

---



# Towards an RFID policy for Europe

## Workshop report

MAARTEN VAN DE VOORT  
ANDREAS LIGTVOET

DRR-4046-EC

31 August 2006

Prepared for the EUROPEAN COMMISSION,  
Directorate General Information Society and Media



# Preface

---

This report, prepared for and funded by the European Commission's DG INFSO, is part of a European-wide public consultation process regarding an RFID policy for Europe, and presents the proceedings of a series of consultation workshops organised on behalf of DG INFSO by RAND Europe and Europe Unlimited.

For each of these workshops Policy framework papers were published containing backgrounds to the topics discussed in the workshops. These papers can be downloaded from the Consultation website<sup>1</sup>. The website also contains the presentations that were given at the workshops and a background paper titled: Your voice on RFID<sup>2</sup>, which summarises the discussions during the workshops.

The main objective of the workshops was to bring together relevant stakeholders, raising and discussing concerns envisaged by these stakeholders in the field of RFID and collaboratively chart out new ways to address the related challenges and opportunities. As this document contains the proceedings of the workshops, the views expressed in the document are those of the presenters and discussants, and are not necessarily shared by the Commission's or the researchers. This report does not claim to present a comprehensive overview of all issues and options related to RFID, but merely provides a reflection of opinions of different discussants. As these opinions may be contradictory, the report does not reach consensus on all points. For more detailed backgrounds on RFID and the issues discussed during the workshops, we refer to the Policy framework papers, which are available at the website.

This report should be of interest to policymakers in the domain of technology policy, research and development centres in private companies, citizens, and consumer associations.

The report is organised in five chapters. The first chapter provides a general introduction to RFID. The following chapters each describe the proceedings of four workshops, which covered the following topics:

---

<sup>1</sup> <http://www.rfidconsultation.eu/>

<sup>2</sup> Background document for public consultation on Radio Frequency Identification (RFID) – Summary of five workshops.

---

15/16 May	RFID applications	Chapter 2
16/17 May	RFID security, data protection & privacy, health and safety issues	Chapter 3
1 June	RFID interoperability, standardisation, governance and intellectual property right issues	Chapter 4
2 June	RFID frequency spectrum – requirements and recommendations	Chapter 5

---

For more information about this document or the contracting companies, please visit <http://www.rfidconsultation.eu/> or contact:

William Stevens

[william@e-unlimited.com](mailto:william@e-unlimited.com)

Europe Unlimited

Place E. Flagey, 7

B-1050 BRUSSELS

Belgium

+32 2 644 65 80

[info@e-unlimited.com](mailto:info@e-unlimited.com)

Maarten van de Voort

[voort@rand.org](mailto:voort@rand.org)

RAND Europe

Newtonweg 1

2333 CP LEIDEN

The Netherlands

+31 721 524 51 51

[reinfo@rand.org](mailto:reinfo@rand.org)

# Contents

---

Preface .....	iii
Acknowledgements .....	vii
Abbreviations .....	viii
CHAPTER 1 Introduction .....	1
CHAPTER 2 RFID application domains and emerging trends .....	3
2.1 How is RFID applied in the European supply chain, distribution & retail sectors and the product life cycle?.....	3
2.2 How can RFID positively impact on European transport and logistics? .....	6
2.3 How can the EU and Member States stimulate the use of RFID within eGovernment and the public sector? .....	8
2.4 What opportunities should Europe explore using RFID to safeguard the health of its citizens and the competitiveness of its pharmaceutical industry? .....	10
2.5 How can RFID support new mobile or Internet applications and what are the policy implications? .....	12
2.6 Summary of policy issues and options with regard to applications.....	13
CHAPTER 3 RFID security, data protection & privacy, health and safety issues .....	17
3.1 What are the policy issues related to security, privacy and safety of RFID? .....	17
3.2 What are the policy options open to mitigate security, privacy and safety concerns of RFID?.....	19
3.3 The international context of RFID .....	22
3.4 What are the security, privacy and safety aspects raised by application or sector domains?.....	23
3.5 Summary of policy issues and options with regard to security, data protection & privacy, health and safety issues .....	24
CHAPTER 4 RFID interoperability, standardisation, governance and intellectual property right issues.....	29
4.1 What is RFID interoperability and standardisation?.....	29
4.2 RFID interoperability and standardisation in practice.....	30
4.3 Standards setting .....	32
4.4 RFID Integration with the Network.....	33
4.5 Intellectual Property Right Issues.....	35
4.6 Summary of policy issues and options with regard to RFID interoperability, standardisation, governance and intellectual property right issues.....	37
CHAPTER 5 RFID frequency spectrum – requirements and recommendations.....	41
5.1 What are the main policy issues related to RFID frequency spectrum? .....	41
5.2 What problems do users face in implementing RFID?.....	42
5.3 What are the technological and policy options related to RFID frequency spectrum? .....	44

5.4	The regulatory and standardisation challenges ahead.....	45
5.5	Research on EMF and RFID reading ranges .....	46
5.6	Summary of policy issues and options with regard to RFID frequency spectrum .....	47
	Disclaimer.....	51

## Acknowledgements

---

We would like to thank all participants to the workshops and in particular the presenters and moderators for their contributions. In addition, we thank the working group members from the European Commission for their constructive comments and stimulating discussions.

# Abbreviations

---

3G	Third Generation (standard for wireless networks)
CEN	European Committee For Standardization
CEPT	European Conference Of Postal And Telecommunications Administrations
DNS	Domain Name Service
DRM	Dense Reader Mode
EMF	Electro-Magnetic Frequencies
EPC	Electronic Product Code
ERC	European Radio communications Committee
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standardisation Institute
FMCG	Fast Moving Consumer Goods
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HF	High Frequency
IATA	International Air Transport Association
Ipv6	Internet Protocol Version 6
ISO	International Organization For Standardization
kHz	Kilohertz
LBT	Listen Before Talk
MHz	Megahertz
NFC	Near Field Communication
OECD	Organisation For Economic Co-Operation And Development
OEM	Original Equipment Manufacturer
ONS	Object Name Service
OSS	Open Source Software
PET	Privacy Enhancing Technologies
PTA	Privacy Threat Analysis
R&TTE	Radio And Telecommunications Terminal Equipment Directive
RAND	Reasonable And Non-discriminatory
RFID	Radio Frequency Identification

SME	Small And Medium-Sized Enterprises
SRD	Short Range Devices
SSL	Secure Sockets Layer
UHF	Ultra High Frequency
ULD	Units Load Device
US FDA	US Food And Drug Administration
UWB	Ultra-Wideband
VAS	Value Added Service
VHF	Very High Frequency
WWAI	World Wide Article Information



Radio Frequency Identification (RFID) attracts attention from citizens, NGOs, businesses and policy makers throughout Europe, because of its potential for improving inter alia supply chain logistics, transport, asset tracking, theft prevention, counterfeit detection, and thereby improving security and health for the European Community. On the other hand RFID is viewed with some suspicion as it is associated with tracking & tracing of persons, profiling of individuals, and the human/employment consequences of radical organisational change. As the development of RFID technology is still in full swing, it is difficult to say the final word about the opportunities and threats of RFID. Even though most stakeholders are still unaware of the potential and risks of RFID, opposing camps seem to have already formed. In order to further the debate in a more objective manner, the European Commission sees its role as providing a balanced overview of the state-of-play and the possible actions needed. For this purpose the Commission organised an extensive public consultation process, which will result in a Communication document on RFID at the end of 2006.

As a first step in this consultation, the European Commission organised five workshops with experts and stakeholders from all over Europe. On 6 and 7 March 2006, the European Commission hosted a technology-oriented workshop that provided an overview of the technological state of RFID development. The workshop on RFID application domains and emerging trends, held on 15 and 16 May, focused on the economic and societal rationale for different RFID applications; it also set the stage for three subsequent ‘horizontal’ workshops: one on RFID security, privacy, health and safety issues (that was held on 16-17 May), one on RFID interoperability, standardisation, governance and Intellectual Property Rights (1 June) and one on frequency spectrum requirements of RFID (2 June).

The workshops on 15, 16 and 17 May featured 57 distinguished speakers and attracted 243 participants. Also, remote access to the conference with web streaming of the presentation was available: On Monday 15 and Tuesday 16 May, nearly 500 server requests were received. On Wednesday May 17<sup>th</sup>, 211 successful server requests were received.

The workshops on 1 and 2 June featured 35 distinguished speakers from a wide range of organisations and attracted, on average, 75 participants. Again, web-streaming services were provided and offered the opportunity for remote interaction with panellists: On Thursday 1 and Friday 2 June, nearly 750 server requests were received.

This document presents the outcomes of these sessions. In addition to this document, a condensed report titled ‘Your Voice in Europe’ is available on the website at [http://europa.eu.int/yourvoice/index\\_en.htm](http://europa.eu.int/yourvoice/index_en.htm), and is open for comments until mid-September 2006.



## CHAPTER 2 RFID application domains and emerging trends

This chapter reflects the outcomes of the workshop on RFID Application Domains and Emerging Trends, which was held on May 15 and 16 in the Charlemagne building in Brussels. The event lined up 30 speakers from industry, academia and the European Commission. The structure of this chapter follows the structure of the workshop, which was split in different sessions. As similar topics were addressed in different sessions, these topics may also be addressed in the different sections of this chapter.

The workshop provided a broad overview of the current and near-term uses and benefits of the technology and where possible indications were given on market potential or the importance of the technology for industry and users. It was felt to be important to consider differences in characteristics of applications and the issues and policy options that specifically relate to these applications. To be able to get a clear understanding of the issues that come into play with the introduction and proliferation of RFID we need to distinguish between fields of application. This workshop distinguishes between RFID applications in 5 areas/sectors:

1. Goods supply chain;
2. Transport and logistics;
3. eGovernment and the public sector;
4. Health and the pharmaceutical industry;
5. New mobile or Internet applications.

The following sections will each go into a type of application. The sixth and final section will summarise the policy options and issues suggested in the preceding sections.

All of the opinions expressed, and evidence presented, in this summary are those coming from participants in the workshops and do not necessarily reflect the opinions of the authors or the Commission.

### 2.1 How is RFID applied in the European supply chain, distribution & retail sectors and the product life cycle?

RFID is likely to become more pervasive with forecasted yearly growth rates of 57% worldwide and 46% in the EU. Part of this growth is driven by new applications and technologies (such as linking RFID to biometrics). The most pervasive applications both now and in the near future are likely to be seen in supply chains.

The purpose of supply chains is to channel goods through supply networks from manufacturer to end-consumer. In order to do this efficiently and in a coordinated timely manner, transparency of supply chains is a prerequisite. If you cannot see what you are moving, you cannot control it, and if you cannot control it, effective timing and planning is impossible, leading to inefficiencies. These inefficiencies include out-of-stocks and phantom inventory, reduced utility rates of production lines, inefficient ordering, and also theft, and counterfeiting, all of which comes at a high cost.

RFID could potentially greatly improve transparency in supply chains and invigorate control driving out inefficiencies. Although RFID's transparency benefits can be reaped to their fullest when end-to-end solutions are implemented, also implementation along parts of the supply chain has shown to be successful. This leads to the following classification, in particular relevant for distinction of possible privacy issues: closed circulation, open circulation, and no circulation.

In *closed circulation* systems RFID tagged items (such as containers) do not leave the internal distribution system of a company or supply chain. Closed circulation is typically applied in asset management systems (for instance to trace at which point crates or containers disappear from the supply chain) and fleet management purposes. Although the investments to implement closed circulation systems are relatively low, companies tend to be reluctant in implementing these types of cost cutting investments, since operations are already perceived "good enough". In addition, ERP systems need to be adapted to handle RFID data as a circulation system instead of units just going through. Moreover, the costs of units (such as containers) are dropping, reducing the impact of loss of these units. Many companies tempted to implement RFID systems are scared off by the perception that they risk investing in a system that will turn out to be incompatible with other, supply chain partners', systems. Privacy issues with these types of systems are limited to employees rather than consumers, since in some cases the tags on units load devices (ULDs) can be linked to specific employees and their performance).

In *open circulation* systems multiple users are using open standards to handle and monitor the flow of tagged ULDs (such as containers, pallets, and their cargo) throughout a supply chain. As a result more items need to be tagged compared to closed circulation systems (since not just ULDs for internal but also those for external use need to be tagged) and thus a far larger investment is required (typically by multiple supply chain partners). Since multiple partners are reading the tags, interoperability issues arise and standards are important. The lack of these standards is hampering open circulation proliferation. The benefits of RFID in open circulation include creating real time transparency, which brings accuracy and certainty.

A recent internal supply chain RFID application pilot<sup>3</sup> on razorblades revealed a 20% productivity increase in distribution centres, less inventory required, better availability, faster checking, and faster loading. Another pilot<sup>4</sup> on similar products was used to check whether shops were compliant with promotion actions. Shops that were compliant showed improved product availability, resulting in an increase in customer satisfaction and increased sales. The pilot also illustrated that RFID applications can assist manufacturers to identify non-compliance of retailers in promotion activities. A

---

<sup>3</sup> Procter & Gamble (2006), The Electronic Product Code "At the Cutting Edge", Internal Gillette Pilot.

<sup>4</sup> Procter & Gamble (2006), The Electronic Product Code "At the Cutting Edge", Venus Disposables Promotion Pilot.

third supply chain pilot<sup>5</sup> found timesavings in warehouse and store processes (faster handling of incoming goods and faster data verification). However, the pilot also revealed that limited and non-harmonised frequency bands are still problematic and an active promotion of RFID in Europe could stimulate take-up.

In spite of these encouraging pilot results, limited and non-harmonised bandwidths adversely affect RFID take-up in Europe compared to the US, especially in the UHF range. Both for the air protocol and the tags' data structure uniform standards could invigorate investments in RFID.

In addition, due to size and associated market power advantages compared to their European counterparts, US retailers are able to impose standards in a supply chain and force suppliers to adhere to these. The size of retailers in the US also introduces advantages of scale resulting in fully loaded trucks loaded with fairly uniform cargo or at least package type (pallets, boxes, etc.), which simplifies RFID reading. In Europe, many RFID promotion activities are national and disregard the fact that companies work and thus need initiatives and standards internationally. Disseminating the successes of RFID implementation could stimulate RFID uptake. Also the sharing of experiences in using RFID by companies could stimulate RFID uptake.

In *no circulation systems* individual items / products are tagged allowing inventory management and tracing products in the supply chain from manufacturer to end-user (end-to-end systems). In retail applications RFID supports speeding up processes as readers can identify multiple tags at once (for example a shopping cart going through a shopping portal) and reduces stock-outs. These types of systems currently are not feasible for all types of consumer goods mainly due to the cost of equipping each item with a tag and the challenges associated with analysing the large data flows delivered by these systems in a useful way. The recently launched Gen2 standard is offering improved performance and is cheaper compared to previous standards, making the tagging of cartons feasible. Eventually a digital supply chain might become feasible, although this would require the cost of tagging to drop even further which is not foreseen within the next decade. However, in high tech markets and for recyclable products there are already some examples of item level tagging (such as for razorblades).

These types of applications may enable coupling a tag to a specific consumer, introducing various privacy concerns. The link between tag and consumer may come about by the consumer carrying or wearing tagged products and using unique personal identification, such as a loyalty card or bank / credit card. Due to the myriad of tags and tag functionalities available, it is vital to apply the appropriate tags in the appropriate environments. In end-to-end solutions standardised tags on an open standard basis could be applied encompassing a kill option on check out to empower consumers to safeguard their privacy. EPCglobal guidelines<sup>6</sup> require that consumers should be notified of the presence of a tag by fitting the product with a label. Currently these guidelines function as a code of conduct on a voluntary basis without enforcement. The choice and thus responsibility for deactivating the tag is with the consumer. If the tag is not deactivated, the consumer may use tag information after check out for recycling or retrieving product information.

---

<sup>5</sup> Procter & Gamble (2006), The Electronic Product Code "At the Cutting Edge", Gillette Fusion Launch.

<sup>6</sup> [http://www.epcglobalinc.org/public/ppsc\\_guide/](http://www.epcglobalinc.org/public/ppsc_guide/)

In all types of circulation systems the value reaped by businesses from RFID is in the data that can be collected from RFID tags. Collecting these data introduces responsibilities regarding secure handling and storage. Integrity needs to be built in at device and network level (privacy by design) and this network needs to be monitored continuously. In addition, the large volumes of data that become available through RFID deployment pose challenges to the validation of data and to distilling useful data. There seems to be a need for middleware equipment taking some weight of the shoulders of ERP systems since these may otherwise become overloaded.

## 2.2 How can RFID positively impact on European transport and logistics?

In the early 80s paperwork was used to control logistical processes, whereas today we typically use barcodes. The problem with barcodes is that they cannot be rewritten and require line of sight to be read. In future, RFID will enable dynamic monitoring and self-organised micro-devices. RFID allows automated scans at different points and continuous data collection. Also, RFID tags can be rewritten to allow for decentralised data storage. This opens the door for purposes including quality monitoring, asset management, temperature monitoring, and track & trace and automated inventory management of high value goods. RFID is only a first step towards intelligent object networks.

Several applications of RFID in transport have been researched and have been shown to be useful:

- Electronic Seals on containers, which are destroyed when containers are opened;
- Observation of transport of animals;
- Fleet management of trucking companies;
- Sea container tracking;
- Collecting tolls;
- Enhancement of road safety;
- Logistics; and
- Combating counterfeiting and theft.

The development of RFID technology can lead to an image of a holistic logistics supply chain, in which individual units (such as packages and boxes) are tagged allowing them to interact with information sources (such as the Internet) to organise their own movement through supply chains from manufacturer possibly all the way to end-consumer: an 'Internet of Things'. However, a precondition for such a pervasive deployment of RFID is that chips become cheaper, which may be achieved by research in materials and printing techniques.

As RFID increases transparency, its application can assist in combating counterfeiting and theft, both of which typically are the work of organised crime. These issues pose a significant problem to industry, introducing additional cost and insecurity to distribution systems, but also affecting consumer interests such as food safety and security. Currently there are several pilot studies ongoing issued by consortia of

manufacturers to combat counterfeiting<sup>7</sup>. A first recommendation that stems from these studies is that the best point of intercepting counterfeit goods is at the border instead of in the store. Reaping the potential benefits from RFID in combating counterfeiting requires companies and Customs to cooperate.

RFID also has a wide range of uses in vehicle identification. Nevertheless, using RFID in vehicle identification is challenging because of physical limits. Implementing RFID requires living with tradeoffs between speed, reliability, size, range and power needed. RFID applied at long ranges will make it difficult to localise items, especially if several items are within the same zone. Currently there already are many examples of vehicle identification in toll systems around Europe and in the US. The tradeoffs mentioned above are typically resolved by having vehicles pass through a single lane at modest speeds, easing the requirements to the RFID system. A further deployment of RFID in vehicle identification systems will require improved reliability and security in RFID technology. Reliability is important with regard to the handling of exception cases, adding cost to RFID deployment in vehicle identification. In systems that gather information from tags that can be linked to individual users (such as in many vehicle identification systems), it is important to transparently show to users that different operators have different levels of access to data, ensuring the privacy and security of these users. In this field, standards such as the CEN TC278 standard for electronic license plates are very important. Both standards for technologies and for processes could be promoted.

Another type of payment system in which RFID can be and currently is used, is in public transport. An RFID fitted card enables payment for single trips, independent of the modalities used. Depending on the functionalities offered (such as reduced duration of the trip, better seat availability, and intermodal connectivity) both public transport and non-public transport users have shown to be willing to bear the cost of these systems. Also in this field of application, standards and interoperability can be problematic, as multiple (public) transport providers need to cooperate and adhere to the same standard. Regulators may have a role in implementing new technologies.

In container transport RFID is driven by increased security requirements, capacity problems in container ports and the complex planning and control of multimodal cargo flows. Different applications can be conceived using RFID in containers: electronic seals, container tags, and also wagon tags. Fitting a seal with an RFID tag is an evolutionary step that is relatively cheap, easy to understand and easy to implement. Barriers to RFID proliferation in container transport are typically related to establishment of and adherence to global standards. Currently ISO 18185 for electronic active seals and ISO 10374 for passive container tags have been issued in this area. The practicalities of these standards still need to be tested. Smart containers, equipped with RFIDs linked to sensors to increase functionalities, could add additional sensing functionalities, such as temperature, light and specific chemical substances. Although these types of functionalities may be required to increase the security of container transport and obviously add to the level of transparency offered, their introduction is challenged by their energy requirements and cost allocation. Lower insurance premiums for secure containers could stimulate the use of these technologies, although insurance companies so far have been reluctant to lower premiums without proof of increased security. The support of pilot projects proving concept and identifying

---

<sup>7</sup> Marcello Barboni, Joint Research Centre (2006), RFID Applications.

financial benefits for insurance companies may stimulate RFID use to secure containers.

From the discussion it may be concluded that interoperability, standards and cooperation are important themes in applying RFID to transport. Additionally, as transport typically occurs in an international environment, the design of RFID equipped systems benefits from including administration and law enforcement (including Customs).

### 2.3 How can the EU and Member States stimulate the use of RFID within eGovernment and the public sector?

RFID offers applications to the benefit of both governments and citizens. From combating forgery of official documents to increasing transparency in document flows and services for citizens, RFID applied in eGovernment and the public sector typically is a way of doing old things differently. Applying RFID may benefit public sector processes by making them more reliable, transparent, efficient, and faster. Examples of promising prospects of deploying RFID in the public sector include:

- Workflow optimisation;
- Speed up of working processes;
- Collection of statistical information to increase administrative processes' transparency;
- Tracking of stolen goods by the police and customs control;
- Monitoring and controlling administrative processes;
- Enhancing document management (although paper may not become obsolete and still needs to be stored);
- Ticketing (which also enables finding lost people and attaining insight into the logistics of the sites);
- Integrated tourist ticket, which requires cooperation among the many parties involved;
- Luggage handling connected to ePassports.

However, so far RFID has not proliferated greatly in these fields of application. As there is no central body of knowledge, Member States tend to reinvent the wheel, which may introduce interoperability issues. Similar as with applying existing standards to new applications, in many cases existing standards can be adapted and adopted, and may function as examples that can be adopted by or adapted to other sectors and by other countries. A central body of knowledge could promote a clear strategy or master plan for RFID, which would invigorate RFID deployment over isolated projects. Some governments seem to embrace the idea that RFID may improve a country's global competitive position. The Australian government for instance recently announced a \$1.1 billion smart card plan<sup>8</sup> replacing 17 current applications. The EU or Member

---

<sup>8</sup> B.W. Schermer, RFID Platform Nederland (2006), An academic and market perspective on e-government RFID applications.

States could also implement such plans, supporting new applications and spreading knowledge. In addition, the EU could stimulate research that addresses barriers to RFID proliferation. Obtaining funding for this type of research currently seems relatively difficult in Europe.

Another issue associated with implementing RFID in the public sector, is that in many applications RFID tags can be linked to individual users / citizens, which may introduce privacy and security concerns. Although these issues are not uniquely related to RFID use and need to be tackled irrespective of a specific technology, they do need to be addressed in designing RFID applications in the public domain. Privacy by design in public domain applications needs to encompass the processes of collection of data, storage and data management. Some speakers note that citizens should be able to either access or be aware of the data stored on them. In the end, if data collection and management are open to misuse, people may tend not to trust or use the system.

A segment that may require government stimulus to further incorporate RFID is SMEs. Currently SMEs seem sceptical about the value proposition of RFID. Although two out of three IT executives see positive chances for RFID, this typically depends on the size of the company. In SMEs, the approach seems to be focused on adhering to supply chain manager and government mandates, also known as Slap & Ship: tagging items on shipment without adding any benefits for the SME itself. SMEs require a friendly ecosystem to pick up the technology: basic compliance packages, managed services and turnkey solutions, vendor independent expertise and consulting. This can be achieved through: stimulating SME vendor networking to build SME tailored services; funding of RFID competence centres; and stimulating knowledge diffusion. A good example of how governments can stimulate RFID uptake among SMEs is the German RFID support centre, which provides consulting, good practice databases, guidelines and checklists. Another good example is the German RFID for SMEs road show. These ways of supporting SMEs appear most effective, as SMEs are worried of over-coordination.

Other ways in which governments can invigorate the use of RFID applications is by acting as launching customer, similar to the role the US government is playing in e-procurement in the US military supply chain. Policy options that are open to the EU and Member states include:

- Framework 7 funds that can be allocated to research communities involving SMEs;
- Facilitation of consultation sessions, platforms, position papers and discussion;
- Monitoring of what has been done;
- Introduction of RFID options in sectoral networks.

Discussants during the workshops argued that self-regulation or co-regulation and guidance would work better than new legislation.

## 2.4 What opportunities should Europe explore using RFID to safeguard the health of its citizens and the competitiveness of its pharmaceutical industry?

Market predictions suggest that RFID deployment in healthcare is to grow from \$90M in 2006 to \$2.1 billion in 2016. Applications that may contribute to the proliferation of RFID in healthcare include:

- Tracking / tracing patients;
- Patient prescription compliance;
- Reducing medication errors;
- Assisting (visually) impaired;
- Tracking medicines for anti-counterfeiting measures;
- Blood tracking; and
- Improving workflow processes in hospitals.

The use of RFID may instigate privacy concerns, which, combined with the privacy sensitive nature of healthcare, demands that additional safeguards be considered in the healthcare sector. Aspects that could be part of the design of these systems should incorporate: proper notice of RFID use, appropriate consent of tag carriers, the option to 'opt-out', and secure storage and transfer of data.

### Tracking / tracing patients

Location tracking with active RFID has a range of applications, such as determining the location of a patient that needs urgent care (e.g. an operation). As location technology can expose identity, it is important that for these applications the OECD guidelines for data protection are followed.

### Assisting (visually) impaired

RFID can be used as beacons for visually impaired, with an antenna embedded in a walking stick. This type of RFID applications could contribute to the EC's i2010 e-Inclusion policy.

### Preventing wrong medication

By applying RFID to both patient and drug, a decision support system could assist hospital personnel in administering drugs and preventing mistakes. RFID by itself is unlikely to provide any significant benefits; it is the coupling with decision support systems that could reduce mistakes. However, these systems would only function as a back up; the health care professional remains accountable for administering the drugs. RFID is not essential to bring these benefits: also (the cheaper) 2-dimensional (2D) barcodes<sup>9</sup> could be used for these purposes. A system making use of these codes could later on be amended to include RFID technology instead of 2D barcodes.

RFID systems are more difficult to use outside the hospital in primary care settings, in which medication errors also occur. RFID may be useful at the pharmacy, the point of dispensing/sale. In addition, it should also be noted that deploying RFID introduces

---

<sup>9</sup> Essentially, a 2D barcode (or matrix) is like a barcode, but made out of dots on a grid, which allows for more information to be stored.

privacy concerns and customers should be able to decide whether to switch off the tag. This would imply that when consumers leave a pharmacy, tags could be either deactivated or set to privacy mode.

#### Combating counterfeited drugs

By assigning unique identifier codes to medication, counterfeit drugs can be identified. Although counterfeited medicines are a major challenge in developing countries, the issue is also raising concerns in Europe. In order to combat counterfeited medicines, tagging cartons or boxes suffices and individual item level tagging is not required. Tagging cartons or boxes also introduces few concerns for privacy compared to tagging individual products. The number of intermediaries making up the medicines supply chain complicates securing the supply chain along all parties involved. Tagging boxes or cartons would secure the medication distribution system at the manufacturer (the manufacturer fits boxes with RFID tags that uniquely identify the consignment), at border crossings, and at the point of sale (the tags on the boxes identify manufacturer, date of product preparation, etc.). As stated, these purposes do not necessarily require RFID deployment: 2D barcodes can provide similar functionalities at less cost, although, as speakers highlighted, this solution also requires prior harmonisation of labelling standards throughout Europe.

#### Blood tracking

Tagging and thereby tracking blood bags offers opportunities to improve patient safety for instance by enhancing blood group matching, etc. When sensors are combined with RFID tags, the exposure to high temperatures that may spoil the blood can also be tracked.

#### Improving workflow processes in hospitals

RFID has been successfully applied to a large number of logistics processes in supply chains. Since some of these processes are quite similar to some hospital processes, RFID could improve the efficiency of these processes (e.g. cleaning in hospitals, food distribution, expiry date registration on medication, etc.)

In conclusion it can be said that hospitals could use RFID technology to enhance patient safety and assisted living, as there is clear potential, to be further explored. One speaker made the remark that in Europe every year three times more patients die due to avoidable mistakes than in car accidents<sup>10</sup>. So far primarily rudimentary applications have been tested, since testing integrated applications is difficult. Performing pilots to assess the effectiveness and feasibility of RFID in hospitals could be perceived as an important option to reduce the number of avoidable mistakes.

In the supply chain for pharmaceuticals, however, technologies such as 2D barcodes could provide more cost effective solutions with less deployment barriers and a similar level of enhanced safety.

Another link between healthcare and RFID is the issue of the potential impact of RFID on the health of those coming into contact with the technology. Studies so far appear not to have been able to detect an effect of RFID on public health<sup>11</sup>. Even though no

---

<sup>10</sup> Prof. Dr. D. Grandt, Klinikum Saarbrueken (2006), Opportunities and problems of using RFID in healthcare.

<sup>11</sup> Marcello Barboni, Joint Research Centre (2006), RFID Applications.

negative consequences have been shown, employees working in RFID environments may still believe that there is a health issue.

## 2.5 How can RFID support new mobile or Internet applications and what are the policy implications?

RFID is a family of technologies rather than a single technology that facilitates unique identification. The use of RFID in modern mobile life (e.g. coupling a payment-function to mobile phones) is already common practice in Japan. Tracking mobile assets and people (e.g. automatically transferring your phone to the office or meeting room you are in, monitoring visitors, etc) applications are no longer science fiction. RFID may be used to retrieve product details of tagged goods or street posters. Combining RFID, mobile and location technologies make many more innovative services feasible. Many of these applications rely on Near Field Communication (NFC): a wireless short-range communication technology that is already supported by existing infrastructure. Similar to other RFIDs, there is a large group of technology stakeholders ready to implement NFC and field trials are taking place in Germany and France.

Similar to open circulation systems for other RFIDs, building useful applications (such as mentioned above) typically requires the cooperation of multiple stakeholders adhering to the same standards.

These applications require actual touching of other devices. This implies a deliberate act by the user to activate the reader. The fact that the user is aware of the technology and actively chooses to use it makes that this application of RFID technology allows for a relatively high level of security and privacy protection. However, in many of these applications the characteristics of the application allow for unique identification of the user and all unique identifier applications may lead to privacy issues.

However, policies should aim to be technology-neutral and assess the privacy consequences of each application individually. Especially with regard to tags carried by individuals (including tags in consumer items), it is important to determine which data is stored on the tag and how data collection and processing may enrich the datasets through correlation. The OECD has developed guidelines for data protection, which can function as a guidebook in designing these applications. These guidelines include recommendations for appropriate design principles for location-based applications, which may expose identity. It is important to be transparent and to aggregate at a level that does not compromise individuals. Users should be made aware of privacy implications.

Current privacy legislation seems to provide an adequate structure to encompass RFID regulation. However, guidance on how to provide notice and achieve informed consent of data collection is needed. Developing such guidance may benefit from involving a range of stakeholders, including manufacturers, service providers, retailers, consumer organisations, and governments. In order to achieve compliance with these guidelines, transparent, robust and harmonised enforcement will be necessary.

## 2.6 Summary of policy issues and options with regard to applications

The reduced cost of tags and their improved performance have opened new markets and applications (especially in logistics) to RFID, which has resulted in increased take-up. Improved standards have furthered RFID proliferation. Next steps towards further deployment would benefit from: developing chip and reader technology, solving interoperability and frequency allocation issues, and addressing privacy and security concerns.

Especially this last category (of privacy and security concerns) seems to be an obstacle in the further deployment of RFID as it hampers the proliferation of (potentially large areas of application including) no circulation systems. These systems may be used to collect personal data posing privacy concerns. Although there already is a legislative framework in place to protect personal data, this framework is not specific in describing a code of conduct to be adhered to in collecting this data. The cloaked and potentially ubiquitous nature of RFID calls for a review of current regulations to assess whether the current framework is successful in regulating privacy concerns related to RFID (type) applications. Government can help fit new technologies into existing rules.

In addition to the legislative framework, industry guidelines for collecting and handling RFID data are in place. However, adhering to guidelines is voluntary and lacks enforcement options to protect the public from non-compliant companies. Therefore guidelines, and thus industry self-regulation, is likely to prove inadequate to regulate privacy issues. This holds irrespective of the claim that as retailers' businesses rely on consumers' trust, they will not introduce technologies that are not accepted by the public. Any legislative framework should address both the collection and data handling (including storing) processes. The data that should be subject to this legislation is personal data or data that can be used to derive personal data. An important term in this respect is proportionality: privacy sensitive information should be subject to different levels of protection than logistic information. For privacy sensitive information informed consent should apply meaning:

- Data should be collected and handled in a transparent way;
  - o A tag carrier should be informed of the presence of tags; and
  - o Of the content, reading and use of the data on the tag;
- The tag carrier should consent to these practices.

As these rights lie with the tag carrier, tag carriers should be presented the possibility to opt-in rather than the possibility to opt-out. This practice would be similar to paying with plastic and loyalty cards which are optional for consumers; something that RFID should also be. Tag carriers can only consider to opt-in if they are aware of the presence of a tag. Therefore, clearly labelling products or other tag-carrying items (e.g. by using logos) is necessary. In addition, tag carriers should be able to deactivate tags. In order for a carrier to thoughtfully make the choice of either enabling or disabling the tag, a carrier should be aware of how data gathered from the tag will be used and potentially combined with other data and who can obtain this data.

Informed consent can only happen if tag carriers have a basic understanding of RFID technology and its applications. Therefore the public should be educated up to an appropriate level; but not be taught the details of RFID technology. Information would have to be easy, understandable, and targeted to the public's needs.

Informed consent is also required to inform the public of the advantages of keeping a tag alive. If activating the kill switch on RFIDs becomes the standard, it would disable certain RFID functionalities that are generally perceived positive (e.g. in drugs<sup>12</sup>). In such cases, there might be more to gain than to lose. Since different applications introduce different issues and concerns, it is important to distinguish between domains of applications and to apply privacy by design in which privacy issues are taken just as serious as technical issues<sup>13</sup>. Since we can envision scenarios showing positive benefits with the technology just taking off, we should be careful not to close off application areas through stringent protective privacy regulations before the technology is thoroughly researched.

If we want to promote RFID use, we should make sure that existing regulation facilitates rather than hinders it:

- Not all RFID applications introduce privacy concerns. Many applications that are perceived to be privacy invasive are not feasible now and are unlikely to become so within the next 10-15 years. There may be a role for FP7 with regard to scoping out potential issues and policy options for these future applications.
- There is a need to differentiate between areas of RFID application. If end users are not involved, such as in many supply chain applications, use is generally safe and privacy is not an issue.
- Use of data in the pharmaceutical sector is already strongly regulated. There does not seem to be a need for additional regulation, but rather for more uniform regulation between Member States.

Table 1 and Table 2 list the issues and policy options that were posed by presenters or discussants during the workshop, to illustrate the debate, which did not conclude with a consensus opinion about all of these issues.

---

<sup>12</sup> Some experts think all pharmaceutical items should be tagged. In the US, the FDA is promoting the use of RFID.

<sup>13</sup> Spam is another example where technology was introduced and on hindsight should have been better thought through regarding privacy issues.

Table 1 – Policy issues related to ‘RFID application domains and emerging trends’<sup>14</sup>

Open circulation proliferation is hampered by a lack of standards and non-harmonised frequency bands
Open circulation systems require large investment (by multiple supply chain partners)
In no circulation systems tag deactivation denies consumers to recycle or retrieve product information after check out
No circulation systems are frequently infeasible for consumer goods due to the cost of tagging each item
Retail applications of RFID are perceived to be privacy invasive and may be distrusted by consumers
In closed and open circulation applications privacy issues for employees may come into play
Applications that collect large volumes of data should be designed to validate and distil useful data
Using RFID in vehicle identification is challenging because of immaturity of RFID technology (at low cost)
In transport interoperability, standards and cooperation are important themes
Public sector applications may require cooperation among the many parties involved
Public sector proliferation may require further research on synchronisation, harmonisation, and security of data
The effects of RFID on people and medication are largely unknown
Employees working in RFID environments may believe that there is a health issue
Many supply chain applications do not add benefits for SMEs
Many applications are not very accessible to SMEs as SMEs require a friendly ecosystem to pick up the technology (basic compliance packages, managed services and turnkey solutions, vendor independent expertise and consulting)

Table 2 – Policy options related to ‘RFID application domains and emerging trends’<sup>14</sup>

Support new applications (e.g. by linking RFID to biometrics and sensors including temperature, light and specific chemical substances)
Explore the use of RFID technology to enhance patient safety and assisted living in hospitals
Educate companies to stimulate closed circulation applications
Bring together companies (and other stakeholders such as Customs) to stimulate open circulation applications
Create legal framework within which end-to-end (no circulation) solutions can be implemented
Empower consumers to safeguard their privacy by standardising a kill option on check out in end-to-end solutions
Bring together and educate companies on how advantages of scale (e.g. through fully loaded trucks loaded with fairly uniform cargo or package type) simplify RFID applications
Disseminate the successes of RFID implementation / Stimulate sharing experiences in using RFID by companies
Distinguish between shielding different types of information (e.g. privacy sensitive information and logistic information)
Inventory requirements of SME to engage in RFID systems (stimulate SME vendor networking to build SME tailored services, provide consulting, good practice databases, guidelines and checklists, RFID for SMEs road show)
Allocate FP 7 funds to research communities involving SMEs
Support RFID pilot projects proving concept and identifying financial benefits (e.g. for insurance companies to secure containers)
Support public domain applications by acting as launching customer for RFID systems

<sup>14</sup> During the workshop on ‘RFID application domains and emerging trends’ several issues were mentioned that are related to issues discussed in the following chapters (privacy, security, interoperability, standards, and, spectrum). These issues are included in these respective chapters.



## CHAPTER 3 RFID security, data protection & privacy, health and safety issues

The holistic character of the previous workshop already touched upon some of the main issues related to RFID. It also touched on issues relating to security, privacy and health, which could be impacted by the introduction and proliferation of RFID technology. These topics, which have been the focal point of most media attention and concerns, are explored in more detail in this chapter, which records the discussions in the workshop on RFID security, data protection & privacy, health and safety issues. The workshop was held on May 16 in the Charlemagne building in Brussels dedicated to these issues and the options that were identified to tackle or mitigate the concerns voiced.

The following four sections discuss the policy issues and options, their international context and the relation with the previous chapter Applications. The fifth and final section summarises the policy options and issues suggested in the preceding sections.

All of the opinions expressed, and evidence presented, in this summary are those coming from participants in the workshops and do not necessarily reflect the opinions of the authors or the Commission. Some content has unavoidable overlap with the previous chapter. Some statements made in this workshop may even be contradictory to comments made in the previous workshop (and chapter), which reflects the nature of the discussion and the opinions of different groups of experts.

### 3.1 What are the policy issues related to security, privacy and safety of RFID?

Privacy and security cannot be treated completely separate as these issues are closely connected: some form of security is required to ascertain privacy. The core principles in the discussion on privacy and security concerns are that (economic and personal) harm should be prevented and that RFID should be non-discriminatory and respect individual identity. In the discussion it was mentioned that technologies such as RFID can be seen as a structural threat to democracy, since collecting data introduces risks as data can become accessible to unauthorised persons.

Some workshop participants claimed databases may not be as secure as we tend to think and criminals may be able to misuse systems that collect data. These databases contain data associated with RFIDs, which can become personal data if the tag itself contains personal data, if the data on the tag can be linked to personal data in databases, or if the tracking of RFIDs reveals the movements or behaviour of individuals. However, other participants contend that current data protection principles (including

use of PET) work fine and can also be applied to RFID. Privacy by design should entail guidelines for the safe and transparent collection, processing and storing of data, irrespective of technology.

RFID may be a stepping stone towards ubiquitous computing, which together with technology-convergence may lead to seamless integration of the physical world with cyberspace. Although such an “Internet of Things” may offer vast beneficial opportunities to society, automatic participation in an “always on” Internet does not comply with the privacy principles set out by the OECD in 1981. These principles, which closely relate to privacy by design, are still valuable today as they warn against:

- *Lack of specificity*: a system should be specifically designed to gather a limited set of data. In RFID, data is often gathered because it is possible instead of because it is necessary: it seems like a solution looking for a problem.
- *No limitations on data collection*: a system should be bounded spatially or temporally in the extent to which data can be collected and stored. Although privacy is a dynamic concept that is culturally bounded, two general concerns with RFID can be identified: 1) who controls information; and 2) who has access to it? The organisations that collect data should be held responsible for safeguarding the data instead of the general public. A technology-specific concern with RFID data collection is that citizens may be unaware of carrying tags, which can be unknowingly read from a distance (eavesdropping), enabling individualised identification and revealing personal data. Tests reveal that tags can be read far beyond the distance for which they are designed (e.g. an ISO 14443 tag designed to be read from 10 cm, can also be read from 3 m given the right equipment).
- *Loss of confidence and trust*: loss of transparency and lack of control. Consumers are concerned about unauthorised readouts of tags, retrieval of social networks (e.g. retrieval of behaviour and social patterns) and technology paternalism (products that take over your life; think instead of you). In short: people are afraid of losing control. Although consumers do enjoy benefits of RFID (e.g. seniors do appreciate applications such as a smart fridge and medical applications), many rather want to kill the tag than enjoy the technology.

Some consumer organisations criticise RFID applications for identifying specific individuals. Although according to one speaker item level tagging will not take place within the next couple of years, this is one of the main applications consumer organisations worry about. Reading tags carried by people (who do not consent) could reveal information on their shopping preferences, which is valuable information to businesses. Although companies tend to play down the use of RFID data, there is a conflict between the consumer’s interest and business interest for which a compromise should be found. Such a compromise may entail the use of guidelines to describe how RFID systems may be applied. The value of guidelines partly is to create consumer awareness and awareness of the rights of consumers in the sector. Studies by marketing professionals<sup>15</sup> reveal that, if consumers are not well aware of the implications of RFID use, they tend to play down the privacy issue as they place higher value on the benefits RFID may offer to them. Consumers may set aside their privacy concerns to reap these benefits.

---

<sup>15</sup> Srivastava, ITU (2006), Considerations of privacy and data security in the context of RFID.

In addition to consumer related privacy concerns, RFID may also pose privacy concerns in captive relations such as employees versus employers and citizens versus governments.

An issue that was not mentioned very prominently in the session was the health and environmental effects of RFID use. Discarding RFID tagged packages and products may cause environmental damage. At present, little evaluative evidence seems available. Also the issue of healthcare effects of electromagnetic radiation was only briefly mentioned. According to DG SANCO<sup>16</sup> there is no conclusive evidence of the influence of radio signals on health. However, there is an obvious risk of perception, as a poorly informed audience may believe there are health risks and reject the technology. The topic is further addressed in the workshop on frequency spectrum issues.

### 3.2 What are the policy options open to mitigate security, privacy and safety concerns of RFID?

Policy options to mitigate privacy, security, health and safety issues include legislative, technical, data management and educative / informative options.

#### 3.2.1 Legislative options

Especially for measures that should be implemented by non-governmental bodies (such as retailers) it needs to be made clear whether compliance is voluntary or mandatory. One may think of a strong legal approach in which such control of data is enforced. However, not all the speakers at the workshop were in favour of strong legal enforcement, as it may hinder the development of a technology that is still in its early stages. Therefore, an option presented (and already proposed by e.g. EPCglobal) is to implement a code of conduct / guidelines. Such a code should be developed in cooperation with consumer organisations and deal with issues such as:

- Consumer friendliness;
- Interoperability;
- Sustainability; and
- Transparent use of data gathered through RFID applications.

The code could describe how RFID presence is stated on product or packaging and the possibility to remove RFID tags or make them dormant after the sales process. According to consumer association speakers, no secret tags and readers should be allowed. In addition, information on RFID tags could be minimised and data collected on consumers should be transparent and accessible. At all times it should be possible for the consumer to detect RFID tags and readers. If the potential impact on privacy is significant, tags should incorporate functionalities to safeguard privacy even if this functionality is costly. As a way of informing tag bearers that tags are being read, the code may include guidelines on the position of readers.

Also the linking of data sources is something that may be addressed in these guidelines as consent for two separate applications does not mean that combined application is agreed upon. Finally guidance could be given to make the system more transparent; this

---

<sup>16</sup> Marcello Barboni, Joint Research Centre (2006), RFID Applications.

is specifically relevant for the software used (open source software). These latter elements are not included in EPCGlobal's code of conduct, which provides little guidance on software that is used to process.

However, setting guidelines and agreeing on a common code of conduct has proved to be challenging. Typically guidelines on consumer privacy and RFID established by a group of companies are not supported by all retail companies (e.g. EPC Global standards do not reach all partners in a supply chain).

In addition, compliance with guidelines is typically voluntary and not enforced. On the other hand, establishing strict regulation to safeguard privacy may hinder the development of RFID. There may be a compromise between strict regulation and voluntary guidelines in which companies are penalised with high fines if they breach privacy guidelines. In assessing whether companies are adhering to guidelines focus should be on areas where there is a particular challenge to fair information. In many cases notice by itself is insufficient and should be supplemented by consumer education.

Regulation on RFID is only valid for a specific timeframe; due to advances in technology regulation can become obsolete and therefore one should be careful with early legislation. EU guidelines should be at the basis of the regulatory framework on top of which local laws (including codes of conduct, best practices, training and awareness) and sector guidelines can be introduced to guarantee privacy. Since RFID is at early stages, guidelines need to be flexible and adaptive and technology-neutral.

At this stage of RFID development, self-regulatory programs and guidance seem most appropriate and should be encouraged. Information security is an ongoing process. A company's security procedures should be reasonable and appropriate, and a breach does not mean that a company failed to have reasonable security measures. Furthermore, RFID usage and deployment should be monitored. In such a self-regulatory environment consumer control is not very likely. Therefore, technologies such as Privacy Enhancing Technologies (PET) could provide solutions. There is a joint responsibility of retailer and manufacturer to adhere to such a code. However, from a legislative perspective we need accountability instead of trust.

Since a lot of aspects of RFID (e.g. health effects and privacy effects in the long run) are not yet well known, some advocacy groups for privacy protection suggest a standstill on the rollout of RFID and a possible prohibition on applications that require implantation of RFID chips.

### 3.2.2 Technical options

As was also mentioned in previous workshops, several speakers hint that privacy should be part of the design of an RFID system. Privacy can be introduced in several ways: from the consumer's side and from the technology deployer's side. A consumer can protect himself through different means: aluminium foil (Faraday cage), RFID sensor detection, active jamming, and RFID zappers (destroying the tag). At the point of sale, other activities can be undertaken: de-active the tag, and hash lock or re-encryption of the tag. Below, we will go into more detail on some of the promising technical options that were suggested during the workshop.

#### *Deactivation*

Deactivation or killing the tag to avoid the system to transcend from a closed circulation system to a no circulation system (e.g. an item level tagged system) typically occurs on check-out or leaving the premises in which the tag was meant to be

read. Deactivation allows retailers to retain the inventory management benefits RFID has to offer, but prevents retailers exploiting data collection from tags that were deactivated on previous checkouts. If these tags would not have been deactivated they might have provided the retailer with a better understanding of the consumers' shopping behaviour. Keeping these tags alive may however induce privacy concerns on the side of the consumer, as individual behaviour of the consumer may be recorded and possibly (in the case of identity information that can be read from loyalty cards, identity cards or other RFID tags that may uniquely identify a consumer) reveal the consumer's identity.

Measures that can be taken in order to enhance privacy may also have adverse effects on the (intended) functionality of RFID. For instance, deactivating or 'killing' a tag on check-out in order to avoid the tag being read outside the store and protecting the carrier's privacy entails the tag cannot be re-activated afterwards and cannot be used in the process of recycling the product or retrieving product data by the consumer. Deactivation therefore does not only rule out providing information and value to vendors, but it also destroys potential value to the citizens who buy tagged products (e.g. recovering product information, warranty, and home inventory management). Furthermore, the kill-commands can be misused, for instance to kill a tag in the store preventing its detection when shoplifting the product.

#### *Encryption*

PET or encryption entails the coding of data on tags, which prevents unauthorised readers deciphering the content on a tag. However, anyone would be able to access encrypted tags (without reading the actual content) and may be able to track a carrier based on that information. In addition, using encryption or passwords may be problematic, as users cannot cope with a large list of passwords for different applications and uses. Moving encryption to the back end (e.g. implementing encryption at the point of labelling) would take away the burden from consumers, although they would then not be able to read the decrypted tag's information.

Encryption includes a large range of technologies, which may lead to standardisation and interoperability issues. However, selecting a single PET and mandating that by law does not seem to be advisable.

#### *Tag clipping*

One way to balance privacy with functionality needs is by clipping RFID tags. With consumers partly removing (clipping) the antenna from the tag the read range is reduced to that of a proximity range tag (approximately 5 cm). This enables the consumer to actively choose to limit the read range and enhance privacy. The basic idea about the clipped tag is that this privacy-enhancing technology should:

- Add the option of consumer choice;
- Provide confirmation that tags have been deactivated;
- Enable later use by completely breaking the tag.

If the technology for 'clippable' tags were further developed, the additional cost compared to plain RFID tags would probably be marginal. Although range is an important issue for privacy and reducing read ranges improves privacy, it does not offer robust security benefits.

### 3.2.3 Data management options

Data security does not merely consist of technical measures. Apart from the technological solutions that may be found to safeguard privacy, there may also be changes in organisation or legislation that would enhance privacy. For example, when the RFID tags reach consumers, introducing informed consent should protect consumers' autonomy and control. According to consumer protection speakers, it is a fundamental consumer right to decide what communication he/she engages in, so the decision which communications run via tags the consumer is carrying should at all times be with the consumer. Although some participants preferred to speak about "the consumer in control", than the value-laden terms opt-in and opt-out, the speakers for the consumer side preferred an opt-in strategy than an opt-out one.

Risks related to the storage and storing data in separate databases can mitigate handling of data. Splitting data over multiple separate databases would limit the dataset that would be disclosed in case of unauthorized access.

Data can also be anonymized to mitigate the risks associated with the handling and storage of personal data.

### 3.2.4 Educative and informative options

Consumer education is vital to understand technology and dispel myths. Furthermore, choices should be easy for consumers to exercise. Information concerning RFID should be clear, conspicuous and accurate. Research by Intel<sup>17</sup> suggests that users are unaware of the effects that RFID may have on their privacy– they believe applications to be generally benign.

RFID offers benefits to society (healthcare, food safety, process and service improvements, cost advantages leading to improved competitive position), but the technology also poses risks (according to one speaker, the ubiquitous nature of RFID potentially threatens values associated with democracy). To be able to balance these benefits from RFID and the associated concerns, a discussion is necessary on values, needs and conditions. Several speakers considered this workshop a good first attempt.

## 3.3 The international context of RFID

Supply chains and the companies composing them operate in a global arena. Therefore the RFID systems used in these supply chains need to suit this environment. To avoid having to deal with numerous different standards and (national) codes of conduct and legislation, global standards are required, also with regard to privacy legislation in spite of differing legal frameworks. There is concern that self-regulated codes of conduct leave too much room for diverging standards both legal (as self-regulation is not necessarily separate from governmental regulation) and in terms of values. International standardisation requires international dialogue and international research cooperation. There seems to be a role for international forums and an international body to come up with global standards. Regardless of how this takes form, it appears unlikely that national or regional legislation (such as EU legislation) that disregards the international context of RFID is the best way forward.

---

<sup>17</sup> Srivastava, ITU (2006), Considerations of privacy and data security in the context of RFID.

### 3.4 What are the security, privacy and safety aspects raised by application or sector domains?

As can be seen from the discussion in the Applications Workshop the issues of privacy and security are typically related to specific applications or fields of applications instead of related to RFID in a general sense. In this section we touch upon some of the interfaces between specific applications and privacy and security issues.

#### 3.4.1 Application specific concerns

At this point in time it seems premature to decide on general regulation. Application-specific solutions seem more appropriate as different RFID applications have very different security requirements as could be seen from Chapter 2. To further illustrate this, tagging participants in a marathon, cattle identification and luggage sorting examples are acceptable since no data is collected that can be linked to or is personal. However, automatic tagging shopping carts is a different issue as are ambient/ubiquitous uses since these applications often do enable linking tag information to personal data.

##### *Supply chain and retail*

Closed systems (including inventory and asset management and pallet level applications) in supply chains raise little concern with regard to privacy and security. Security issues may arise depending on the type of cargo involved, although this is generally not typically related to the application of RFID but rather related to unique identification (which is also enabled through for instance barcode systems). If these systems expand into open (networked) systems privacy issues may arise depending on the kind of application.

An exception to the statement above may occur when RFID systems allow for the tracking of employees, which may pose privacy concerns. RFID's capability to unique identification of employees (or materials that can be associated with these employees) may enable data collection on the performance of employees without their awareness or consent. However, there seems to be a consensus that in general there are sufficient legal frameworks available on the collection of data by employers.

Item level tagging may introduce both privacy and security concerns. Tagged items that can be read outside confined environments may reveal information to undisclosed / unauthorised readers. For this reason there should be a minimum level of security for all tagged products, regardless of the price of this functionality. Given the current uncertainties about potential (negative or illegal) RFID use, it is suggested to make RFID encryption mandatory.

The alternative, in the case where the tag and its information cannot be protected from unauthorised readings (for instance by means of encryption etc.), is killing the tag by default while leaving it on is made optional (opt-in versus opt-out). This would solve the issue of liability: i.e. who is liable if tag information gets out in the open or gets misused? If a consumer consents to carrying a live tag, disclosure of the tag's contents may be a calculated risk. However, in case the tag bearer is unaware of the tag, its protection, or the information stored on it, the question arises of who is liable in case of unauthorised access to this information.

Item level tagging can also be used to prevent counterfeiting. Counterfeiting, especially of drugs and valuable commodities, has become of growing concern to industry, though far less to consumers. Consumer organisations tend to view this application with some

scepticism as it is seen as the ultimate privacy-killing application. The application does not necessarily require item level tagging as typically tagging boxes and pallets to be inspected at borders, which are convenient choke points to intercept counterfeit goods, suffices. In addition, some participants claim that anti-counterfeiting and privacy concerns are not mutually exclusive. Lack of design considerations may introduce privacy concerns in this arena.

#### *Spare parts*

Another RFID application in logistics systems is in spare parts. RFID can assist in assessing whether spare parts are the right ones. These types of applications have large market potential, mainly for safety-critical applications. When these types of systems are used for non safety-critical applications, there is a risk of illegal competition issues.

#### *Healthcare applications*

Predictions suggest that RFID in healthcare is going to grow from US\$90M in 2006 to US\$2.1 billion in 2016. There are many useful RFID applications in healthcare: tracking medicines for anti-counterfeiting measures, patient prescription compliance, reducing medication errors, reducing hospital errors, home health care monitoring. However, studies suggest that the following conditions need to apply: proper notice, appropriate consent, opt-out of technology, secure storage and transfer of data.

#### 3.4.2 Assessing concerns per application

As is illustrated by the examples above, many applications in RFID do not pose privacy risks. Therefore it is important to build privacy design in application-specific context. Generally when a link to a person is made, it starts to become a vulnerable technology. It is therefore suggested that for personal data tracking systems, a Privacy Threat Analysis (which is also done in Canada with positive experiences) should be performed. Such a PTA would provide an integrated list of threats and possible solutions to counter these threats, as most users of such systems are not aware of the privacy implications of the systems they deploy. The analysis would also assist in educating the public about the privacy impacts of specific applications. The PTA could be made legally mandatory, with actions taken based on PTA obligatory.

### 3.5 Summary of policy issues and options with regard to security, data protection & privacy, health and safety issues

There are privacy and security concerns with certain applications of RFIDs. It was clearly stated that in assessing those, we should guard against introducing general privacy debate in the RFID debate.

*1995/46 EC Directive* is applicable in most conceivable situations. However, the term “personal data” needs to be interpreted. For RFID the principles of purpose limitation, proportionality, data quality, and lawfulness, should also hold.

*2002/58 EC Directive's* article 9 addresses location data. RFID may reveal or be primarily used for the localisation of people. Still, the directive is not directly applicable: only where there is an additional feature of the terminal equipment, which provides value added service (VAS).

Should the regulatory framework be revisited? At least the EC's approach should focus on setting principles to ensure transparency and trust. Currently there are no legislative

measures in relation to RFID in Europe – the discussions during this workshop suggest that it is too early to move to regulation.

Table 3 and Table 4 below list the issues and policy options that were posed in the workshops. Again, this listing is merely a reflection of opinions of different discussants, and does not pretend to be consistent or comprehensive.

Table 3 – Policy issues related to ‘RFID security, data protection & privacy, health and safety’<sup>18</sup>

<b>Technical</b>
RFID can be spied upon at many places: Eavesdropping
There is concern that standards (legal, values) around the world are different
Password applications can be problematic, as users cannot cope with a large list of passwords for different applications and uses
The kill-commands can be misused to stop a tag from being traced
Tags can be read far beyond the distance for which they are designed
Deactivating or ‘killing’ a tag also denies consumers from RFID capabilities
<b>Education and Information</b>
Technology paternalism
Unauthorised readouts of tags
Retrieval of social networks
EPC Global standards provide little information about software how data is processed
<b>Legislative</b>
Administrative requirements to RFID users
Different codes of conduct (from different countries) may adversely affect the internal market and may hamper global trade
Strict legislation may hinder the developments of a technology that is still in its early stages of development
No mechanism of enforcement in place to make companies comply with code of conduct
Guidelines on consumer privacy and RFID established by a group of companies are not supported by all retail companies
<b>Data management</b>
Collecting data introduces risks as data can become accessible to unauthorised people (e.g. by breaking into databases)
Loss of accountability
Who controls information and who has access to it
When you are able to link a RFID number to a person, it becomes personal data
Who is liable if tag information gets out in the open or gets misused
There is no trust model for handling the data in the databases
Consent for two separate applications does not mean that combined application is agreed upon (linking of systems)
<b>Other</b>
Tracking employees poses privacy concerns
Lack of design considerations may introduce privacy concerns
An “Always on” Internet does not comply with the privacy principles set out by the OECD in 1981
Lack of specificity (a system should be specifically designed to gather a limited set of data)
No limitations on data collection (a system should be bounded spatially or temporally in the extent to which data can be collected and stored)
RFID should be non-discriminatory and respect individual identity
Globalisation is deemed unavoidable and thus is standardisation
Implantation of RFID chips
Priority is given to objects
Prevent economic and personal harm
There is a conflict between the consumer’s interest and business interest
Privacy is a concern for item level tagged products
Illegal competition issues

<sup>18</sup> During the workshop on ‘Security, data protection & privacy, health and safety’ several issues were mentioned that are related to issues discussed in other chapters (applications, interoperability, standards, and, spectrum). These issues are included in these respective chapters.

Table 4 – Policy options related to ‘RFID security, data protection & privacy, health and safety’<sup>18</sup>

<b>Technical</b>
Encryption
Aluminium foil (Faraday cage)
RFID sensor detection
Active jamming
RFID zappers (destroying the tag)
Tag deactivation
Hash lock
Re-encryption of tag
Clipping RFID tags (not hinder later use by completely breaking the tag)
Tags should incorporate functionalities to safeguard privacy (even if this functionality is costly)
PET (e.g. encryption) mandatory
<b>Information</b>
Indicating the presence of RFID tags on products (uniform clearly approved label indicating RFID presence)
Add the option of consumer choice (opt-in strategy rather than opt-out)
Introduce informed consent (e.g. explicit approval of bearer of tag)
Provide confirmation that tags have been deactivated
Consumers should have access to data gathered and have control of the data that are gathered about them
Transparent use of data gathered through RFID applications
Discussion on values to underpin how we feel about the benefits from RFID versus the concerns it raises
Consumer / public education (information concerning RFID should be clear, conspicuous and accurate)
<b>Legislative</b>
Strong legal approach
Implement a code of conduct
Develop a strategy for RFID privacy
Make privacy threat analysis (PTA) legally mandatory, with actions taken based on PTA obligatory
High fines when legislation is breached
Monitor RFID usage and deployment
<b>Data management</b>
Organisations that collect data should be held responsible for safeguarding the data instead of the general public
Secure storage and transfer of data
Minimise information on RFID tags
Keep separate databases to minimise damage / loss in case data is accessed in an unauthorised way
<b>Other</b>
Enhance privacy through changes in organisation
Privacy by design (technological, organisational)
Distinguish between applications (e.g. open (networked) and closed systems)
Review EC Directives and clarify the actual scope
Interpret the term “Personal Data”



## CHAPTER 4 RFID interoperability, standardisation, governance and intellectual property right issues

This chapter reflects the outcomes of the workshop on RFID interoperability, standardisation, governance and intellectual property right issues, which was held on June 1 in Brussels. This workshop discussed the relevance of standards and interoperability in deploying RFID, and the roles governance and intellectual property rights play in this arena.

The workshop on RFID applications illustrated that interoperability and standardisation are closely related issues that can pose important barriers towards a wider deployment of RFID. Many applications using RFID technology require multiple users to be able to read the same tags. In order to enable companies and organisations to work together, technologies need to be aligned through standards. This does not only enable cooperation, but also stimulates innovation and ensures competition can take place on a level playing field. Sometimes, these standards are proposed by industry itself and little outside intervention is required or asked for. However, competition issues with regard to standards may arise, particularly when standards are not set or decided upon transparently, or when standards become barriers for newcomers.

All of the opinions expressed, and evidence presented, in this summary are those coming from participants in the workshops and do not necessarily reflect the opinions of the authors or the Commission. This chapter follows the structure of the various workshop sessions. In the first part we address issues related to Standards in RFID. These are further explored in the following sections discussing standards in the context of different sectors; issues involved with the process of standard setting; the concept of 'Internet of Things' and other ways how RFID may be integrated with the network. In the second part we address the role and consequences of IPR, with more in depth discussions on EPC standards and open source software. Finally we summarise relevant policy issues.

### 4.1 What is RFID interoperability and standardisation?

Interoperability is concerned with having sufficient technological differences to prevent ambiguity between different data carrier technologies, so that if one data carrier technology was required, the others could be switched off automatically part-way through the recognition process, or switched off physically. On the other hand, if there is a need to support two different data carriers (for example EAN-13 and Code 128) then both data carriers are interoperable in the sense that each can separately be read

unambiguously, with the same reading equipment. In summary, interoperability is a characteristic that allows boundaries between technologies to exist where required and to be absorbed in an unambiguous manner where necessary.

To make this work in practice, we need to agree on how we communicate: i.e. we need to set standards.

It has been frequently stated that there are no global standards for RFID. This is not true as there are a lot of different application standards. Each application standard comprises of standards covering: the air interface, application protocol, and data content. The air interface standards (laid down in ISO 18000) describe frequency, modulation and bit encoding and optionally include an anti-collision protocol. The data protocol fills a gap in communications and addresses sector specific business issues. In addition, application guidelines covering labels and packaging, recycling, and interrogator implementation have been developed. Similar guidelines for education, privacy, security and safety are on the horizon.

## 4.2 RFID interoperability and standardisation in practice

Industries and governments are interested in automated systems that enable them to monitor the performance of their processes, in order to be better able to manage those. Without aiming to be comprehensive we consider several sectors of RFID application to identify current practice with regard to standardisation and interoperability. Then we scope out the issues that come into play in these sectors.

### 4.2.1 Automotive sector

In the automotive industry there are three regions (Europe, North America and Japan) each with its own standard setting body, which develop recommendations for communication and collaboration. The main automotive players operate on a global scale and in (global) joint ventures. Therefore, standardisation, interoperability, and thus the collaboration between these bodies are vital. Since 1985 barcodes and later 2D barcodes, were used as a vehicle to facilitate collaboration. Currently RFID is being looked into to take over from barcodes in pilot projects although its use is not yet proliferate. Although these pilots have revealed beneficial uses of RFID for the entire life cycle of car components<sup>19</sup>, they have not yet convinced the sector to widely adopt RFID. Key barriers include the complexity of technology and standards and the fact that automotive is a very low-margin cost-focused industry. These barriers may be mitigated if companies would be able to deploy proven, off the shelf technology and established data formats and content for RFID based on open standards.

Two important types of standards can be distinguished between: 1) airwave standards; and 2) data standards. Both standards categories include various ISO standards for all kinds of car parts. Currently the sector is developing common formats for data content and syntax for three subgroups: 1) returnable containers; 2) unique identification of components; and 3) vehicle identification. Data privacy and airwave standardisation are issues that still need to be addressed and in which the EC may play a role.

---

<sup>19</sup> Canvin, Odette International (2006), RFID and the Automotive Industry.

#### 4.2.2 Fast Moving Consumer Goods sector

In the fast moving consumer goods (FMCG) sector manufacturers need to collaborate globally with trading partners at high quality and at low cost. Typically these companies will operate many warehouses: both self operated and outsourced or shared. For these reasons standardisation and interoperability are key issues for the FMCG sector.

Retailers are pushing manufacturers to improve delivery flexibility. The transparency that can be facilitated through RFID can help manufacturers meet these demands. High-potential applications in the FMCG sector include:

- Store operations, such as inventory management and shelf-life control;
- Distribution operations: direct store delivery, track and trace of produce, and food safety;
- Promotional activities: checking compliance, consumer feedback;
- Shrink management: including decay, theft and administrative losses.

For most FMCG manufacturers RFID benefits are in the supply chain and not in item level tagging due to the low value of products and relatively high cost of tags.

Currently, economic and privacy barriers hamper RFID deployment. However, there may be a lot of benefits from RFID that are not perceived now but will play out in the future. Therefore standards will be challenged and thus should be flexible. If standards are established they must be industry driven and reflect current business requirements. An example of good practice in the development of global standards has been the development of the EAN barcode. The EPCglobal and ISO that have been established are complementary.

#### 4.2.3 Government

Standards affect the interoperability, technology development, adoption and maturation, and innovation of RFID. Interoperability issues are among the concerns of governments and other stakeholders. These can flow from:

- Differences in national/regional regulatory approaches;
- Existence of multiple standards setting organisations interested in addressing similar issues; and
- Early market presence, defacto standards.

From a government's perspective, a level playing field and open standards foster trade and competition, engender confidence for companies to invest in RFID systems, ensure interoperability between government and private systems, and may facilitate innovation.

The US government stimulates federal agencies to use voluntary, non-government standards to cut cost, in order to provide incentives to develop standards that meet national needs, and promote efficiency and economic competition. These standards will need to meet certain requirements including security and privacy considerations. In order to apply these standards agencies within governments would benefit from sharing information on RFID applications.

#### 4.2.4 Military

The military may apply RFID in the management of assets in support of troops, by enhancing logistics processes through product identification. In the US military two such types of RFID application are in use:

- Active 433 MHz tags for consolidated shipments (such as containers), which suppliers are rarely obligated to apply and which are not used commercially on a wide scale; and
- Passive Gen2 tags for shipments of boxes and warehouse pallets, which suppliers are contractually obligated to tag and which have wide scale commercial implementations.

The objective of applying shipments with tags when leaving the warehouse is to make inventory automatic instead of manual and improve logistics / sending process. The current level of tagging is not very costly. In future all items are likely to be tagged to facilitate automatic inventory management.

To reap the full benefits of the RFID deployment, it is important to get all suppliers and clients to use the tags. In addition, collaboration will need to be sought with partner nations, many of which have their own RFID systems in place, to exchange data picked up by their readers. For these systems to integrate, interoperability is important. Since many suppliers to DoD also supply private companies and use the EPC standard, DoD has also adopted EPCglobal standards for passive RFID putting Government and Commercial sectors on the same standard.

#### 4.2.5 Multinationals

Many companies do not require RFID systems to be interoperable since they deploy RFID in closed systems, or do not require the tags to be read by readers other than the ones originally intended for a specific application. For example tags compliant with IATA's baggage handling standard do not have to communicate and therefore be compliant with other aviation processes.

However, multinationals (or rather large companies) suffer from the increased complexity and cost if they deploy different non-compatible RFID systems. Similar interoperability or complexity issues are caused when these companies expand into new business sectors that use other RFID standards. For this reason these companies favour international cross-sector industry standards. Some large retailers and manufacturers even have a (global) RFID task force to internally coordinate RFID pilots and maintain intra company RFID standards. Currently within industry sectors individual standards (typically per application or type of application) are being developed, which is no significant problem, but may become one in the future due to interoperability problems.

### 4.3 Standards setting

In some sectors the existence of a variety of standard setting bodies is leading to fragmented standards and a lack of interoperability. Companies / standard setting bodies may introduce application specific standards whose use later on expands to include similar applications. Due to inkblot spread different standards may be developed for the same applications. To overcome these problems there is a need for an agreed basic architecture. The European Telecommunications Standardisation Institute (ETSI) focuses on technical standards: such as requirements, architecture and protocols, and develops test standards for RFID and tests these standards in practice (for instance

on trolleys). In order to achieve interoperability ETSI collaborates with other standard-setting bodies and forums.

EPCglobal is a standards setting organisation with a history in developing barcode standards that are used worldwide. Currently work is underway to do the same thing for RFID incorporating perceptions from different areas of RFID application, and regions (e.g. several European companies, Japan, US FDA, and IATA). EPCglobal's membership is growing strongest in North America, Asia and Europe indicating strong RFID awareness in these regions.

A new problem may be emerging as individual companies are starting to present solutions as quasi standards (e.g. in aviation) without consulting the body that is responsible for establishing standards. The EC may help prevent this by bringing major end user organisations together to participate in the process of establishing standards. For example, the CEN225 (barcode) was able to develop standards per application with all stakeholders, which could be a good practice example for RFID.

The EC should beware of restricting or over-regulating the setting of standards, but aim to promote flexibility and adaptability instead. Restrictive regulations may adversely affect development and take up of RFID and will hurt the competitive position of Europe vis-à-vis its competitors. Although the pace at which new standards can be introduced has increased, standard setting (for instance by ETSI) can still slow down RFID rollout since many end-users are reluctant to invest as long as the standard is under development. For example, the development of recent ETSI standards halted RFID developments and investments for 12 months until the standards were published.

To support the use of RFID over barcodes in the design of new logistics management systems, some of the main concerns with the application of RFID technology – such as privacy – need to be addressed. Due to the functional resemblance between barcodes and RFID, companies will be comparing their respective attributes when designing new logistic management systems as companies are unlikely to invest in two parallel infrastructures (both RFID and barcode systems).

In stimulating RFID standardisation, the Far-East (especially Korea and Japan) may function as a good role model, with governments investing to establish application standards. The EC could support the uptake of RFID by addressing the question of what the minimum standardisation requirements needed to ensure harmonised usage of RFID technology across Europe are, with minimised interoperability problems. In supporting RFID take-up special attention may be required to involve user groups such as SMEs.

#### 4.4 RFID Integration with the Network

Typically problems with logistic systems arise when the physical world and the information in these systems are no longer synchronised. Recent advances in miniaturisation have generated small, lightweight, cheap, mobile processors coupled with mobile communication capabilities, which help link (at low cost) real world objects to virtual counterparts. This trend in which objects become individuals is referred to as '*Integration with the network*' or the '*Internet of Things*'.

RFID networks are not the same thing as the Internet of Things. For instance, you cannot log into RFID tags. The databases that store RFID data typically are private networks with closed user groups. Vice versa, the components of the Internet of Things

do not necessarily have to include RFID, but may also include networks such as: NFC, GPS, GSM/GPRS/3G, Felica and Ipv6. However, although all these networks facilitate search and find capabilities (which may increase sales), trust (end consumers can check whether a product is real or fake; product information), and linking information to sites, currently RFID EPCglobal tags have strong support from industry and thus have an edge. Due to its potential RFID demand, the Internet of Things seems to be one of the prime (future) drivers for RFID deployment. However, the Internet of Things may not materialise fully or rapidly, since it is not embraced by everyone, as not all users want to put their data on the Internet.

The next generation of interfaces will use the Internet to retrieve information on tags. In the future the data will be stored on the tags to reduce dependence on remote databases. Information stored in these databases is secured via company firewalls etc. In addition, authentication protocols (SSL identification) determine identity, with which information is shared, manages access control, and facilitates data protection and federated identity. All these tools can be used to address privacy concerns.

Consumers want to have control and expect that they have the choice to opt-in instead of being left to the decision making of self-intelligent items. The software that processes the tags' information should contain the intelligence to ensure that only authorised readers can communicate with the tag. For this purpose three levels of information sharing can be distinguished: communicate solely with one reader (read 'myself'), with several authorised readers (named information providers), or with all readers (public).

The concept of the Internet of Things requires the 'things' to be defined. As these 'things' are mobile and change carriers it should be clear where and how information about them can be accessed. For this purpose each 'thing' is equipped with a Global Unique Product Identifier and indicates where and how to access product information. If products would not have a unique identifier, you would not be able to determine how many products you are reading.

For the purpose of accessing this data several protocols have been suggested all managing unique ID creation, including:

- Electronic Product Code (EPC) identifiers, Object Name Service (ONS) lookup mechanism (based on current Domain Name Service (DNS));
- ID@URI approach (DNS based), in which the ID can be EPC or any other suitable identifier;
- World Wide Article Information (WWAI) protocol (peer-to-peer based), which can use EPC or any other unique identifier.

Each of these look-up mechanisms has its specific pros and cons and no 'global winner' can be identified. Although EPC has strong support by standards bodies, the other systems show potential and therefore it is not realistic to expect that all standards become one. An advantage of these other protocols is that they can also be applied for technologies other than RFID extending the scope to identity integration in the network and are independent of technology, industry, hardware and IT infrastructure.

As such WWIA is an object-based network protocol, which generates a unique number and can be associated with any other code including EPC. The WWAI protocol is based on an open standard and a non-proprietary network, and has been tested in pilot

studies<sup>20</sup> in the pharmaceutical industry (counterfeit), FMCG, and logistics. In logistics, tracking and tracing enhances visibility, which helps organisations optimise their value chain with real-time business critical information delivery in global non-closed applications and enables collaborative supply chain management. These pilot studies illustrate that sharing information may increase a company's profitability<sup>20</sup>. However, standards cannot define the world and as industries are different and organisations are unique, we must limit standardisation efforts somewhere.

## 4.5 Intellectual Property Right Issues

For (a rapid) widespread adoption of the Internet of Things, its components need to be based on non-proprietary solutions and open standards.

### 4.5.1 EPC standards

EPCglobal is committed to drive towards royalty free standards, similar to GS1 with barcodes. However, this is a best effort and EPCglobal cannot guarantee that there will not be any royalties on EPC standards in the future. Today all necessary published standards are royalty free. Additional services and the implementation in applications may be subject to IPR. Essential claims will be sorted out by the marketplace.

The EPC standards are designed in cooperation with all EPCglobal members and ratified by the EPCglobal Board after which they may be submitted for ISO approval (as was done with the G2 standard). Since these standards, which define interfaces not implementations, are submitted to ISO, there is no either/or between ISO and EPC: it can be both. After introduction, standards are publicly available and open (e.g. anyone can see how standards work and several open source initiatives now build on EPC). For a standard to be successful, it has to be supported by its end-users. Therefore end-users, technology providers and application vendors are consulted in the process of establishing standards. Involving all these parties also brings balance to the discussion on IPR since this will typically be a matter in which end users and software vendors are on opposite sites. Currently discussions on the implementation of RFID standards are ongoing in several sectors.

In addition, non-profit organisations (such as the ANEC consumer organisation) and public policy bodies have been invited to contribute to establishing EPC standards, although they do not have a vote. Since in a European context standards are co-regulated there is a role for the Commission. Consumer participation is essential to cover topics such as privacy and safety. As standards do not adopt themselves, but require industry leaders to get behind and adopt them, the EC could also play a role in inviting these players to participate in these initiatives. Involving a large number of stakeholders would be beneficial, although too many stakeholders may cause the initiative to stagnate.

Royalty free standards have enabled getting the cost of tags down to 5 cent, which would have been unlikely to happen if royalties would have been in place. The further tag costs can be driven down, the more proliferate RFID is likely to become. Technology providers tend to impose royalty rights, but also want to build market. As it

---

<sup>20</sup> Benjamins, Stockway (2006), ID-Integration with the Network.

is not possible to have it both ways, companies currently increasingly choose to build their standard instead of issue high royalty rights.

For many companies the objective of implementing RFID is to transform their business processes and make these more transparent and efficient. This does not solely come about by replacing bar code by RFID. Companies typically prefer a single standard within their line of business even if they are active in different products or sectors. This can imply that a single standard is used across business sectors. The advantages of adopting a single standard may include:

- Improved customer availability;
- Patient safety;
- Demand driven supply chain;
- Reduced inventory;
- Reduced counterfeit;
- Improved ability to track and trace;
- Reduced shrinkage;
- Returnable assets; and
- Promoting competition between manufacturers.

Companies that are leading implementation will figure out which standards are working and which are not. The EC does not have to play a role in establishing or barring standards, as there are already too many organisations involved in standards setting. If additional standards are required, the market place will sort it out. The EC could assist industry (including SMEs) by scrutinising existing standards to assess whether they comply with European values and contain any hidden costs or submarine IPR.

The ultimate goal of the EPCglobal community is mass adoption of the standards, which can only be achieved through a royalty-free development process. For this reason use of EPCglobal standards is voluntary without constraining users to a single vendor. If users require applications that are covered by IPR, EPCglobal may adopt these solutions irrespective of the fact that royalty rights should be paid for that specific application. Although claims have been made, to date there has not been a finding that an IP declaration was based on a necessary claim to a specification. If it would happen, the end-user is liable for claims regarding IPR on applications, as EPCglobal applies “best efforts” and is not responsible to avoid IPR. Also in a royalty-free approach reasonable and non-discriminatory practices may apply.

#### 4.5.2 Open source software

Open Source Software (OSS) is an innovative and flexible way of licensing software or knowledge, which is available with its source code but does require special licenses to use, modify and redistribute it. Open source software is not necessarily free, since it can be subject to IPR, but is transparent. If contributing to OSS is voluntary, the development of OSS can stagnate if users do not pay for use and developers do not invest. To a certain extent however, OSS developers are willing to work for free due to indirect benefits, including: opportunities for complementing services, consulting services, hardware, other proprietary software, image, and strategic advantages such as undermining competitors.

The introduction of open standards fuelled the development of the Internet, which came to replace many private, proprietary networks (e.g. BITNET, Compuserve, ARPANET, and USENET). Opening the source code triggered adoption (due to affordability, availability and flexibility), standardisation (open code makes it easier to create or extend interfaces) and innovation (many minds and eyes involved, knowledge builds over knowledge, and end-user involvement with quick test and feedback). An OSS approach can prove very useful in cases with significant network externalities and innovation requirements: e.g. RFID. Market forces on their own are unlikely to trigger the “Internet of Things” as proliferation on this scale is affected by important market failures, including:

- Asymmetry of information (most stakeholders do not know much about RFID, and programs cannot be easily inspected or tested);
- High transaction costs (risky and disruptive investments);
- “Lock-in” typical of proprietary software products;
- Liable to submarine patents; and
- Multiple stakeholders and negative externalities.

The best remedy for paranoia is transparency. Opening the source code can show that RFID has no hidden agenda. In addition, the problem that not all supply chain partners can afford RFID systems can partly be overcome by introducing OSS, as this would make RFID cheaper and better available for these users. For these reasons some believe that standardisation should build on open source software. Over the past couple of years OSS, which depends on participation, has become more proliferate.

Standardisation bodies such as EPCglobal are essential, but standardisation alone is not enough: more openness is also required. Not all software needs to be open source. OSS is mostly ideal for the RFID core infrastructure, from which applications that build on open source systems can add value.

The number and size of companies that use open source in RFID systems so far is limited. Industries will need to find a structure to develop OSS for RFID otherwise OSS projects remain messy. Similarly, Wikipedia had to enforce rules to prevent incorrect information being put online. Everybody can contribute as long as it can be validated.

#### 4.6 Summary of policy issues and options with regard to RFID interoperability, standardisation, governance and intellectual property right issues

Although there is a clear appeal for standardisation, most discussants seem to agree that the role of government is merely to facilitate and stimulate the standardisation process, but restrain as much as possible for interfering. In the end, the market place will sort out standards that work, although government may stimulate and speed up this process by bringing together stakeholders and facilitate knowledge sharing.

Table 5 and Table 6 below list the issues and policy options that were posed in the workshops. Again, this listing is merely a reflection of opinions of different discussants, and does not pretend to be consistent or comprehensive.

Table 5 – Policy issues related to ‘RFID interoperability, standardisation, governance and intellectual property right issues’<sup>21</sup>

Many industries are very low-margin cost-focused and risk averse towards investing in RFID
Large companies suffer from the complexity and cost introduced if they deploy different non-compatible RFID systems
Privacy, security and interoperability concerns may complicate RFID systems and predispose companies to stick with barcode systems, as companies are unlikely to invest in two parallel infrastructures (RFID and barcode systems)
The existence of a variety of standard setting bodies is causing fragmentation in standards and lacking interoperability
There are concerns regarding RFID and data privacy
Individual companies are presenting solutions as quasi standards without consulting the body that is responsible for establishing standards
A lack of standards reduces competition between manufacturers
Proprietary software products may result in lock-in of consumer
Proprietary software products are liable to submarine patents
There are standardisation problems with the airwave protocol
Differences in national/regional regulatory approaches, existence of multiple standards setting organisations interested in addressing similar issues, and early market presence (defacto standards) may lead to interoperability issues
Stakeholders cannot easily inspect or test software used with RFID

<sup>21</sup> During the workshop on ‘RFID interoperability, standardisation, governance and intellectual property right issues’ several issues were mentioned that are related to issues discussed in other chapters (applications, privacy, security, and spectrum). These issues are included in these respective chapters.

Table 6 – Policy options related to ‘RFID interoperability, standardisation, governance and intellectual property right issues’<sup>21</sup>

Use the Far-East (especially Korea and Japan) as a role model in stimulating RFID standardisation (with governments investing to establish application standards)
Address the minimum standardisation requirements needed to ensure harmonised usage of RFID technology across Europe with minimised interoperability problems
Introduce an agreed basic architecture on airwave and data structure protocols
Facilitate deployment of proven, off the shelf technology and established data formats and content for RFID based on open standards
Stimulate government agencies to use voluntary, non-government standards to cut cost, provide incentives to develop standards that meet national needs, and promote efficiency and economic competition
Drive towards royalty free standards
Assist industry (including SMEs) by scrutinising existing standards to assess compliance with European values and contain any hidden costs or submarine IPR
Promote open source software applications by targeted services development
Beware to restrict or over-regulate, but promote flexibility and adaptability instead
Governments would benefit from sharing information on RFID applications
Bring together major end user organisations to participate in the process of establishing standards
Invite industry leaders to participate in developing, getting behind and adopting standards
Make standards open for everyone to see how they work
Promote open interfaces that allow citizens to see what data is gathered on them
Research and promote storing data on tags to reduce dependence on and risks with remote databases
Enforce databases containing privacy or security sensitive information to be secured via firewalls
Enforce authentication protocols (such as SSL identification) to determine identity, with whom information is shared, manage access control, and facilitates data protection and federated identity



RFID technology depends on the availability of spectrum in Europe and worldwide. This chapter reflects the outcomes of the workshop on RFID frequency spectrum, which was held on June 2 in Brussels and raised and discussed obstacles of technical, economic and political nature related to RFID and frequency spectrum. The workshop addressed both the short/medium term issues as well as long-term perspective of RFID and frequency spectrum. In the short term emphasis is put on the timely implementation of existing standards and spectrum regulations, especially in the UHF band. For the longer term, a sustainable implementation strategy for Europe should be defined, including an assessment of quantitative and qualitative spectrum needs.

All of the opinions expressed, and evidence presented, in this summary are those coming from participants in the workshops and do not necessarily reflect the opinions of the authors or the Commission.

### 5.1 What are the main policy issues related to RFID frequency spectrum?

RFID is a radio technology and as such requires the use of radio spectrum to operate. Generally, when discussing spectrum issues, focus tends to be on tags that make use of the UHF range, which designates a range (band) of electromagnetic waves whose frequency is between 300 MHz and 3.0 GHz. Waves whose frequency is above the UHF band fall into the microwave or higher bands, while lower frequency signals fall into the VHF or lower bands. UHF (together with VHF) is the most common frequency band for television. In addition, it is used mobile telephony, two-way radio communication and increasingly for digital services. Since RFID shares the UHF range with other applications, only a limited bandwidth within UHF is available for Short Range Devices (SRDs) and RFID: 865-868 MHz. Although there are RFID tags and applications that make use of other frequency bands (tags operating at other (higher) frequencies and battery-operated (active) tags), most spectrum issues seem to concentrate round the UHF range and many sectors and applications (e.g. in retail and supply chains) use UHF tags. Therefore this workshop also focuses on this range.

According to EN 302208 requirements, the designated SRD band ranges from 865-868 MHz. It should be pointed out that RFID is just one technology using the band. This 3 MHz bandwidth available for SRD is split into 15 sub channels of 200 kHz each. Only 2 MHz (10 sub channels) are allowed to operate at 2 Watts for a maximum of 4 seconds, the remaining 1 MHz has more power restriction, which makes it unsuitable

for many RFID applications. In addition, there is the requirement of Listen Before Talk (LBT), which makes the devices less efficient.

Although theoretically the technology is able to read multiple tags (up to 500 per second) at 3-4 metres distance, there are still many technical challenges that need to be tackled before RFID reaches maturity:

- Reading of unwanted tags, which slows down the reading process and increases the chance of inaccuracy;
- In a situation where many readers are present, interference can take place between the readers, as readers transmit at the same frequency. This may also occur when readers operating under regulatory geographical exemptions (e.g. for military use) interfere with common regulated applications. However, since military uses are commonly not close to city centres, these types of exemptions do not pose serious interference problems.
- Operating portal devices is difficult: the interrogator can be anywhere and pointing in any (i.e. often the wrong) direction reducing reading performance;
- Reading performance will need to be improved: although the accuracy can reach 98.5% when scanning 50 items simultaneously, this performance does not meet current high-volume good tracking requirements;
- Tags typically need to be positioned towards the reader to achieve high reading performance;
- There are a limited number of sub channels (10) that can be used and channel availability cannot be guaranteed.

The example was given of dedicated channels in dense reader mode (DRM); here the readers transmit in channels 4, 7, 10, 13; adjacent readers (e.g. in dock doors) would only use two channels, so that adjacent systems can use the others (4+10 & 7+13). It was said that currently 2 MHz is adequate bandwidth, but LBT stops rollout, and if channels 4,7,10, and 13 can be used for RFID, the others could be used by other SRDs. However, in the discussion it was made clear that LBT is an intended element of the recommendation, and that other SRDs would need to use the mentioned channels as well.

Many of the issues with RFID spectrum arise in the field of retail and supply chain operations. As these areas are considered key for the further deployment of RFID, the following section will discuss specific problems and solutions relating to frequency spectrum for these applications areas.

## 5.2 What problems do users face in implementing RFID?

In spite of the restrictions mentioned in the previous section, large European retailers are moving ahead to implement RFID under current legislation. They do point out that developments in North America are moving faster because of a more lenient regulatory regime. One of the main problems in frequency spectrum discussions is that decision-making is slow. Currently only 14 of 25 countries of the European Union have adapted their frequency plan to accommodate the UHF bands as specified in the European Telecommunications Standards Institute (ETSI) published European Standard EN 302 208 (of September 2004) and the European Conference of Postal and Telecommunications Administrations (CEPT) update to ERC Recommendations 70-03

on SRDs (in October 2004). Although France, Spain and Italy are expected to adapt their national frequency plans in the near future, the European Commission may want to speed up adoption by regulatory means. Furthermore, long-term spectrum requirements could also become a concern that would require action by the EC.

For large retail organisations such as Tesco and Metro, RFID provides many opportunities, including reducing costs and avoiding waste. Tesco has identified more than 40 opportunities for applying RFID. Also Metro is keen to deploy RFID to improve internal business processes to be able to remain competitive. In the retail sector tagging takes place on re-usable assets, pallets, cases and finally at item level (small pilots have been carried out). However, RFID tagging involves large investments: complex solutions are required to get things to work, hardware and tags are very expensive, and implementation cost is astronomical. As uncertainty about the legislation could negate these sizeable investments, it would be advisable to create clarity about the expected direction of RFID related policy development and the limitations this might pose on RFID use.

Although tag prices have dropped, the 5-cent tag price can only be reached with volumes of 100s of millions of tags. While users have been sensitive to these price drops, they also need a tag that works even if that means it is more expensive.

Currently, the deployment of RFID is still hampered by technology immaturity: standards were not developed with use cases in mind, and are not harmonised across the EU, also the bandwidth limits the number of tags that can be read. Tesco has only been involved in the development of RFID for 4 years. In their opinion a lack of experience and exaggerated marketing can easily lead to disappointment.

Another issue large retail organisations run into in applying RFID throughout their supply chains is that many standards are developed for a specific sector. As large retailers interact with a multitude of sectors (e.g. different types of consumer goods) they need to integrate and be knowledgeable about all these different systems, which adds to the complexity and cost. Therefore standardisation across sectors with broadly applicable RFID for different stores would be welcomed.

According to Metro, retail deployment of RFID depends on spectrum availability. The ETSI standard is welcomed, but should be taken up by all Member States. Given the available channels, only a small number of readers can be operated in the same space. Interference is a large problem and therefore research and development for dense reader mode (DRM) is needed. The development of synchronisable readers is a precondition for further deployment of RFID and large-scale efficiency gains.

Tesco's view is that the USA is ahead because of Wal-Mart's market power, the different regulatory environment, more spectrum availability and lenient FCC requirements. If Europe wants to progress, compliance should be simple, standards should not stifle development, and further research should be funded. Metro suggests that more (dedicated) spectrum is needed and that RFID should be seen as a key radio service.

In spite of its perceived shortcomings, the existing European legislative basis is considered to be quite reasonable. The EU has the required skills base and resources to keep a leading position on RFID.

### 5.3 What are the technological and policy options related to RFID frequency spectrum?

The limitations mentioned before impede fast proliferation in the retail sector, which requires dense reader deployment reading simultaneously in confined spaces. There are some technological solutions to these problems, such as:

- Use of narrow beam antennas and electro-magnetic absorbing material (although the absorbing material is expensive);
- Use of two interrogators at the same portal with different frequencies;
- Use of tags that respond at higher data rates;
- Increase the power level for 13.54MHz;
- Implement (several) RFID channels without LBT requirements;
- Decrease duty cycle restrictions; and
- Implement different spectrum parameters for high and low duty readers.

Furthermore, investment in readers and reader technology would also benefit reader performance. Readers should be directional and aware of their location. Another solution to the LBT requirement would be synchronisation: to treat a system of readers as a single reader, to synchronise the channel at which signals are transmitted. This requires communication between readers.

The examples given indicate that technical solutions to existing problems can be developed, given the limitations of the spectrum available. However, it would require additional research. Currently a significant amount of funding seems to be spent on product development for specific European regulations, while global harmonisation would be preferable. If spectrum requirements were harmonised, the cost of development would drop and the time to deployment would be enhanced. However, in the short to medium term Europe will have to live with the current restrictions.

For future foreseen developments to take place more spectrum would be needed at UHF frequencies within an acceptable tuning range. Ideally, this should be dedicated spectrum with no or minimum mitigation techniques and channels of 200 kHz. Given the current situation, this would require a 10-15 year channel plan. Several speakers voiced a need for a careful study into the market requirements for frequency use. This does not mean that in the meantime RFID development will not take place: technology vendors will make RFID work, but it will not happen quickly.

RFID should be seen in the context of all wireless communication technologies that range from Bluetooth, ZigBee, UWB, and NFC to RFID. RFID technology will not be used alone, but with other technologies at the same time. Other (RFID) technologies are still being researched and should be considered viable alternatives. The optimal deployment of specific RFID tags depends, once again, on the application. Therefore, broad research and development activities are called for. Focusing on RFID alone would be limiting the view of all options available.

Unlicensed spectrum may be another option to allow for a broad development of technologies. There are many interesting applications that have not been introduced to the market place, such as finding your books, inventory assessment at home etc. These applications are expected to flourish only in an environment where experimenting is as unrestricted as possible. Therefore, spectrum reform would need to free up more

spectrum for unlicensed uses, to clear up spectrum restrictions. In the choice between licensed versus unlicensed spectrum, the EU should be aware that this choice not only impacts government's role, but also favours involved companies based on size and type of company.

Different applications require different functionalities leading to different spectrum requirements. Spectrum parameters are closely linked to RFID performance: frequency, power level, bandwidth, duty cycle limitations, listen before talk, and parallel channels all influence the usability of the technology. As certain frequencies are more suitable for specific applications than others, there may be ways to optimise band usage for example by identifying whether we use UHF for things we could be doing in other (e.g. HF) bands. There will be compatibility issues, but broadening RFID's scope beyond UHF should be possible and allow for more efficient use of spectrum available.

A tag's reading range is another performance issue. Currently, improvements in antenna design are underway to increase antenna performance. This would mean that tags could be read from a larger distance, which would have privacy implications. Mitigative measures include kill options on tags (when a customer leaves a store), developing a Faraday cage (e.g. a jacket of aluminium foil), blocker tags, and smart tags with encryption. If possible, the tag should contain as little data as possible; intelligence and storage should be moved to the reader and the underlying databases. Since interconnection is the most expensive part of a network and storage has increasingly become cheaper, there is a trend to put processing as close to the data as possible. Processing data is increasingly going to the edges of the network and thus away from central processing as where privacy concerns regarding from RFID would arise.

#### 5.4 The regulatory and standardisation challenges ahead

At present, standardisation efforts in the EU are already taking place in a number of organisations. ETSI, for example, sets standards but does not impose regulations. The European Commission can incorporate ETSI standards into its legislation and make them mandatory for all European countries to comply with. ETSI tests RFID solutions, which includes interoperability and conformance tests.

Historically, national administrations are responsible for allocating spectrum. CEPT is the coordinating body for national administrations. However, it should be realised that spectrum regulation is a moving target; legislation is always behind on practice. The increasing pace of change requires improvements in the spectrum management system in order to increase flexibility and transparency to make optimal use of this scarce resource. The European Commission, mandating the strategy for SRDs to CEPT, seems to favour permissive conditions for RFID, but needs to anticipate future demand for spectrum. According to CEPT regulation on RFID should be minimal and the principle of neutrality should be pursued for applications and technologies.

The use of 40+ GHz spectrum could be further explored, but additional spectrum should only be made available if the need can clearly be proved. In the end the market place, and not the regulators, will decide which applications and technologies will succeed. The absence of a market-based approach reduces incentive for effective use of spectrum.

With spectrum being in great demand, particularly at UHF, there is a need to take decisions on a more informed basis. SRDs should not be considered in isolation from

other radio services. There needs to be greater transparency in the decision making process, which includes the use of Impact Assessments to ensure that the whole picture is taken into account. Impact Assessments do not need to prolong the decision-making process – they can be carried out in parallel with other assessments.

In future, a greater emphasis on the use of existing SRD spectrum for new SRD applications is expected as well as increasing use of Impact Analysis to determine the best use of spectrum. Technical and application neutrality will lessen the need for decision making in the future.

When looking at spectrum from a broad economic perspective, we see that spectrum is property, and that it has public goods characteristics, the scarcity of which may be an artefact of wrong allocation. A lot of discussion focused on reaching consensus on the use of spectrum bands. However, if consensus is achieved at the wrong level (for instance national), innovation (legal, social, technical, etc.) is choked off on a higher level (European, global). If regulation is unified, then useful innovation may not take place.

Government intervention in spectrum allocation may affect efficiency and equity of allocation. Decisions that we take now influence the developments of the technology (and behaviour of companies) later on. The good may be the enemy of the best: this means that we may better wait with implementing something that is possible now to reap even better implementation benefits later on. Radical changes in the way spectrum is allocated are unlikely, especially not in the short term.

## 5.5 Research on EMF and RFID reading ranges

Until 20 years ago the question about the effects of electro-magnetic frequencies (EMF) and their impacts on health was not asked. Nowadays, we know that EMF can have effects on humans but the risk to health of people is largely ignored. It is not clear exactly which effects occur during the use of RFID, as research in this field is sparse. Based on the current rules of the Radio and Telecommunications Terminal Equipment Directive (R&TTE), radio equipment that complies with the Directive is allowed. Although deployed telecommunication equipment complies with the Directive, there is increasing discussion whether these guidelines are correct and protection is sufficient.

The claim that RFID frequencies have a non-ionising character and thus are not harmful is doubted<sup>22</sup>. Non-ionising radiation will not destroy DNA directly<sup>22</sup>, but may release free radicals that may harm DNA. The only way to ascertain whether this is true is to perform tests that measure damage to cells and DNA, and are performed in a blind way (the researchers do not know beforehand which specimen is irradiated) to ensure objectivity. Research on the effects of GSM did not find effects on hearing, genotoxic effects, or disruptions to the nervous system. However, researchers contend that, in general, there is too little research into EMF and no into RFID effects on health to draw any conclusions. Although currently the balance tends to tip towards no health risks associated with EMF exposure (related to radio masts that operate within the guidelines), it has to be taken into account that research on health effects takes place in a research setting, which is different from real-life settings. In addition, there are many examples of cases in which research only later proved that there had been a danger (e.g. in the cases of smoking, X-ray, asbestos, etc.). Conclusive research should at least include reproducible tests that show a relationship between exposure and effect.

Recent research<sup>22</sup> suggests that EMF exposure's negative effects seem more dependent on duration of exposure than on its frequency. As an RFID reader has approximately the same power as a GSM device, it is expected to result in similar effects.

Another field of research is into the effects of the use of RFID in hospital environments. One of the basic problems in this type of research is having engineers talk to medical staff and seeing the world from different points of view. The Massachusetts Institute of Technology is studying the effects of RFID-tagged blood bags on the quality of blood. However, research is still at the beginning of development. The same issue arises about the impact of RFID on pharmaceuticals.

## 5.6 Summary of policy issues and options with regard to RFID frequency spectrum

As RFID becomes more pervasive, large end-users such as Metro and Tesco seek to implement RFID technology, but are discouraged by regulatory and technical constraints and suggest urgent action. Although these two major users are not the only users of RFID and these signals must be seen in perspective, the concern raised should be taken seriously. Nevertheless, the technical constraints appear resolvable: for the moment 2 MHz in the UHF band seems adequate. Technology vendors will make it work, but it will not happen quickly unless additional activities are undertaken in the regulatory field. At current, there seems to be a disconnect between the commercial world and the regulatory world. Users urge regulators to act faster to be able to reap the benefits of the technology.

Currently, RFID deployment is still in its infancy. Although it is tempting to quickly respond to the community's needs in term of frequency availability, it would be better to make a balanced review of needs, costs and benefits through the existing mechanisms and management structures. The pressure on spectrum regulators is exemplified by the imminent switchover of analogue to digital television; freeing up spectrum on which many interest parties already put their claim. The positions across Europe in allocating this spectrum will differ as not all frequencies are harmonised, and this spectrum is unlikely to be available before 2012. Also, lessons may be learned from earlier activities of spectrum reallocation, such as GSM, and solutions may be sought in extending into the higher frequency ranges.

The fragmented spectrum legacy in Europe is a fact that cannot easily be changed. Spectrum regulation is both a key enabling and inhibiting factor. In the short term, radical changes to reallocate spectrum are not feasible. As all SRDs are dependent on the UHF band, it is difficult to allocate dedicated bandwidth to a single application, such as RFID. Therefore, a broader view balancing technical efficiency, allocational efficiency, and incentives to further research is needed. Since in future more applications may be deployed that require dedicated spectrum with minimal limitations, there is a need for a long-term plan as a basis for a system reference document, a spectrum plan that is valid for the next 10-15 years. Developing such a plan requires studies into the coexistence of SRD and RFID in common bands. These studies may show that some spectrum would need to be cleared to make additional spectrum resources available.

---

<sup>22</sup> Adlkofer, Verum Foundation (2006), Lessons from the REFLEX study on biological effects of radiofrequency electromagnetic fields

The study required would be an Integrated Assessment weighing different market requirements in the future and determining frequency opportunities. Given that there are differentiated needs arising from various RFID applications (such as the amount of spectrum, spectrum parameters, and global interoperability), would a dedicated RFID spectrum really be required? Answering this question could lead to a roadmap of spectrum availability, which provides priorities and milestones. Only on the basis of such a study can a trade-off between sophistication and “easy” spectrum usage conditions be made.

Table 7 and Table 8 below list the issues and policy options that were posed in the workshops. Again, this listing is merely a reflection of opinions of different discussants, and does not pretend to be consistent or comprehensive.

Table 7 – Policy issues related to ‘RFID frequency spectrum’<sup>23</sup>

<b>Technical</b>
Listen Before Talk requirement makes devices less efficient
Small bandwidths and power restrictions hinder implementation
Reading of unwanted tags slows down the reading process and increases the chance of inaccuracy
In dense reader environments interference is a problem
Portal devices are unreliable as they can be anywhere and point in any direction
Reading performance will need to be improved (current accuracy levels are unsatisfactory for high-volume good tracking)
There is a limited number of sub channels that can be used and channel availability cannot be guaranteed
RFID tagging involves large investments (complex solutions, cost of hardware, tags and implementation are high)
RFID deployment is hampered by technology immaturity: standards were not made with use cases in mind, limited bandwidth, and standards are not harmonised across the EU
RFID technology will not be used alone, but with other technologies (such as Bluetooth, ZigBee, UWB, and NFC) at the same time
There is insufficient information on the coexistence of SRD and RFID in common bands
<b>Legislative</b>
Decision-making is slow (especially from an entrepreneur’s perspective)
RFID developments in North America are moving faster because of a lenient regulatory regime
Legislation on the spectrum management system is behind on practice jeopardising flexibility and transparency to make optimal use of this scarce resource
<b>Information and education</b>
Lack of experience and exaggerated marketing can lead to disappointment
<b>Other</b>
Stakeholders need to agree on using single standard or multiple standards (e.g. for different stores)
The health effects of EMF from use of RFID are not clear
There is no long-range plan as a basis for a system reference document, a spectrum plan that is valid for the next 10-15 years

<sup>23</sup> During the workshop on ‘RFID frequency spectrum’ several issues were mentioned that are related to issues discussed in other chapters (applications, privacy, security, interoperability, and standards). These issues are included in these respective chapters.

Table 8 – Policy options related to 'RFID application domains and emerging trends'<sup>23</sup>

<b>Technical</b>
Research and promote use of tags that respond at higher data rates, operating at other (higher) frequencies and battery-operated (active) tags
Research and promote use of narrow beam antennas
Research and promote use of electro-magnetic absorbing material
Research and promote use of two interrogators at the same portal with different frequencies
Research and promote reader synchronisation to tackle LBT (treating a system of readers as a single reader to synchronise the channel at which signals are transmitted)
Technological solutions require additional research
Reform spectrum to free up more spectrum for unlicensed uses clearing up spectrum restrictions
Research dense reader mode (DRM) options
Implement RFID channels without LBT requirements
<b>Legislative</b>
Speed up adoption by regulatory means
Harmonise spectrum requirements to lower cost of development and enhance time to deployment
<b>Information</b>
Create clarity about the direction and limitations of RFID use to avoid uncertainty about legislation
Explore future uses of spectrum
<b>Other</b>
Research and perform reproducible test showing relationship between EMF exposure of RFID use and health effects
Make a balanced review of RFID needs, costs and benefits

## Disclaimer

---

This report is part of a European-wide public consultation process regarding an RFID policy for Europe and presents the proceedings of a series of consultation workshops. As this document contains the proceedings of the workshops, the views expressed in the document are those of the presenters and discussants, and are not necessarily shared by the Commission's or the researchers. This report does not claim to present a comprehensive overview of all issues and options related to RFID, but merely provides a reflection of opinions of different discussants. As these opinions may be contradictory, the report does not reach consensus on all points. For more detailed backgrounds on RFID and the issues discussed during the workshops, we refer to the Policy framework papers, which are available at the website<sup>24</sup>.

---

<sup>24</sup> <http://www.rfidconsultation.eu/>