additional costs are negligible. Otherwise, costs are very high. Provided that the verification of the data is done correctly and completely, this countermeasure is highly effective against wrong or malicious data entering the system, including modification of tag contents by outsiders.

- *Screen servers and shield different groups of users:* One-time costs are incurred by installing and configuring firewalls, or similarly, to protect servers. Recurring costs are incurred by managing the firewalls and maintaining user groups and access permissions.

- *Principle of least privileges:* this is a very effective measure to prevent unauthorised use and/or modification of data by users, including insiders.

- *Procedures:* Having a proper set of procedures in place, according to an adequate security policy, will reduce the risk of security and privacy incidents.

ANNEX 4: IMPACTS OF RFID TECHNOLOGY

1. *Impact on economic performance of sectors*

Wider deployment of RFID will impact on the **economic performance of sectors** that are using RFID. In Table 5.1, a number of examples are given of the potential impact of RFID on sector performance.

RFID in logistics

RFID in logistics is used throughout the whole supply chain: from manufacturing to procurement. The tags are mostly used for asset tracking and for tagging on pallets, all within a closed loop situation. Tagging on pallet level is already taking place on a large scale. In 2006 around 200 million of tags[66] were supplied worldwide for pallet tagging alone. Once costs drop further, more tags will be used first for tagging at a case level and next at an item level tagging, making it possible to track and trace cases and items instead of pallets throughout the supply chain.

Benefits of the use of RFID in the supply chain are numerous, but in general it can be said that it will improve the efficiency of the processes across the chain. In the production stage, RFID tagging can lead to a more effective capacity utilisation and lower material losses. Also, improved product quality can be established.

Table 4.1 Economic performance impacts of illustrative RFID applications in various sectors

Sector	Potential market (*)	RFID applications	Key benefits and threats
Industry & logistics	Significant (23% of tag revenue in 2017)	- tracking and tracing of goods - Inventory management - Asset tracking - Process automation - Quality monitoring	- efficiency and productivity gains - less material losses - improved capacity utilisation - error minimisation - improved product quality
Retail	Significant (16% of tag revenue in 2017)	- Item tagging - Self-scanners - Theft protection	- efficiency and cost savings - improved inventory management - enhanced automation - marketing support - theft and counterfeiting reduction - reallocation of jobs
Transport	Considerable (smart cards 16% of tag revenue in 2017) Small (< 1% of tag	- Vehicle identification - Toll collection - Public transport payment	- service improvement - cost reductions - error minimisation

[66] IdTechEx (2007).

Sector	Potential market (*)	RFID applications	Key benefits and threats
	revenue)	- Luggage handling - Car tyre pressure monitoring	
Finance		- Credit card transactions - Payments by mobile phone (Near Field Communication)	- operational efficiency - customer convenience - improved customer management - anti-fraud/ counterfeiting
Consumer services		- Ticketing (ski, entrance, events)	- fraud prevention - cost savings - customer service
Health	Small (patient tags 4% and pharmaceuticals 3% of tag revenue in 2017)	- electronic patient file - hospital medication provision - drugs authentication	- improved safety - error minimisation - efficiency gains

(*) Future tag revenue based on projections IDTechEx (2007).

Assets' visibility is another important aspect. When a manufacturer can monitor the movement of goods throughout the supply chain, this will eventually lead to a more demand driven supply chain (instead of forecast-driven supply chain). This in turn results in a more effective capacity utilisation and cost savings. In warehousing, cost savings can be achieved as well. RFID enables more effective order picking, automatically checking incoming goods and reducing out of stocks. Thus errors are minimised and productivity can be increased. For instance, reliability of delivery time windows has improved by 90% at Dow Chemical Company. RFID also makes product recalls easier (a.k.a. reverse logistics).

RFID in retail (B2C)

Until 2003, the retail sector, even including suppliers and supply chains, was a small part of RFID business. Currently, item level tagging is only taking place on high value goods with a high velocity, such as DVDs, retail apparel and computer video games. Nevertheless, expectations for this sector are high as significant costs savings are expected[67] [68].

One of the benefits for the retail sector when using RFID on item level is more visibility in the supply chain and a more demand-driven planning. When goods can be easily tracked and traced, out of stock situations can be prevented (smart shelves)[69]. As a result, less stock buffering is needed. In addition, costs savings can occur as RFID technology may reduce the need for cashiers. For instance, trade unions in France have estimated that the new self checkout systems (rapid self-checkouts and self-scanning) could pose a threat to the jobs of the 170000 cashiers in large scale retailing. CFDT and Force Ouvrière share the view that

[67] Manhattan Associates, "RFID: The UPC of the 21st Century," 2003.

[68] US Department of Commerce – RFID opportunities and challenges in implementation, April 2005.

[69] A recent evaluation done by IFRI shows that the reduction of out-of-stocks can be up to 30%. This is expected also to contribute to higher sales (see ITRI 2005, 2006).

self-service tills will put 50% of checkout jobs at risk over the next 4-5 years. In the longer term, trade unions are most concerned with RFID which will make it possible by around 2017 to automatically print till receipts after passing through a detector frame.

But implementing RFID can also support the marketing strategy. Retail companies like Marks & Spencer, Best Buy and Tesco report 5 to 20%[70] increase of the annual sales in the first year after implementing RFID. In addition, preventing theft and counterfeiting is frequently mentioned as an advantage of RFID.

RFID in transport

The transport sector includes air transport, public transport and road transport. RFID is already used in this sector for vehicle identification (including car keys), toll collection, public transport payment and luggage handling at airports. Up till now, this sector has been the most important sector for implementing smart cards, mostly used for public transport. Besides this, RFID is used for asset management. When its use grows further, additional benefits can be achieved.

The most important benefits in public transport are lower waiting times and improved customer service. Within the field of luggage handling at airports, there are also important benefits to be achieved. There include significant service improvements and cost reductions as errors in luggage handling are minimised. An IATA survey has shown that airlines could save up to €513 million in baggage mishandling costs[71] with an investment of €0.07 incremental on the cost of baggage labels[72] Because of these huge benefits, IATA has developed a transition programme for airports to stimulate RFID implementation.

RFID in health sector

The first use of RFID in the health sector goes back to the 90s and, since then, RFID in the health industry is mainly used for drug registration, asset tracking and patient or personnel tracking. For some of these applications passive tags are used, for others only active tags are appropriate.

The benefits of using RFID within this sector include improving the safety of patients (tracking, as well as decreasing medical errors), efficiency improvements and cost reductions. In many cases, there is no direct financial business case for implementing RFID at the moment. However, costs are not always the key driver as safeguarding patients' safety or reducing errors can be considered to be more important. For example, RFID can reduce blood transfusion errors up to 100% as has been shown in pilots in Italian hospitals.

However, when the use of RFID increases and costs of the technology drop, for many applications within the health sector, it will be possible to achieve a return on investment. According to some estimates, the savings for an average-sized hospital of 250 beds can reach the level of approximately € 4 million per year[73].

[70] See http://www.csasupplychainsummit.com/ and http://www.idtechex.com/research/articles/rfid_update_from_wal_mart_00000313.asp.

[71] Used exchange rate: 1 USD=0.7 EUR.

[72] IATA (2007). RFID Transition Plan For Baggage. Available at www.iata.org/stbsupportportal.

[73] Source: RFID Journal (2004), RFID Remedy for medical errors.

Another application is the use of RFID in combating counterfeiting of drugs. According to the World Health Organisation, the sale of counterfeit prescription drugs is an €18 billion-a-year illegal business.[74] If drugs are RFID tagged at the pallet, case and package level, they can be quickly and accurately tracked from the manufacturer all the way to the pharmacy. As they enter and leave each link in the distribution chain (manufacturer, distributor, wholesaler and retailer), the drugs are scanned and authenticated. Any counterfeits can be immediately identified and removed from circulation before they do harm[75].

Apart from combating counterfeiting this will also have positive impacts on health. Other cost savings may also be expected. An HDMA study published in November 2004 entitled: "*Adopting EPC in Healthcare: Cost and Benefits"* said there were financial gains to be made through widespread incorporation of RFID into the supply chain. It estimated that pharmaceutical manufacturers stand to gain €350 million to €700 million annually by adopting RFID technologies. For distributors, that annual gain would amount to between €140 million and €280 million. The report, based on research by A.T. Kearney, said most benefits would be realised by improving the accuracy of claims and deductions and inventory and warehouse efficiency.[76]

RFID in finance sector

At the moment, RFID in the finance sector is used for customer convenience and asset management (operational efficiency). Regarding the customer and RFID, the finance sector focuses on smart financial cards (contactless credit cards). Applications that have started to become popular in Europe are those used within closed circuit; e.g. to pay for drinks. Other developments focus on payments by RFID enabled mobile phones (Near Field Communication). There are many ongoing pilot projects introducing the contactless credit card. Mobile phone companies have started to equip cellular phones with the necessary technology to allow several types of payments. Industry analysts predict that there will be almost 40 million contactless payment devices in the use in the US by the end of 2006.

Benefits of contactless cards over traditional credit cards are the speed of transactions and a better management of customer relationships. As concerns asset management within the finance sector, RFID is used to track and trace financial documents and to act against counterfeiting. Misplaced documents can prove to be very costly for banks and can lead to financial and/or reputation loss. Tracking the most important documents can therefore save a lot of money. Next to tracking of documents, RFID can be used to prevent fraud as well, resulting in high cost savings.

RFID in leisure/consumer services

Within the consumer service sector, many RFID applications can be found. Once costs drop and the use of RFID rises, this sector will be of importance for the RFID industry. At the moment, RFID is used for ticketing, in library books, in sports, in casinos and in theme parks.

[74] Wasseman, E. A prescription for pharmaceuticals. http://www.rfidjournal.com/magazine/article/1739 visited on 26-11-2007.

[75] Bacheldor, B.(2007). Manufacturers Propose Tools to Fight Counterfeiting. http://www.rfidjournal.com/article/articleview/3421/1/1/

[76] Wasseman, E. A prescription for pharmaceuticals. http://www.rfidjournal.com/magazine/article/1739 visited on 26-11-2007.

Smart tickets, like the ones used during the World Cup in Germany, are used mainly to prevent fraud. The ticket contains a tag on which information is stored (this could be either personal, or non-personal information, depending on the purpose of the ticket). When entering the event, the genuineness is checked and, in case the ticket contains personal information, is matched against the person. This has proven effective to, for example avoid hooligans attending a soccer match.

Instead of buying a ticket with an integrated RFID tag, it is also possible to buy a ticket with RFID enabled mobile phones. The phone can then be used for identification and access. As described at the finance sector section, the use of NFC and mobile phones is growing.

Besides eTicketing, the use of RFID in library environments is increasing. In this application, books and library cards are tagged to save time and costs by improving check-out and check-in processes.

2. *Impact on employment*

Employment impacts in RFID industry and other industries are difficult to assess as relevant estimates and economic data in this respect are very scarce. It can be stated that the employment impacts are manifold and refer to the fluctuations in the number of jobs, the quality of jobs and the skills.

Impact on the number of jobs

Firstly, RFID is expected to improve the economic performance of sectors by stimulating efficiency and productivity gains. The increased automation that is made possible by the introduction of RFID technology will reduce the need for administrative staff and jobs that involve bar code scanning such as cashiers in supermarkets or jobs in distribution centres. A report from the US Yankee Group forecasts that efficiency advantages of RFID will cost 4 million employees their jobs[77]. The loss of jobs is expected to be a gradual development coupled to a long transition period of at least 10 years from the bar code scanning towards RFID applications. For example, EFPIA (European Federation of Pharmaceutical Industries & Associations) proposes a 2D Matrix Bar Code system to be introduced across Europe for coding and identification while conversion to another data carrier such as RFID would take place when "this is economical and mature enough" – i.e. not before 10 years from now.

As indicated in Section 2.2.5, the International Labour Office (ILO) report of 2006 on "Social and labour implications of the increased use of advanced retail technologies" is a valuable source of information. The report recommends initiating an extensive dialogue between workers and employers on worker privacy concerns, employment effects of RFID, and skills and training for employability.

Yet, most economists stress that technological change and productivity growth have historically been associated with expanding rather than contracting total employment. It must be assumed that employment in industries directly affected, especially retail, will see a decline, at least initially, and some workers will certainly be displaced. As with previous technological innovations, it is possible that RFID adoption and diffusion could be gradual, with employment impacts taking considerable time to be felt, depending on the absorptive capacity of retail and supply chain networks. The extent of such impacts will be affected by

[77] Yankee Group (2004), *Sers and vendors are beginning to explorer the utility of RFID technology In the supply chain.* Cite In JRC (2007).

their interaction with the concurrent processes of sectoral restructuring, globalisation, consolidation, and concentration.

The introduction of RFID alters demands on employees, with the elimination of routine warehousing tasks. Staff support measures for the transition include training and career development. For instance, retailers that have launched RFID pilots usually have offered comprehensive training to their employees. A major retailer has stressed that displaced workers could be shifted to customer service positions, benefiting both them and the company.

It is worth stressing mentioning the report entitled "RFID Adoption and Implications". This report[78] is the first one in Europe to describe how companies in the manufacturing, transportation, healthcare and retail industries use ICT and RFID for conducting business, to assess impacts of this development for firms and for the industry as a whole, and to indicate possible implications for policy. The impact of RFID on employment and workforce composition will be addressed in this report. As revealed in a survey of European companies carried out as part of this report which was presented at the recent eBusiness Watch Conference[79], about 70% of surveyed enterprises using RFID technology did not reduce jobs after its introduction as opposed to less than 1% of respondents who have significantly reduced their workforce and 28% of respondents who have made some workforce reductions.

At the same time the position of the RFID related industry itself will be positively impacted as the competitiveness of this specific sector will improve worldwide, thus allowing a higher share of RFID related jobs to be created in Europe. Companies will be able to make and move far more products with far fewer people, but because the goods will cost less to produce more people will be able to afford them. And many more people will be needed to manage the massive increase in goods flowing through the supply chain and service all of the new customers. In Europe, as revealed by the aforementioned eBusiness Watch report, a minority of enterprises created new technical (22% of companies) or business oriented (18%) jobs. Globally, based on current RFID-related employment trends the world's RFID workforce will grow to 1 million people by 2017[80].

Impacts on the quality of jobs

In addition to the impact on the number of jobs, the quality of jobs will increase as losses will be mainly in administrative and relatively lowly skilled positions, which will be replaced by automated processes. Several analysts predict a transition towards more added-value positions such as information (data processing, quality control of a certain process) and service related jobs. The RFID applications will give companies access to large amounts of data that have to be processed to generate actual, value-adding knowledge. Also customer service positions are expected to increase. This expectation has been confirmed in the above mentioned eBusiness Watch study which indicates based on case studies that some workforce in companies introducing RFID has been reallocated to other business functions. This transition will be gradual and spanned in time so that experts agree that no disruptive impacts on the labour market are expected in the transition period.

[78] "RFID Adoption and Implications. A Sectoral e-Business Watch study by IDC / Global Retail Insights". European Commission, DG Enterprise & Industry. Impact Study No. 07/2008.

[79] "The Penetration of RFID Technology across EU Industries", eBusiness Watch Conference, Brussels, 19-20 May 2008.

[80] http://www.rfidjournal.com/article/articleview/3389/.

It is interesting to note as well that the eBusiness Watch report states that the impact of RFID on work organisations is also witnessed by the fact that the majority of respondents developed training programs to re-qualify in-house personnel, while some 23% of respondents are considering the development of such a training programme in the future

Impacts on skills

There is currently a broader societal discourse on foreseeable shortages of the technically skilled workforce in Europe. RFID skills encompass a set of unique requirements including physics of radio frequencies (radio waves, frequencies, interference, shielding, etc.), RFID standards (air protocols, data coding), RFID hardware knowledge (tags, readers, antenna, labels, printers, etc.), and RFID data (acquisition and filtering, database storage and retrieval, electronic data exchange). According to the Computing Technology Industry Association (CompTIA) there are fewer than 1000 qualified IT professionals available worldwide who understand and know enough to deploy and service RFID technology (source: Business Week, 13 March 2007) – most capabilities are with major RFID consultancies and a few Auto-ID / data collection integrators. It is certainly one of the factors that are keeping back the deployment of RFID technology. Current market levels suggest that RFID skills training is likely to remain a major concern in the upcoming years: there are today more than 10000 RFID projects underway worldwide, more than 1000 suppliers offering RFID hardware and software, and more than 2000 RFID deployments in some 85 countries.[81]

The aforementioned eBusiness Watch study revealed that 15% of respondents are considering the recruitment of new personnel with specific technical and business process RFID skills. Furthermore, 22% of respondents already using RFID have hired new personnel with RFID specific technical skills.

In conclusion, the competitive position of European companies will improve as a result of the efficiency improvements resulting from the introduction of the RFID technology. This will spur economic growth, which in turn will create more jobs.

3. Impacts on public health and safety

The use of RFID can have an impact on public health and safety. On the one hand potential health risks are investigated with respect to the diffusion of RFID. On the other hand positive impacts on health can be expected from implementation in the health sector itself.

The electromagnetic fields which are related to RFID frequencies do not have sufficient energy to produce biological damage, including changes in DNA. In technical terms these frequencies are labelled non-ionising. The known effects of this type of radiation are principally short-term effects caused by heating processes. Aside from the level, it is also important to know the amount of radiation that is absorbed and therefore the potential to do harm. The magnitude that gives us an idea of this absorption is the “specific absorption rate”. RFID take up is expected to happen alongside a generalised increase in wireless applications (Mobile TV, Digital TV, Wireless broadband, etc). Effects of the cumulative exposure to electromagnetic fields are still subject to further research. It should be noted that close monitoring of the possible impacts of **electromagnetic field (EMF) on health** is undertaken

[81] e-Skills Certification Consortium at EU RFID Forum of 13-14 March 2007.

by SCENIHR (Scientific Committee on Emerging & Newly Identified Health Risks) which is established under the auspices of DG SANCO[82].

Some studies have indicated that the possibility may exist of “non-thermal” biological effects, although it is unknown whether these effects may constitute a risk to human health. Therefore, more research is needed to determine the effects and their possible relevance as regards human health. On the basis of preliminary scientific results, limits are established that are several times more restrictive than scientific limits. The minimum health and safety regulations in the European Union regarding exposure of workers to risks derived from electromagnetic fields, is Directive 2004/40/EC. In the case of RFID, where the maximum power in the antenna is 2 W (in the UHF band), the field values can never be higher than those established as limit values.

Finally, RFID has a potentially important role to play in the healthcare sector, by improving patient tracking[83], reducing medical mistakes[84] or contributing positively by helping society face an ageing population.

4. *Impacts on the environment*

Potential waste implications of mass deployment of RFIDs

Communication COM(2007)96 mentions the following environmental issues with respect to waste. “Regarding the environment, RFID meet the definition of electrical and electronic equipment provided for in the Directives 2002/96/EC on waste electrical and electronic equipment (WEEE) and 2002/95/EC on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS). RFID can be considered to fall under Category 3 "IT and telecommunication equipment". Therefore, RFID components are covered by RoHS, which means that the use of the hazardous substances Cd, Hg, Pb, CrVI, polybrominated biphenyls (PBB) or polybrominated diphenyl ethers (PBDE) is restricted.” As such, RFID tags themselves must be disposed after use – the process of etching metal antennas with acid produces hazardous waste. Matters like these must be regarded carefully for a successful adoption of RFID technologies.

It can be anticipated yet that thanks to technological progress the RFID antenna will be printed and the microchip attached during the normal printing process. Such printed antennas using conductive inks will not only be cheaper and faster to manufacture than metal antennas but also environmentally friendly. Tag producers like RF Code now produce lead-free tags and have launched a recycle programme for their tags. If these developments continue waste implication of RFID will diminish.

Secondary impacts on environment

In the future the enhanced track-and-trace functions of RFID will reshape supply chains as well as waste disposal and recycling processes. RFID is expected to improve the logistic processes, and in particular significantly benefit reverse logistics and recycling, according to Cambridge AutoID Lab. The key reverse supply chain issue nowadays is the lack of returned

[82] This committee provides regular updates on the potential risk of EMF. See http://ec.europa.eu/health/ph_risk/committees/04_scenihr /docs/scenihr_o_007.pdf.

[83] See EPIC: Radio Frequency Identification (RFID) systems: Tracking patients and personnel (retrieved from www.epic.org/privacy/rfid at 24th September 2007.

[84] National Academy of Sciences (2000), To Err Is Human: Building a Safer Health System.

product information[85]. RFID could enable more effective and more efficient Lifecycle Information Management Systems and thus positively contribute to environment. Also RFID use for recycling purposes is frequently stated as one of the possibilities of the technology[86].

Furthermore, in the emerging "Internet of things", most components of the "smart house", such as the heating system and refrigerator, can communicate with each other and with the outside world. The potential exists to optimize energy use by having the heating system respond to weather forecast and by having electrical appliances communicate with the power utility to lower energy demand when energy prices are high. Environmental protection will move from managing industries to managing every object, which includes knowing the properties and histories of these objects. RFID has the potential of becoming an important contributor to environmentally friendly economic development as postulated in the renewed Sustainable Development Strategy[87].

5. *Animal health and food safety*

Animal identification may be pursued for a variety of reasons, ranging from pure research (studying movements of animals) to economic and health reasons (being able to trace back the origins of meat when quality standards enforce this).88 The RFID tag is implanted in or attached to the animal and has a unique identification number with which the animal can be traced. The tagged animal can be a livestock animal, whereby tagging helps for instance to protect animal welfare disease spreading or trace back the origins of meat when quality standards enforce this. Increasingly pets are being tagged as well, which allows for more efficient identification than it is the case with traditional identification methods.

RFID can also contribute to **food safety** by offering support in product recalls. Firms operating in the grocery supply chain had to be able to identify the origin and destination of food products, and provide immediate information to governments by January 2005, as part of the European Health and Consumer Protection Directorate. This was meant to contribute to cost savings in recall actions for manufacturers and retailers[89]. In addition, smart tags are expected to be developed which may directly support food safety[90].

6. *Impacts on third countries*

Impacts on the third countries are expected not to be significant. To date, RFID has not been dealt with at the forum of the World Trade Organisation (WTO). Most impact on the international trade is expected in the area of labelling of products with logos and signs which indicate that the product is RFID-tagged. This negative impact is mitigated by similar initiatives at the other parts of the world, especially in the US. Moreover, logos for RFID-tagged items are currently subject of standardisation works at the International Standardisation Organisation (ISO).

[85] Kulkarni et al (2006), Reverse Logistics in Supply Networks, presentation on 4th Supply Chain Academic Forum July 2006, Bath.

[86] For example, HP started a trial with RFID on their printers which is expected to contribute to recycling purposes. Source: Kimberley Knickle (2007).

[87] Council of the European Union, "Renewed EU Sustainable Development Strategy", 10917/06.

[88] See JRC (2007) RFID Technologies – Emerging Issues, Challenges and Policy Options.

[89] Forrester suggested that Coca-Cola may have been able to save a large amount of the €11m spent recalling 13 million cases in Europe in 1999 if such a system had existed.

[90] E.g. smart label are developed to monitor the shelf life of product packed with modified atmosphere gases or RFID technology is developed that combines tracking and tracing with temperature readings (source Food productiondaily.com, various articles).

Discussions with governments of most concerned international partners, including the US, are ongoing on cooperation, common policy towards privacy and date protection, as well as RFID standards. In this context, the cooperation on common RFID transatlantic pilots was endorsed by the European and US leaders at the EU-US summit lighthouse priority projects. Similarly, dialogue with administrations in Korea, Japan, and other third countries on RFID policy is taking place.