RFID: New "Killer Application" in the ICT World, New Big Brother, or Both?

EGMONT PAPER 30

RFID: NEW "KILLER APPLICATION" IN THE ICT WORLD, NEW BIG BROTHER, OR BOTH?

FRANKLIN DEHOUSSE
TANIA ZGAJEWSKI

Royal Institute
for International Relations

June 2009

ACADEMIA PRESS

The Egmont Papers are published by Academia Press for Egmont – The Royal Institute for International Relations. Founded in 1947 by eminent Belgian political leaders, Egmont is an independent think-tank based in Brussels. Its interdisciplinary research is conducted in a spirit of total academic freedom. A platform of quality information, a forum for debate and analysis, a melting pot of ideas in the field of international politics, Egmont's ambition – through its publications, seminars and recommendations – is to make a useful contribution to the decision-making process.

* * *

President: Viscount Etienne DAVIGNON
Director-General: Raf VAN HELLEMONT
Series Editor: Prof. Dr. Sven BISCOP

* * *

Egmont - The Royal Institute for International Relations

Address Naamsestraat / Rue de Namur 69, 1000 Brussels, Belgium
Phone 00-32-(0)2.223.41.14
Fax 00-32-(0)2.223.41.16
E-mail info@egmontinstitute.be
Website: www.egmontinstitute.be

Eekhout 2
9000 Gent
Tel. 09/233 80 88 Fax 09/233 14 09
Info@academiapress.be www.academiapress.be

J. Story-Scientia NV Wetenschappelijke Boekhandel
Sint-Kwintensberg 87
B-9000 Gent
Tel. 09/225 57 57 Fax 09/233 14 09
Info@story.be www.story.be

All authors write in a personal capacity.

Lay-out: proxess.be

ISBN 978 90 382 1480 1
D/2009/4804/122
U 1305
NUR1 754

Table of Contents

Introduction

RFID ("Radio-Frequency Identification") is a new telecommunications service that has received a lot of attention in the last years, due to its growing use[1]. Though it is based on a rather old technology (the Radar), a progressive rise in quality and decrease in price seem to have opened a lot of new opportunities. It has been estimated that this market could reach the world value of 30 billion euro in 2015. In 2007, its value was already estimated at 5 billion dollars. Worldwide sales of RFID tags reached approximately 2.16 billion in 2008, a substantial increase from the year before. In 2015, some estimate that 400 billion could be sold. According to the European Commission, in 2007, tags sold were used in smart cards and payment key fobs (36%), smart tickets/bank notes/secure documents (14%), cases or crates of consumer retail goods (13%), retail apparel (5%), animals (5%), and books (4%).

Much hype has surrounded RFID during the last years. One describes ill patients who would be automatically treated in the hospitals or at home through body sensors, immigrants who could be tracked anytime anywhere on the map, refrigerators which would select outdated food or compose propositions of menus according to their content, prisoners under permanent radio control through chips borne or injected under their skin, cars which will pay fees and find their way in the traffic alone, food whose origin will be permanently controllable. Sometimes, however, the deployment of RFID has not brought the anticipated benefits. It has also brought protests in some parts of the public.

The rise of RFID systems provokes a lot of interrogations. They encompass among others health protection, privacy, standards' compatibility, and the development of a new Internet system. RFID thus leads to a broader reflection about the Internet of the future. Furthermore, RFID appears at the vanguard of a much broader and deeper change of the Internet, though not fully clear until now, which is described as "the Internet of things" (IoT). In such a context, many colliding interests must be taken into consideration. In 2006, the European Commission thus launched a consultation process on this topic, which produced various reactions. In 2007, it presented a communication[2].

1. See S. AHSON and M. ILYAS, RFID Handbook: Applications, Technology, Security, and Privacy, CRC Press, 2008.
2. COM (2007) 96.

The present report aims at describing the main stakes of this technology in Europe[3]. It will describe the nature of RFID (§ 1), the numerous new uses of the technology (§ 2), the main problems it generates (§ 3) and the present regulatory framework in the European Union applying to RFID (§ 4).

Franklin DEHOUSSE
Tania ZGAJEWSKI[4]

3. For more detailed analysis, one must consult very interesting reports financed by the European Commission: M. VAN LIESHOUT et alii, *RFID Technologies: Emerging Issues, Challenges and Policy Options*, 2007 and the five CE RFID reports. http://ftp.jrc.es/EURdoc/eur22770en.pdf. http://www.rfid-in-action.eu/public/results. (accessed May 7, 2009).

4. F. Dehousse is Professor at the University of Liège and Judge at the Court of first instance of the European Communities. Tania Zgajewski is EU Monitoring Advisor at ELIA S.A. and was previously Senior Researcher at the University of Liège. This comment is a personal one and does not represent the opinion of the institutions or company to which they belong.

1. What is RFID?

1.1. Definition

The acronym "RFID" stands for "Radio-Frequency Identification" (in French "identification par radio fréquence (IRF)"). This technology, thanks to radio waves, allows without physical or visual contact to identify everything (objects or animals or persons) in order to track, trace and locate it anywhere. Basically, RFID is a system based on chips that communicate through radiofrequencies.

This technology is not new and is partly linked to the development of radar. 0riginally, it was used for military purposes. It allowed during the Second World War to distinguish friendly ships and planes from enemy ships and planes. This system was called "Identify friend or foe (IFF)". RFID technology continues to be deployed for military purposes (for instance nuclear material logistics). At the commercial level, RFID was initially developed to replace the bar code. Since the 1970s, the applications have become numerous. However, despite its already long history, the RFID technology still remains in its formative years.

The topic is complex for different reasons. Firstly, the terminology remains often highly imprecise. The name in itself is already misleading. In fact, RFID systems do not provide only identification but also other services through radio frequency. From another perspective, some systems identified as RFID are not always based on radiofrequency communication, but they can also use electromagnetic induction, which is the production of voltage across a conductor situated in a changing magnetic field or a conductor moving through a stationary magnetic field.[5]. RFID is also sometimes confused with NFC (Near Field Communication). NFC is a short-range wireless connectivity technology standard designed for simple communications between electronic devices. NFC communication is enabled by bringing two NFC compatible devices within a few centimeters of one another[6].

5. Such imprecision also haunts the question of standards. For example, "systems based on ISO 14443 standards are often not called RFID systems by experts but "contactless integrated circuit cards", which is the ISO standard's terminology. However, what everybody calls today an "RFID passport" is based on ISO 14443" OECD, *OECD policy guidance on radio frequency identification*, 2008, note 11. http://www.oecd.org/dataoecd/19/42/40892347.pdf (accessed March 30, 2009).

6. Applications of NFC technology include contactless transactions such as payment and transit ticketing, simple and fast data transfers including calendar synchronization or electronic business cards and access to online digital content. The main NFC application until now remains mobile payments. Near Field Communication is based on inductive-coupling, where loosely coupled inductive circuits share power and data over a distance of a few centimetres. NFC devices share the basic technology with proximity (13.56MHz) RFID tags and contactless smartcards, but have also specific features.

RFID has thus vague boundaries and many facets. It is a part of different types of data carrier and identification techniques, generally attributed to automatic identification and data capture (AIDC). Other techniques can provide important and complementary roles to RFID and are highly relevant in interfacing with the physical world and people-oriented services. Finally, a RFID system may present many characteristics, and also many different levels of complexity, going from the very simple identification portal, to a complete industrial production system, managing the call of inputs, the delivery of outputs, and the correction of occasional mistakes.

1.2. Functioning

A RFID system is composed of three elements: (a) one or several RFID tags (also called "transponders" or "RFID labels"), (b) one or several RFID readers (also referred to as "interrogators") and (c) a computer system (hardware and software).

1.2.1. RFID Tags

A RFID tag consists of a microchip (which can be reduced to the size of a point and whose memory stores data) and of an antenna (which is printed, etched or stamped on a substrate). The tag can be stuck on, printed on or incorporated into a product, an animal or a person, providing a unique identifier for each. In 2006, the size of existing tags was about 10 cm x 4 cm for 900 MHz operation, and 6 cm x 1 cm for 2,45 GHz operation. It was reported that Hitachi had an embedded microchip for a RFID that is 0,15 mm square and 7,5 lm thick[7]. In 2009, the testing phase of some 2-millimeter (0.1-inch) passive RFID chips was announced[8].

One must distinguish passive and active RFID tags.

a) passive RFID tags

A passive RFID tag has not its own internal power source. It does not contain a battery. The power is only supplied by the RFID reader. When radio waves from

7. CEC, From the RFID to the Internet of things – Pervasive networked systems, 2006, p. 10.
8. Economically, it seems generally wise not to go too far and to keep most intelligence out of the tag. Putting more information on it increases the risks of theft or counterfeiting. It is also more costly to put more information on mobile tags, and thus can reduce mass use. Until now, business models have also been easier to make with reusable tags, which reduce capital expenditures.

the RFID reader are encountered by a passive RFID tag, the antenna within the RFID tag forms a magnetic field (which decays very rapidly over distance). The RFID tag draws power from this magnetic field for long enough to emit a signal and transmit stored information back to the reader. Consequently, the passive RFID tag has not the possibility to initiate a communication with the reader. It can only emits signals when queried by a RFID reader.

The two major advantages of a passive RFID tag are that it has a long lifetime and that it is much less expensive to manufacture (in US currency, currently priced in the 10-cent to 50-cent range for large quantities). The four major disadvantages of a passive RFID tag are the following. Firstly, the information contained in a passive RFID tag can generally be read but not modified. This means that a new passive RFID tag must be purchased in case the information contained in a passive RFID tag must be changed. Secondly, the passive RFID tag can only be read at very short distances (a few feet at most) since it must stay in close proximity to the RFID reader. Thirdly, the passive RFID tag has a limited data storage capacity. Fourthly, it is not possible to include sensors to measure and record parameters such as temperature, humidity, pressure, etc.. These four major disadvantages greatly limit the device for certain applications.

b) active RFID tags

By comparison, the active RFID tag has its own internal power source. It is equipped with a battery which provides power to emit a signal and transmit directly stored information to a reader. Consequently, the active RFID tag has the possibility to initiate communications with a reader but also with other RFID tags. The major advantages of an active RFID tag are the following. The information it contains can be read and modified (useful for updating data). It can also be read at longer distances (one hundred feet or more) and has a greater data storage capacity. It can integrate sensors to measure and record parameters such as temperature, humidity, pressure, etc. These advantages allow more functionalities.

The three major disadvantages of an active RFID tag are the following. It has a shorter lifetime, has a larger size because of the presence of a battery and is more expensive to manufacture (in US currency, currently priced in the $10 to $100 range). This said, with time progressively, the lifetime of active RFID tags is increasing. The size and the cost of manufacturing of active RFID tags are also with time reducing because of (a) the integration of new generations of electronic components stemming from the world of mobile telephony (GSM/GPRS) or from the world of wireless networks (WIFI, Blue tooth ...), (b) new technologies for batteries offering more autonomy and weight gains.

c) semi active tags

In addition to passive and active RFID tags, there are also battery-assisted tags, sometimes called semi-passive or semi-active tags, in which the battery is used to power the tags. Battery-assisted tags may also have sensors to measure and record parameters such as temperature, humidity, pressure, etc..

1.2.2. RFID Readers

The RFID reader (which can be fixed or portable) is also composed of an electronic card and an antenna. The RFID tags communicate with one or several RFID readers over a radio channel. This communication can be made according to various frequencies. There are four main frequency bands used for RFID systems. The radio frequencies used can be low (LF) [125-150 KHz LF] or high (HF) [13.56 MHz HF] or ultra high (UHF) [433 MHZ or 860 to 960 MHz] or microwave [2.45 GHz]. The performances vary depending on the radio frequency used, notably in terms of reading distance or speed of interrogation by the reader or reaction to humid environments or to the presence of metals.

The RFID reader asks the RFID tag for the code or processes the signal being broadcast by the RFID tag. A dialogue establishes according to a predefined communication protocol and data are exchanged. An essential capacity of the reader is to avoid collisions among various RFID tags which use specific methods.

1.2.3. Computer System

The reader transforms the data transmitted by the RFID tags into digital data and transfers them to a computer. The computer may simply store them or look up the tag ID in a database to direct further action, and may also direct the reader to write additional information to the tag. The reader and the computer are connected by radio or by cables.

To sum up, RFID technology leads to very different applications, depending on the characteristics presented above that it integrates.

1.3. Advantages and Disadvantages of RFID compared to Barcodes

Originally, the important commercial use of RFID was the replacement of the barcodes. RFID has an enormous potential in the supply chain management. This is the clear lesson from a comparison between the two instruments.

1.3.1. Advantages over Barcode

Barcodes:

- Require labels to be "seen" by lasers. That line-of-sight between label and reader is often difficult, impractical, or even impossible to achieve in industrial environments;
- Are limited to the data printed on them and cannot be updated, other than by replacement or sticking a label over them (which may be labor intensive);
- Need to be substantially flat for reliable reading by lasers;
- Are typically (but not always) paper labels, or printed on paper based packaging, and therefore prone to damage;
- Typically provide inventory data to the level of product category. (For instance, it might indicate that the product is a 250g packet of Danish "Product Name" unsalted butter, but is unlikely to indicate the sell by date (shelf life), nor the best before date);
- Are very unlikely to show through which distribution depots and transport means the product arrived at the point of sale.

RFID advantages can overcome some of the limitations of barcodes:

- Readers do not require neither line-of-sight to the tag;
- The tag can stand a harsh environment;
- The tag can trigger security alarm systems if removed from its correct location;
- The tag can be read only or read/write depending on the RFID technology used;
- Because each tag has a unique ID, the reader may be able to recognize many tags in its field virtually simultaneously;
- Since each tag can be unique, they can act as a security feature if lost or stolen;
- The tag is more difficult to counterfeit than a barcode;
- The tag can hold more information than a barcode;
- The tag may be read more easily, more frequently and at longer distances. This improves the quality of information;

- Automatic scanning/reading and data logging is possible without operator intervention;
- Tracking objects, animals, persons in real time.

1.3.2. Disadvantages over Barcode

Despite all these advantages, the RFID technology has also some disadvantages.

- Tags remain more expensive than a printed barcode. This extra cost, plus the potential greater infrastructure capital cost, has to be bettered by other benefits or represent an application for which the barcode is not suitable;
- There is a high cost (long pay back) for integrating RFID technology into existing inventory systems;
- External influences such as metalwork or radio interferences can constrain RFID remote reading;
- Increasing RFID technology uptake also depends on standardization.

1.4. RFID and the "Internet of things"

During the last years, RFID has appeared at the vanguard of a much broader and deeper change of the Internet, which is described as "the Internet of things" (IoT), or sometimes Internet of the objects[9]. This new Internet could connect billions of objects and places. Originally, this concept was introduced by the MIT, Auto-ID center in 1999. Its determining features were radio frequency identification (RFID) on one side, and the electronic product code (EPC) on the other side.

Progressively, the concept developed into something much bigger and ambitious... but not necessarily better defined[10]. As the ITU anticipated in 2005, "developments are rapidly under way… by embedding short-range mobile transceivers into a wide array of additional gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves. A new dimension has been added to the world of information

9. On the connection between RFID and the Internet of things, see LU Y. et alii (eds.), *The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems* (Wireless Networks and Mobile Communications), Boca Raton: Auerbach Publ., 2008.
10. See C. FLOERKEMEIR et alli eds., The Internet of Things: First International Conference, IOT 2008, Zurich, Switzerland, March 26-28, 2008, Proceedings, Berlin: Springer, 2008; T. IGOE, Making Things Talk: Practical Methods for Connecting Physical Objects, London: Make Books, 2007.

and communication technologies (ICTs): from *anytime*, *any place* connectivity for *anyone*, we will now have connectivity for *anything*"[11].

The European Commission went still further in 2008, explaining that "these objects will be active participants in business and information processes, exchanging data including their identities, their physical properties and information 'sensed' about their environment"[12]. Such a definition introduces new elements, related to the devices' power and to their functioning autonomy. The concept becomes then an Internet of intelligent things. This deepening will have a lot of consequences. It will impose many new requirements on the network. It will generate a much greater heterogeneity of the Internet. Finally, connecting billions of objects to the Internet will of course multiply the privacy problems. From 2006, the European Commission has organized different conferences on the Internet of things. In 2006, a conference was meant to analyse the mutation "from RFID to the Internet of things – pervasive networked systems"[13]. In 2008, a workshop was organized again about the same topic[14].

Though the two projects are linked, it is necessary to distinguish clearly RFID and the Internet of Things. From a time perspective, many RFID systems already exist, but the Internet of Things remains essentially a project for the future. From a functional perspective, a RFID system can fully function without being connected to the Internet. Some enterprises will in fact be quite reluctant to connect their RFID system to the Internet since this would relinquish their control on absolutely strategic data, and also increase various security risks. On the other side, the Internet of Things can also function without RFID. A lot of other technologies can be used: NFC, GPS, GSM/GPRS/3G, Felica and Ipv6, for example.

11. ITU, *The Internet of things*, Internet reports n° 7, 2005.
http://www.itu.int/osg/spu/publications/internetofthings (accessed March 30, 2009).
12. European Commission staff working document, SEC (2008) 2516, p. 3.
13. ftp://ftp.cordis.europa.eu/pub/ist/docs/ka4/au_conf670306_buckley_en.pdf. (accessed April 23, 2009).
14. See ECC, Internet of things in 2020 – A roadmap for the future, September 05, 2008.
http://rp7.ffg.at/upload/medialibrary/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008.pdf.
(accessed April 19, 2009).

2. The Development of RFID Use

Though RFID systems are already deployed in various areas, recent trends indicate that the market of RFID technology will be booming in the next decade. The RFID technology offers a huge potential. It can radically change the way in which business processes are designed and executed. This means that it is potentially a very disruptive technology – probably as disruptive as the barcode was 30 years ago. Introducing a disruptive change into any organization is challenging. The larger that organization is, the harder that change is likely to be. This said, a wider take-up of RFID technology in the mass market depends also on the tags' falling prices and on standardization efforts.

RFID technology has also the potential to bring benefits to consumers and citizens. It could increase tremendously the information and services brought to the consumers. It could also help to increase the efficiency of services of general interest (security and health are obvious examples)[15]. However, this will only be realizable if appropriate guarantees (privacy safeguards, notice of presence of a RFID tag and choice of de-activation, security) are brought.

Finally, RFID technology should contribute to the development of the information society and to the promotion of innovation. In the future, indeed, it should be deployed in all sectors of the economy. For that reason, the European Commission considers that it has the potential to become a new motor of growth and jobs.

2.1. RFID and Sovereign Functions

RFID can facilitate some State's sovereign functions. For instance, Hitachi, the Japanese electronics company, has developed an extremely tiny RFID chip it calls the "mu-chip" which is reportedly able to make money counterfeit-proof. The USA requires that all US passports issued after October 2006 contain an RFID chip. The chip is meant to make passports impossible to forge.

The Council of the European Union adopted in 2004 the Regulation 2252/2004/CE mandating the inclusion of both facial image and fingerprints in future pass-

15. See D. WYLD, *RFID: the right frequency for government*, IBM Center for the business of government, 2005. For an interesting perspective on RFID and education, for example, see M. WARD, *RFID: Frequency, standards, adoption and innovation*, JISC, 2006, pp. 16-20. The increased use of RFID in the American schools to control students has provoked some controversies. See the California State Senate Bill (Simitian): http://www.aclusandiego.org/article_downloads/000678/SB%2029%20RFID%20Fact%20Sheet.pdf. (accessed May 12, 2009).

ports and travel documents issued by EU Member States[16]. This regulation aims at better protecting EU passports against forgery, at enabling better identification of passport holders and at harmonizing security standard features used in the production of passport and travel documents issued by Member States. Germany was the first EU Member State to introduce the first e-passport. These new German passports issued since 2005 contain a RFID chip which stores usual ID information but also biometric features.

In USA, RFID bracelets have been adopted in jails and prisons to reduce inmate violence. In USA again, RFID tags were implanted into human cadavers to help the authorities to speed up the process of identifying victims of hurricane Katrina.

2.2. RFID and Healthcare

RFID systems are progressively used in the health sector to improve patients' safety but also to reduce expenses[17]. There are already a lot of applications. They have of course important consequences about the protection of these most private data[18].

For instance, the firm VeryChip received the authorization in 2004 by the US Food and Drug Administration to sell their RFID tags for implantation into patients in hospitals. The VeryChip RFID device is injected just below the skin and its location is invisible to the naked eye. It contains a serial number or password that can be read by a specific scanner. The intent is to provide immediate positive identification of the patients in hospitals and in emergencies. Doctors, emergency-room personnel and ambulance crews can get this way immediate identification through the serial number which is entered into a computer database to access the medical file. If, for example, the patient is diabetic or allergic, this could be taken into account immediately and could avoid medical errors.

In certain hospitals, to prevent infant abduction, babies have RFID tags attached to their ankles by a bracelet. There are sensors on the doors to the maternity

16. OJ, 2004, L 385/1-6. See article 1.2.
17. In 2009, a detailed study was published by the European Commission. See A-M. VILAMOVSKA, E. HATZANDRIEU, R. SCHINDLER, C. VAN ORANJE, H. DE VRIES, J. KRAPELS, *Study on the requirements and options for RFID application in healthcare*, Rand Europe, 2008. http://ec.europa.eu/information_society/activities/health/docs/studies/200807-rfid-ehealth.pdf (accessed April 14, 2009).
18. See for example, J. KIL et alii, Towards a Security Policy for Ubiquitous Healthcare Systems, in *Ubiquitous Convergence Technology*, Springer, 2007, pp. 263-272.

ward, and if a baby passes through, an alarm goes off. Such RFID tags are also used to prevent accidental baby swaps.

RFID wristbands are also worn by adult patients to avoid mistaken identities because of duplicate names, misplaced record card or language difficulties. This in turn helps ensure patients are not given the wrong drugs. RFID wristbands are also worn by patients to track and find them easily within the hospital (for instance the patient is missing from the hospital bed or has several medical exams during a specific day). RFID systems are also used to accurately track and locate doctors and nurses in case of emergency as well as medical equipments.

2.3. RFID and Protection of Intellectual Property

A lot of products are nowadays continuously the target of counterfeiters. It is specially the case for pharmaceutical products. RFID tags can then be useful to check whether the content is genuine. That is applied by the firm Pfizer, for instance. This company, which produces Viagra, fights fake Viagra with RFID tags. It began in 2005 to affix RFID tags on bottles and pallets of Viagra used for shipments to USA in order to detect counterfeit pills. Pharmacists and drug distributors can retrieve the codes with a special reader and verify their authenticity by checking a Pfizer database via the Web.

2.4. RFID and Anti-Theft/Faster Recovery Capabilities

RFID systems are used to reduce thefts. Anti-theft hard plastic tags attached to merchandise in stores are RFID tags. FIFA implanted RFID tags in tickets to the 2006 World cup football matches in Germany in order to cut down the number of cases of theft, but also of counterfeiting and black market trading of ticket.

RFID tags are also used to track high-cost items (paintings, jewels, musical instruments, tools, trucks, cars, etc.) or critical equipment. This is particularly useful for faster recovery of the stolen items.

2.5. RFID and Payment Systems

Several companies (such as SmartCode Corporation or OTI or JCB, VIVOtech, SkyeTek, Société Générale in partnership with Visa and Gemalto, Alarci in

partnership with the Aduno group,etc…) have recently introduced RFID contact-less payment solutions which are meant for small or micro payments. These RFID solutions do not require any physical contact between the credit card (Visa, MasterCard, Amercian Express, etc.) and the terminal. The cardholder just taps or presents the card in front of the reader. This enables merchants and consumers to reduce card processing time and increase point of sale throughput. These RFID credit card solutions are suited for quick-service business such as movie theatres, convenience stores, gas stations, fast-food restaurants. In Europe, such solutions are envisaged to replace the Proton card.

Some initiatives are more audacious. For example, discotheques, such as the Baja Beach Club in Barcelona, use RFID tags as a club card for cashless payments. The club injects a chip under a member's skin using a syringe.

2.6. RFID and Supply Chain Management

Supply chain forms the backbone of an organization. It consists of manufacturers, retailers and their transportation partners. RFID technology has here the advantage to offer a complete visibility within such a chain, by making it fast, responsive and flexible. Here are two very different illustrations.

RFID technology has been introduced for use in the retail supply chain, for instance. The tagging of pallets, cases to make them traceable makes the supply chain more efficient. Eventually, RFID tags can be used to label individual retail items. Many large retailers, such as Wal-Mart, have instructed their suppliers to tag pallets and cases with RFID tags carrying the Product Electronic Code (EPC). Metro Group or Marks & Spencer have also began to use RFID tags (including on individual retail item) to track goods along the entire supply chain to optimize order and inventory management, avoid out-of-stock situation and help reduce costs. This Wal-Mart mandate has been an important step in persuading many enterprises to give more attention to RFID development[19]. Nonetheless, one must observe that many unforeseen problems have arisen in its implementation during the last years.

19. "Many of the original 600 companies are still tagging cases sent to several Wal-Mart distribution centers in Texas. While a handful of companies have stated they were getting benefits from the RFID-based data on inventory movements and consumption, the vast majority perceived nothing but cost from the program. Besides the cost of tags, companies have to manually apply the tags to cases, which often requires manually breaking down full pallets of product in the distribution center, tagging the goods, only to rebuild the pallets. This often brought the effective cost of tagging a case to 30 cents or more – a huge cost to consumer goods companies. In some cases, manufacturers bought expensive print-and-apply equipment, along with small conveyors and supporting software, to automate this DC tagging process." http://www.scdigest.com/assets/On_Target/08-01-08-2.php?cid=1399. (accessed April 18, 2009).

In USA, Blood Center of Wisconsin was awarded funds from the National Institutes of Health for the extension of a study to introduce RFID technology into the blood product supply chain. This would allow for improved identification, tracking and condition-monitoring of blood products across the entire transfusion medicine supply chain. The benefits of the technology would be twofold. RFID technology would have the potential to increase efficiency and accuracy in the material handling of blood products – reducing production and handling costs, and possibly healthcare cost as a result. It could also reduce or eliminate blood transfusion errors at the patient bedside.

In a very different context, RFID has been used by libraries or bookshops to simplify the organization of shelves, book referencing and book lending[20].

2.7. RFID and Food Retail Sector

In the food retail sector, RFID enhances products freshness in supermarkets, by monitoring expiration dates, helping inform retailers when to remove an item from a shelf, and thus preventing consumption of out-of-date products.

RFID technology can also help in food security and traceability. Animal tagging has shown its value in tracking livestock after the BSE (mad cow disease) outbreaks. However some technical problems remain. The EU IDEA project provides a very good illustration. It was launched in 1998 to control the reliability and the advantages of an electronic identification system of animals[21]. They were generally based on ruminal boluses (a stable encapsulated RFID tag introduced in the animal's stomach) or an ear tag.

20. "Advanced ID Corporation (OTCBB: AIDO), a leading developer of radio frequency identification ("RFID") technology for livestock tracking, pet recovery and supply chain applications focusing on the tire management industry, today announced that its recently introduced Ultra High Frequency 500 Series RFID reader has been selected for use and successfully implemented for item level tracking at a Portuguese retailer. This is the second European contract for the 500 Series readers since the product was introduced to the market in November 2007.
The recently opened book store Byblos in Lisbon, with over 35,000 square feet of selling area, is the biggest in the country and is the first to implement item level RFID, according to Creativesystems, the official distributor of Advanced ID's RFID reader and product lines in Portugal which handled this retail contract. All shelves, books, CDs, DVDs, and other products are uniquely identified with industry standard passive RFID tags that are read at the kiosks and points of sale in a fraction of a second." (source: RFID ready, February 18, 2008).
21. See the final report: http://idea.jrc.it/pdf%20report/7%20general.pdf. (accessed May 10, 2009).

2.8. RFID and Transport (including transport safety)

2.8.1. Road

Many toll collection systems function with RFID. In USA, toll road authorities have equipped drivers with a tag that is connected with their credit card. This allows them to pay their tolls at 40 miles-per-hour rather than stopping to throw quarters into a basket and slow the flow of traffic. In Europe, Austria's road toll system, for instance, uses stickers with an integrated RFIDtag. DaimlerCrysler offers a child seat with RFID. The tag controls the airbag pressure, helping to prevent injuries to small children. Car keys worldwide incorporate RFID technology.

2.8.2. Aviation

RFID technology is also use for baggage handling purposes in the aviation sector. At the checking point, baggage are tagged and readers installed in different sectios of the airports track the baggage as it moves from one airport to another and within the airport itself.

2.8.3. Public Transportation

Many public transportation tickets are already based on RFID technology. Some experiences have been organized during the last years. They sometimes provoked reactions from the consumers regarding their privacy's protection. Though such systems are also complex and costly[22], the advantages seem quite obvious and they are not contested: optimisation of the logistics, fight against fraudulent use, simplification of handling and control of the passengers, increased safety, connections with other services, etc.

2.9. RFID and Energy Networks

RFID also offers the possibility to improve the efficiency of energy networks[23]. By providing more about energy demand and transfers, it will allow both producers and customers to adjust better to the evolution of demand and offer. It is thus one important instrument in the development of the "Smart Grid"[24].

22. See B. MENEZES et alii, *Challenges in RFID Deployment – A Case Study in Public Transportation*, 2007. http://www.it.iitb.ac.in/~kamlesh/Page/Reports/iceg06.pdf. (accessed May 13, 2009).
23. See P. SEN, D. SEN and A. DAS, *RFID for Energy and Utility Industries*, Pennwell Books, 2009.
24. See CEC, *European Smartgrid Technology platform*, 2006. http://www.smartgrids.eu. (accessed May 5, 2009).

In the field of electricity especially, this could allow the transformation from a centralized to a decentralized structure of the network. This would permit bi-directional power flows, and also the growth of micro-producers. The development of smart grids would also increase the ability of networks to deal with the new problems created by the increased use of renewable energy, either solar or wind. Such systems can also improve the control of the network against possible degradation[25]. The use of RFID will depend on the costs, the potential of the existing infrastructures, and the existing regulations.

2.10. RFID and Access Control

RFID systems are now used for building access control. Security badges have been equipped with RFID tags to allow centralized control of access to facilities and specific rooms within buildings. These can also be used to track the locations of people in a facility by identifying the door they last passed through.

RFID systems are also used for parking access control applications. RFID tags are affixed to vehicle for activating hands-free access control to parking lots. Each access can be recorded in the computer's database to maintain an history of access activities and administer billing of daily, weekly or monthly fees.

2.11. What is the Potential of RFID?

Though real, the success of RFID has certainly been less impressive than foreseen around 2000. Tests were realized, deployments were launched, but not always as easily and successfully than anticipated. The Wal-Mart mandate and Metro experiments have revealed substantial problems. The costs were often higher than originally expected. The reading errors have been numerous. There remain compatibility problems between standards. It is therefore necessary to be careful and to distinguish the reality from the hype. This is difficult since most companies are generally not eager to provide too much information about their RFID projects[26]. They are seen, quite rightly, as an important part of their competitive advantage.

25. For example, IBM proposed such a service (R. WESSEL, Fly-By RFID for Monitoring Power Towers, *RFID Journal*, April 13, 2007).
26. One will find nonetheless interesting pieces of information in DGESTSI, *Etude sur les étiquettes électroniques et la traçabilité des objets – Panorama stratégique*, 2007, pp. 55-73; OECD, *RFID implementation in Germany: challenges and benefits*, 2007; Institute of Computer Science and Social Studies, *RFID Report 2008 – Optimizing business processes in Germany*, VDI Nachrichten, 2008.

A correct assessment of RFID potentialities requires a precise analysis of their benefits and costs. For various reasons, both are not always evident. From the point of view of benefits, some returns are quite obvious, but others may be more indirect, as it has been the case for the bar codes before. The return of close loop systems or in-house use is easier to analyze than for open loop systems or cross-company use.

From the point of view of costs, one must distinguish between the hardware (tags and readers), the middleware (filtering, routing, storage, device management, which ensure that erroneous, duplicated and redundant information is deleted) and the applications' software. The more RFID is sophisticated, the more it requires a reengineering of the production process. What seems fundamental in this domain is a proper integration into the companies' general information system. Collateral costs can become important, since most enterprises do not possess the required knowledge and must also launch training programs.

It remains that RFID is a technology which has much potential. Fundamentally, it could extend the productivity gains of the ICT sector during the last 20 years in many other sectors. Especially, it can revolutionize the supply chain. This explains why its first mass market will come from supply-chain management applications. RFID could thus become a new essential step in the digitalisation of human activities.

Seen from the point of view of the competitiveness of European enterprises, RFID could become quite important. The EU countries suffer from a weakness in some particular sectors, the ICT as the retail sectors in particular. Research is also weak in these sectors, which probably explains a good part of the problem[27]. RFID is quite clearly at the crossroads between those sectors.

27. See K. UPPENBERG, *RD in Europe – Expenditures among sectors, regions and firms sizes*, CEPS, 2009.

3. Potential Problems

RFID technology can provide useful services and can offer through them a lot of benefits to economic operators but also to citizens. However, it also raises worries. This was clearly indicated by the reactions to the European Commission 2006 consultation document. As a first step in this consultation, the Commission organised five workshops. They were based on five background papers[28] and covered an overview of the technological state of RFID development, the economic and societal rationale for different RFID applications, RFID security, data protection and privacy, health and safety issues, RFID interoperability, standardisation, governance and Intellectual Property Rights, and frequency spectrum requirements of RFID[29].

3.1. Privacy-related Issues

The public's greatest fears related to RFID generally concern privacy[30]. Adequate personal data protection and privacy safeguards remain key for a wide consumer acceptance of the technology. This is increased by the complexity of the RFID technology and more fundamentally by the fact that RFID is often invisible. The focus of consumers' concerns envisages scenarios where (a) the technology is used on individual products and (b) a link is made to personally identifiable information.

In that perspective, consumers generally indicate different significant private-related concerns. Firstly, they fear that third parties will use their data surreptitiously since anyone can detect the presence of particular RFID tags with a standard reader. Secondly, they fear that their product purchases will be tracked. Thirdly, they suspect that they could be targeted with more direct marketing. Fourthly and finally, they fear that tags will be read at a distance since retailers do not erase tag data on individual items after purchase. In other words, RFID tags are seen by consumers as a data aid linked to the person. The possibility to establish a link between the tracked item and the owning individual can reveal a person's history.

28. http://www.rfidconsultation.eu/docs/ficheiros. (accessed April 16, 2009).
29. CEC, Background document for public consultation on Radio Frequency Identification (RFID – Summary of five workshops, p. 4).
http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdfn (accessed April 16, 2009).
30. See for example K. ALBRECHT and L. McINTYRE, Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID, Nelson Current, 2006; M. ALBERGANTI, Le RFID et la démocratie, Actes Sud, 2007.

RFID has the capacity to promote strongly the creation of a real digital identity for humans[31]. This could be seen as an essential change in the relation between citizens and the State[32]. The tagging of humans is already a reality and the possibility of tagging babies has already been studied. Studies are even made on the possibility of associating nano-antennaes to the cell DNA. RFID can gather, store, analyse all kinds of personal data. The risk for privacy could still be aggravated by the use of nanotechnologies in this field. RFID tags can already be invisible now, but they could become undetectable even with a magnifying glass.

Specific privacy problems can rise in the workplace. RFID will certainly increase the enterprises' abilities to control their employees. There will be more possibilities to monitor employee location, activity and performance. For example, "in 2006, two workers of the US company Citywatcher were implanted with a RFID chip (MSNBC, 2006). Another example is a store of McDonalds (US) where employees are checked whether they have washed their hands after using the toilets, which was made possible by the application of RFID technology"[33].

However, the European authorities will have to thread very carefully here between contradictory interests. RFID can bring important advantages to individuals, too. It can also bring substantial productivity increases, and thus contribute to the competitiveness of the European enterprises. Most likely, it will be necessary to find compromises, and to begin to distinguish very different applications, rather than applying a general rule to all of them. Obviously, objects' identification systems are less dangerous than persons' identification systems. Closed systems are less dangerous than open ones. Some pieces of information (health, travel, payments) are clearly more sensible than others (retail, luggage).

3.2. Health-related Issues

Are radio waves emitted by RFID systems harmful for the health? Most publications consider them as harmless, but some assert that they could present some risks for health, notably because of their accumulation. One indicates that it would be useful to apply the precautionary principle until studies confirm that radio waves emitted by RFID are harmless. Recently, the French Health agency

31. See ETAG, *RFID and Identity Management in Everyday Life Striking the balance between convenience, choice and control*, 2007.
32. See J. ASHBOURN, *The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies*, 2005.
33. M. VAN LISHOUT et alii, *RFID Technologies: Emerging Issues, Challenges and Policy Options*, 2007, pp. 114.

(AFSSET) published a detailed report about these aspects[34]. The main conclusions were that, in general, the development of RFID would not create huge health threats. Nonetheless, they could create such threats in a work environment where the exposition to radio signals may become much more important. In the logistic chain, for example, workers could be permanently working among high powered readers in the high frequency spectrum.

Presently, the level of RF emission from RFID equipment must comply with limits established by various national regulatory agencies before the equipment can be placed on the market. The regulations for RF exposure limits that apply to cell phones, wireless remotes, WLAN and other wireless devices also apply to RFID systems. These national regulatory limits are based on international standards such as recommendations from the World Health Organisation (WHO) or the American National Standards Institute (ANSI). The WHO standards refer to the limits provided by the International Commission On Non-Ionising Radiation Protection (ICNIRP) – the body responsible for determining RF exposure limits.

3.3. Environmental Issues

The growing use of RFID tags can become a challenge not only for human health, but also for the environment. The more RFID is used for low added-value products, the more tags will be included in products which are currently either easily recyclable or biodegradable. For this reason, dealing with the waste of such products could become more difficult.

There are however two sides in this debate. RFID has also the ability to rationalize many production processes. It has also the ability to improve the efficiency of the energy consumption, or to reduce waste[35]. A global evaluation is thus complex.

3.4. Security-related Issues

The development of RFID will probably multiply the security risks[36]. Many threats are common to all information systems, though some, related to the

34. AFSSET, *Les systèmes d'identification par radiofréquences (RFID) – Evaluation des impacts sanitaires*, 2009.
http://www.afsset.fr/upload/bibliotheque/726108694775617668756800952202/RFID_Afsset_janvier_2009.pdf (accessed April 12, 2009).
35. See TechEx, *How green is RFID?*, 2009.
36. See German Federal Office for Information Security, *Security aspects and prospective applications of RFID systems*, 2004, pp 37-60.

transmission between tags and readers, are specific[37]. The results of a study conducted by a group of European computer researchers demonstrate that it is possible to insert a software virus into RFID tags.[38] The results of another study conducted by researchers, at the University of Massachusetts, have revealed potential security and privacy holes in a new generation of credit cards (credit cards whose data is relayed by radio waves without need of a signature or physical swiping through a machine), despite the fact that the card companies said that the data stored in the tags were encrypted. The researchers found that the cardholder's name and other data were being transmitted without encryption and in plain text. Because these cards can be read even through a wallet or an item of clothing, the security of information, the researchers said, is startlingly weak.[39] An additional source of insecurity comes from the undefined nature of the warranty given on RFID products, whether it concerns systems, readers, antennas pr RFID consultants.

Basically, greater data transfers require more computing capacity, and thus more risks of breakdowns, viruses, hackers, etc. The system is riskier but, in addition, the costs of a paralysis of the system will increase. In a hospital functions with RFID, the need to keep the transmissions and the computing becomes vital. Connecting RFID to the Internet will only compound these risks. To be honest, the Internet is not presently a great success from the point of view of security. Risks abound now, but they would become much greater with the permanent need to manage dozens of billions of new mobile addresses more.

Here too, the European authorities will need to thread carefully between conflicting objectives. The security preoccupation could lead to the adoption of proprietary standards, which would cost more and brake competition. From the point of view of the Internet governance, it could also lead to a centralized root and to the end of the "open structure" of Internet.

3.5. Jobs Issues

The question of jobs is seldom mentioned in debates or consultations about RFID[40]. In a long term, it nevertheless needs attention. Firstly, the reorganiza-

37. OECD, RFID: a focus on information security and privacy, 2008, pp. 25-36.
38. The researchers, M.R. RIEBACK; B. CRISPO; A.S. TANENBAUM, have posted their paper entitled "Is Your Cat Infected With a Computer Virus?", at http://www.rfidvirus.org.
39. See T. S. HEYDT-BENJAMIN et alii, *Vulnerabilities in First-Generation RFID-enabled Credit Cards*, 2007.
http://prisms.cs.umass.edu/~kevinfu/papers/RFID-CC-LNCS.pdf. (accessed May 10, 2009).
40. See, however, M. VAN LISHOUT et alii, *RFID Technologies: Emerging Issues, Challenges and Policy Options*, 2007, pp. 112-115; A. KRUSE, The regulatory framework for RFID, 2008, pp. 98-102.

tion of the supply chain thanks to RFID can certainly reduce costs, but through the suppression of different human functions. The obvious example here comes from the cashiers at the supermarkets, the controllers at the distribution centres, or some security services. Secondly, though new jobs will be created, they will require a lot of training[41].

Fundamentally, RFID will represent a new important step in the diffusion of ICT in the world of enterprises. In the long run, technology has generally positive effects. Nonetheless, it has also transitory disruptive ones.

3.6. Intellectual Property Issues

Some aspects of RFID can be covered by patents. As a matter of fact, the number of assigned patents related to RFID has increased from 1995. According to 2005 study, these patents do not present the same importance[42]. Most of them are not critical but a few of them are, because they cover a breakthrough technical specification. Interestingly, many of the key RFID patents originate in non-USA countries, but virtually all worldwide RFID patents are finally issued USA patent numbers.

This could brake the development of RFID in different ways. It is noteworthy to see that RFID vendor Intermec has for example introduced various law suits based on different of its patents[43] Enterprises will hesitate more to commit to systems controlled by others, and more expensive. Furthermore, in the perspective of an Internet-connected RFID, this could make the open and free character of the Internet more fragile.

3.7. Strategic Aspects related to the Internet of Things

The development of the Internet of things will require the definition of a unique universal numbering scheme. From that perspective, the present situation is a problem. EPC global and Ubiquitous Networking Lab have proposed two different methods allowing the identification of objects. Most unfortunately, these methods are not compatible. Furthermore, an object naming service (ONS) has been created in the framework of the EPCglobal architectural framework. It

41. See ILO, *Social and labour implications of the increased use of advanced retail technologies*, 2006.
42. See R. STEWART, A RFID patent update, *RFID Journal*, 2005.
http://www.rfidjournal.net/live05/IP/Room_miss_100pm_stewart.pdf. (accessed May 9, 2009).
43. See L. WIEBKING et alii, *A roadmap for RFID – Applications and technologies*, CE RFID, 2008, pp. 187-190.

should offer similar functionalities that the present Domain Name Service (DNS) for the Internet. However, this new framework would build a unipolar system where the root of the ONS could be controlled, and possibly blocked, by a single company or a single country. This perspective is bound to increase the present worries about the governance of the Internet.

From this point of view, it is important to remember that the governance of the present Internet has already provoked debates. They were linked, among other things, to the American control of much backbone and of ICANN[44]. These preoccupations were expressed by many UNO States, and by the European Union, at the World Summits on the Information Society (WSIS) of Geneva and Tunis in 2003 and 2005. They led to the creation of the international Internet Governance Forum (IGF). Such preoccupations will be increased by the development of the EPCglobal architecture and ONS. In this framework, the limited State's control provided by the DNS's address system would completely disappear[45].

In this context, the difference of approach between the USA and the EU remains quite striking. The American Minister of Defence (DoD) has been very active in the deployment of RFID. It is also involved in the board of EPCglobal, where it represents most interestingly the public sector. The American department of Homeland Security has commissioned a controversial report about the use of RFID for human identification, which was submitted to a consultation in 2006. This report expressed doubts about the security aspects of such a project and indicated that it would generate many privacy problems[46]. There were in 2008 twice as many American members than EU members in EPC[47]. Furthermore, EPC remains until now the most elaborate and known version of a full data standard. Obviously, the strategic aspects were not as prominent in the EU reflection process about RFID.

44. See for example the EC Commission's communications on the World Summits on the Information Society: COM (2003) 271, COM (2004) 111 et 480, and COM (2005) 234.
45. See F. ROURE, J.C. GORICHON, E. SARTORIUS, *Les technologies de radio-identification (RFID): enjeux industriels et questions sociétales*, GTI, 2005.
http://www.cgti.org/unique.php?personne=Jean-Claude%20GORICHON. (Accessed May 1, 2009).
46. See the draft submitted for consultation in 2006.
http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf. (accessed May 1, 2009).
47. From the legal point of view, EPCglobal is a joint venture of GS1 (formerly EAN International) and GS1 US™ (formerly Uniform Code Council, UCC).

4. The EU Regulatory Aspects of RFID

The European legislation remains in line with international rules or standards. The latter are mentioned here when it seems necessary to understand the EU legislation.

4.1. RFID and Radio Spectrum

The widespread adoption of RFID technologies depends on timely availability of Radio Spectrum in adequate quantity, suitable frequencies and bandwidth, and harmonization at global and European levels.

High frequencies, and especially UHF, are very important for the RFID development. Though they are more easily interrupted, such communications allow an extended read range, and this is essential for many applications in logistics and distribution. The band 840-960 MHz is essential for the development of logistical applications. It also supports the important EPC Class1 Gen2 standard. Most unfortunately, it is not yet harmonized in Europe. Furthermore, there are no unique global frequencies in the UHF band[48]. In 2008, "the leading frequency remained HF (13.56 MHz). In fact, HF RFID working at the ISO14443 specification was responsible for more than five times the expenditure on RFID to any other specification, with large new applications added such as passports and RFID enabled phones"[49].

Lower frequencies work better near water, metals or humans. In spite of one often reads, everything cannot be tagged, especially at high frequency; the world of frequencies has its own limitations. The lower frequencies have a limited range. On the other side, they are less regulated, which allows RFID to be used freely (for electronic car keys, for example).

4.1.1. At the International Level

At the global level, the ITU (International Telecommunication Union) seeks to coordinate spectrum use. The ITU's World Radiocommunication Conferences (WRC) take place every two to three years to review, and when necessary, revise the Radio Regulations which form the international treaty governing the use of the radio frequency spectrum. The ITU also holds Regional Radiocommunica-

48. See E. WALK et alii, *RFID standards and radio regulations*, CE RFID, 2008, pp. 89-94.
49. IDTechEx, RFID Market Forecasts 2009-2019, 2009.

tion Conferences (RRC). These are conferences of either an ITU Region or a group of countries with a mandate to develop an agreement concerning a particular radiocommunication service or frequency band. RRCs cannot, modify the Radio Regulations, and the decisions of an RRC are only binding on those countries that are party to the agreement.

Until now, there are not many internationally agreed frequencies for RFID operations (essentially 13.56 MHz)[50]. At the end of 2008, ISO has revised the International Standard ISO/IEC 18000-1. It defines the generic architecture concepts in which item identification may be commonly required within the logistics and supply chain and defines the parameters that need to be determined in any standardized air interface definition in the subsequent parts of ISO/IEC 18000. Nonetheless, the permitted scanner/reader powers differ between countries. Furthermore, there are different approaches regarding UHF use in the United States, the European Union and Japan, which are linked to different spectrum uses regarding mobile communications.

The following table reveals the complexity of the frequencies' problems (particularly in the UHF bands). This can be an obstacle to international trade of products labelled with RFID[51].

	Low Frequencies (LF)	High Frequencies (HF)	Ultra High Frequencies (UHF)	Special High Frequencies (SHF)
Region 1 Europe and Africa	< 135 kHz	13,56 MHz	865,0-868,0 MHz	2,446-2,454 GHz
Region 2 North and South America	< 135 kHz	13,56 MHz	902-928 MHz	2,4-2,4835 GHz
Region 3 Asia and Oceania	< 135 kHz	13,56 MHz	No harmonization. For instance: 952-954 MHz (Japan) 910-914 MHz (Korea) 865-867 MHz (India) 918-926 MHz (Australia)	2,427-2,47 GHz

It has sometimes been recommended, as a general rule, to use open frequency bands, particularly ISM (Industrial, Scientific and Medical) bands. However, the problems with such bands are, on the one hand, that they are overloaded and, on the other hand, that they are not harmonized at the international level. For

50. ISO/IEC 18000-1:2008, Information technology – Radio frequency identification for item management – Reference architecture and definition of parameters to be standardized.
51. This table is extracted from the following document: DGESTSI, *Etude sur les etiquettes électroniques et la traçabilité des objets – Panorama Stratégique* – 2007, pp. 88, spec. p. 35.

that reason, it is always necessary to check, in a given country, which frequencies are used, the power strength and the maximum gain of effectively authorized antennas.

4.1.2. At the European Union level

Directives 2002/77/EC, 2002/20/EC and 2002/21/EC already set principles related to the management, the allocation, the use and the transfer of radiofrequencies. In addition, Decision 676/2002/EC gives the European Union an increasing role concerning Radio Spectrum. This decision seeks to:

- relate spectrum demands to EU policy;
- ensure, where appropriate, harmonization measures with regard to the availability and efficient use of radio spectrum necessary for the establishment and functioning of the internal market [the European Commission assisted by a Radio Spectrum Committee (RSC) places mandates on CEPT (European Conference of Postal and Telecommunication Administrations) which has a specific technical expertise in the area of spectrum management. The European Commission can then issue an EU Decision based on the CEPT technical proposal following approval by the RSC (qualified majority is needed) which is applicable throughout the European Union];
- increase transparency and information on the use of spectrum by requiring Member States to publish spectrum tables and other relevant information in a common format accessible to all interested parties;
- promote European interests in international negotiations.

RFID technology is classified by CEPT in what is called "Short Range Devices "SRDs"[52]. The CEPT has been dealing with coordination of spectrum usage conditions for SRDs for many years. It has developed in the mid-1990s and has maintained recommendation 70-03 which opens the 856-868 MHZ UHF spectrum to SRDs.[53] In 2004 and 2005, the Commission mandated the CEPT to address more specifically the topic of SRDs in Europe. The first mandate (2004) concerned the harmonization of SRD spectrum.[54] The second mandate (2005) concerned the improvement of the effectiveness and flexibility of spectrum avail-

52. To be complete, "Short Range Devices" are low power transmitters which have low capabilities of causing interference to radio services. They are used for many types of applications such as alarms, local communications, door openers, medical implants and RFID applications. They are usually mass-market products.

53. It should be noted that the provisions of this recommendation reflect a consensus among CEPT members, but are not legally enforceable.

54. See doc. RSCOM 04-07 EN Final (Revised) dated 3 March 2004 and doc. entitled "Second Mandate to CEPT to develop a strategy to improve the effectiveness and flexibility of spectrum availability for Short Range Devices (SRDs) dated 10 March 2005, DG INFOSO/B4 final.

ability for SRDs in the European Union.[55] CEPT's reports on these mandates were issued respectively in 2004[56] and 2006[57]. On the basis of these reports, and taking into account recommendation 70-03, two decisions were adopted in 2006 by the Commission.

The first decision 2006/771/EC is a framework decision on EU harmonization of spectrum (frequency bands and technical parameters) for SRDs[58]. It foresees five important things: (a) a licence-exempt use of radio spectrum for SRDs; this means that their use is not subject to individual authorization pursuant to Directive 2002/20/EC; (b) an exclusive responsibility of manufacturers to guarantee SRDs' users against harmful interference originating from radiocommunications services in conformity with Directive 1999/5/EC; (c) a classification of SRDs as "Class 1" equipment under Decision 2000/299/EC[59], which means that SRDs can be placed on the market and put into service without restriction in the whole Community; (d) a possibility for Member States to allow SRDs to operate under less restrictive conditions than those specified in the technical Annex to the decision, with the inconvenience in this case that SRDs are considered as "Class 2" equipments under Decision 2000/299/EC which cannot operate throughout the Community without restrictions; (e) a regular update of the technical Annex to the decision establishing the list of frequencies and associated conditions of use. CEPT has been given a permanent mandate with regard to this annual update of the technical Annex[60]. It is requested to deliver a proposal for amendment of the technical Annex to the Decision in July of each year. This permanent mandate also includes a provision allowing the Commission services to provide "input and orientations" to CEPT to support the preparation of the yearly update of the Decision. Such "input and orientations" should help prioritise the activities undertaken by CEPT in this context.

The first decision 2006/771/EC has been amended by decision 2009/381/EC[61]. The latter replaces the technical Annex with an updated version, while leaving unchanged the article of the decision 2006/771/EC which had already been modified previously by decision 2008/432/CE[62].

55. See doc. RSCOM 05-07 (Rev.1).
56. See doc. RSCOM 04-66 (Rev. 1).
57. See doc. RSCOM 06-77.
58. Commission Decision 2006/771/EC of 9 November 2006 on harmonization of radio spectrum for use by short range devices (OJEU 2006, L 312/66).
59. Decision 2000/299/EC of 6 April 2000 establishing the initial classification of radio equipment and telecommunications terminal equipment and associated identifiers (OJEC 2000, L 97/13).
60. See doc. RSCOM 06-27 Rev. and RSCOM 06-94.
61. OJEU 2008, L 151/49.
62. OJEU 2009, L 119/32.

The second decision 2006/804/EC covers more specifically RFID and aims at ensuring the availability of harmonized frequencies in the UHF band within the European Union[63]. The latter foresees in its Annex the frequency bands and their conditions of use. The table below reflects the Annex and shows that only 3 MHz of spectrum is available in Europe for RFID (compared with 26 MHz available in the United States, which is a very important asymmetry). In order to maximize efficient spectrum use, however, this relatively narrow bandwidth is divided into 15 channels of 200 KHz each. A very important progress comes from the increase of radio frequency power to 80% of that allowed in North America. This means that the range performance will be quite similar in the two regions[64].

UHF Frequency band	Specific conditions	
	Max. power/Field strength	Channel spacing
Sub-band A: 865-865,6 MHz	100 mW e.r.p.	200 kHz
Sub-band B: 865,6-867,6 MHz	2 W e.r.p.	200 kHz
Sub-band C. 867,6-868 MHz	500 mW e.r.p.	200 kHz

Channel centre frequencies are 864,9 MHz + (0,2 MHz × channel number).
The available channel numbers for each sub-band are:
Sub-band A: channel numbers 1 to 3;
Sub-band B: channel numbers 4 to 13;
Sub-band C: channel numbers 14 and 15.

Fundamentally, the development of RFID will impose changes in the management of frequencies in the European Union, for a very simple reason. RFID will provoke a much higher use of the spectrum. This will provoke of course problems of collision. One of the most important present problems comes from the difficulty of reading too many signals at once. The error rate in retail remains too high. One must thus increase the ability of readers to analyze the signals, but this will not be possible without increasing the complexity of the signals and the capacity of the networks. But the most important long term problem will probably be the capacity of the spectrum. RFID will require the secure and simultaneous transmission of many signals over the same frequency range. This will require a lot of computing power... and another regulatory framework.

63. Commission Decision 2006/804/EC of 23 November 2006 on harmonisation of the radio spectrum for radio frequency identification (RFID) devices operating in the ultra high frequency (UHF) band (OJEU 2007, L 329/64).
64. So far, only France has introduced a request for a transitional derogation to decision 2006/804/EC. It has been granted by a Commission decision 2007/346/EC of 16 May 2007 granting a derogation requested by France pursuant to Decision 2006/804/EC on harmonisation of the radio spectrum for radio frequency identification (RFID) devices operating in the ultra high frequency (UHF) band (OJEU 2007, L 130/43).

From this perspective, the reforms of the 2002 regulatory framework proposed by the European Commission in 2007 must be considered as essential[65]. The Decision 2002/676/EC of the European Parliament and of the Council on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision)[66] does not appear sufficient.

4.2. RFID and Standardization

Any technology needs standards to gain wide international acceptance and RFID is no exception. Indeed, the realization of the benefits of RFID technology is very dependent, particularly for commercial uses, on open standards. The lack of standards means that firms will be forced to incur high costs to ensure compatibility with multiple readers and tags.

There are many well-established standards for RFID systems and they are still evolving. One must distinguish two types of standards for the implementation of RFID technology. There are technical standards which specify performance requirements for interoperability. There are also application standards often set by industry associations that describe how RFID can be used for a specific function.

4.2.1. At the International Level

A. Technical Standards

There are several international standardization bodies which focus on technical standards that are accepted globally (ISO, IEC, ITU). Among them, ISO (International Organization for standardization) plays an essential role concerning RFID technologies. In brief, ISO has developed generic standards (for instance, ISO 18000 family standards, adopted in 2004 and 2005 and developed by ISO/IEC JTC1/SC31 committee, covering much of the RFID air interface requirements for logistics/supply chain/manufacturing) and for item management (for instance, ISO/IEC 15963). With ISO/IEC 15963, the ISO approach is closely akin with the EPCglobal approach underneath. ISO also has developed sector specific standards for RFID tags [for instance, freight containers (ISO 10374 currently being replaced), cattle (ISO 11784, 11785 and 14223), ...].

65. See COM (2007) 697, 698 and 699.
66. OJEU 2002, L 108/1.

ISO is the main international source, but it is not the only one. For example, sector specific standards organisations have also defined RFID standards, such as the specification for RFID biometric passports adopted by the International Civil Aviation Association (ICAO). This one defines how ISO 14443 standard on contactless smartcards should be implemented for travel documents (ICAO, 2004). The Automotive Industry Action Group (AIAG) has defined a "Application Standard for RFID Devices in the Automotive Industry" (ARF-1) or "Tire and Wheel Identification Label Standard" (B-11).

B. Application Standards

Formerly known as the Auto-ID Centre, EPCglobal Inc.'s main focus is the standardization of the data format embedded in the RFID tag or label. It has established the Electronic Product Code (EPC). EPC is simply a number, typically from 64 to 256 bits long, for the identification (and tracking) of individual items (for instance, one knows not only that the item in question is a can of X, but which can of X it is). This is an internationally accepted item-level code[67]. RFID is the favored medium to transmit and read that number remotely, and thus EPC and RFID are complementary. The former Auto-ID Centre chose not to select a specific type of RFID system to be used for EPCs in order to allow maximum flexibility in the choice of frequencies. For sure, EPC has helped to significantly increase the adoption of RFID products across Europe and North America.

EPCglobal Inc., has also established a standard on how information is passed from RFID readers to various applications, as well as from application to application in the supply chain. This standard set for supply chain management is referred to as "GEN 2". Tags that comply with EPCglobal's GEN 2 standard are designed to operate between 860 MHz-960 MHz without degradation in performance. GEN 2 allows for global interoperability (of EPC systems) and creates a single converged standard. The process of ISO/IEC standardization of EPC GEN 2 is ongoing. Nevertheless, international application standards remain insufficient and many existing standards are only available at the national level. They also often have a rather narrow focus.

4.2.2. At the European Union Level

The aim of the EU standardization consists in supporting both the approximation of legislation for the establishment, operation and consolidation of the internal market (technical harmonization) and improving the competitiveness of

67. About EPC, see E. SCHUSTER, S. ALLEN and D. BROCK, *Global RFID: The Value of the EPCglobal Network for Supply Chain Management*, Berlin: Springer, 2007.

firms. Technical harmonization measures can cover a range of subjects, among which security and interoperability aspects. Apart from the internal market aspect, European standardization can support a wide range of Community policies aimed at boosting the competitiveness of European firms.

The European Union recognizes three European standards organizations[68], i.e. CEN (European Committee for Standardization), Cenelec (European Committee for Electrotechnical Standardization) and ETSI (European Telecommunications Standards Institute). Standardization work is entrusted to these European standards organizations on the basis of the European Commission's requests for standardization issued after consulting the Committee referred to in Directive 98/34/EC[69] in accordance with the provisions laid down in the Directive and those of Decision 87/95/EEC in the field of information technology and telecommunications (ICT)[70].

These European standards organizations base their work on international standards. Where international standards exist, they are, wherever possible, uniformly transposed by the European standards organizations and used as a basis for Community legislation. They have been granted a Community financing for their activities since the adoption of Decision 1673/2006/EC[71]. With regard to RFID, in addition to standards provided by ISO, the Commission relies on standards proposed in particular by ETSI. ETSI was created in 1988 by CEPT. The latter transferred all its standardization activities to ETSI.

RFID standards can be divided into twelve categories[72]. They encompass General standards – describing the basics and the structure of systems, and vocabularies, EC legislation – legal framework, Harmonised standards and frequency regulations, Air interface standards, Reader interface standards, Data management and Interface standards, Data standards, Sensor standards, Application interface standards, Application standards, Information network service & interface standards and Guidelines. One could conclude in some ways that an essential barrier to RFID expansion precisely lies in an overdose of standards. There are from this point of view contradictory pressures in favour of more

68. See Annex I of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations (OJEC 1998, L 204/37). This Directive was modified by Directive 98/48/EC (OJEU 1998, L 217/18) and by Directive 2006/96/EC (OJEU 2006, L 363/81).
69. Op. cit.
70. Council Decision 87/95/ECC of 22 December 1986 on standardization in the field of information technology and telecommunications (OJEC 1987, L 36/31).This Decision was modified by Regulation N° 807/2003 (OJEU 2003, L 122/36).
71. Decision 1673/2006/EC of the European Parliament and of the Council of 24 October 2006 on the financing of European standardization (OJEU 2006, L 315/9).
72. See E. WALK et alii, *RFID standards and radio regulations*, CE RFID, 2008, p. 17.

centralization (for the sake of connection) or more decentralization (for the sake of innovation). The balance is certainly not an easy one to find. One cannot contest anyway the need of less but broader standards.

ETSI is in charge of proposing technical standards that European countries have the choice to apply or not. For ETSI, RFID technology is classified in what is called "Short Range Device". ETSI standards relevant to RFID operations in the UHF bands are defined in ETSI EN 300-220 and ETSI EN 302 208. The latter, adopted in 2004, allows RFID readers to use more power and operate in a wider UHF band to perform nearly as well as UHF readers operating under the FCC rules in the USA. ETSI EN 302 208 provides a narrow band of frequencies allocated to RFID in the range of 865 MHz to 868 MHz, with channel spacing of 200 kHz.

4.3. Radio Equipment

The development of a single market for wireless equipment is an objective of Directive 1999/5/EC (R&TTE Directive). Placement on the market and into service of wireless equipment throughout the EU is regulated by this Directive. If equipment falls under the so-called "Class 1" category, it may be used in all Member States without restrictions. In addition, manufacturers must ensure that RFID devices effectively use the radio frequency spectrum so as to avoid harmful interference to other SRDs.

More generally, this Directive relies for its operation on harmonized standards developed by ETSI at the request of the European Commission. These harmonized standards define technical characteristics which can be used to meet the essential requirements of the Directive, which include effective use of the radio spectrum and orbital resource so as to avoid harmful interference.

Finally, as spectrum management remains a national matter, authorities in the Member States are allowed to regulate radio interfaces, but are required to publish their regulations.

4.4. Environment Protection

RFID tags have the reputation to contain potentially polluting elements (for example copper, silver, glues, ...). From the environmental perspective, according to the European Commission, RFID meets the definition of electrical and electronic equipment provided for in the directives 2002/96/EC on waste elec-

trical and electronic equipment (WEEE) and 2002/95/EC on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS). It can "be considered to fall under Category 3 "IT and telecommunication equipment".

RFID products are covered by the RoHS Directive. The situation is slightly different in the WEEE Directive. If RFID tags are put on the packaging of the electrical and electronic equipment they are considered to fall outside the scope of the Directive because they are part of a product that is not covered by the WEEE Directive. If they are put on the equipment, the producer of the equipment is responsible for recycling[73]".

4.5. Health

The use of spectrum is subject to the requirements of EU law for public health protection. The framework in place intends to protect workers and citizens. It recommends limits to exposure to electromagnetic fields (EMF) of the general public (Council recommendation 1999/519/EC currently under review) and imposes strict rules for the exposure of workers (directive 2004/40/EC). In addition, directive 1999/5/EC, already mentioned above, imposes restrictions on EMF emissions from products to ensure the safety of both users and non-users.

Electromagnetic fields (EMF) related to RFID applications are generally low in power. In such cases, and under normal circumstances, the exposure of general public and workers to RFID-related EMF is expected to remain below the current standards limits. However, the RFID take-up is expected to take place alongside a general growth of wireless applications (mobile TV, digital TV, wireless broadband, etc.). The respect of the EU framework must thus remain controlled regularly, and research deepened.

4.6. Personal Data and Privacy

The basic principles set out in the data protection Directive 95/46/EC and the Directive 2002/58/EC on privacy and electronic communications apply to information collected through RFID technology. Under those directives, Member

73. CEC, *Frequently Asked Questions on Directive 2002/95/EC on the Restriction of the Use of certain Hazardous Substances in Electrical and Electronic Equipment (RoHS) and Directive 2002/96/EC on Waste Electrical and Electronic Equipment (WEEE)*, 2005, p. 13. http://ec.europa.eu/environment/waste/pdf/faq_weee.pdf. (accessed May 4, 2009).

States have to ensure that RFID applications comply with relevant data protection legislation. Both directives foresee the drawing up of Codes of Practice which can be reviewed at national level by competent authorities (Office of the Information Commissioner in the UK) and at European level by the 'Article 29 Working Party' (consisting of national data protection authorities and the European Data Protection Supervisor).

In 2005, the Group 29 on Data protection issues, created in the framework of directive 95/45 on private data protection, produced a working document providing an overview of personal data and privacy implications when RFID technology is used[74]. This document gives also guidance to the manufacturers of the technology (RFID tags, readers, applications) as well as RFID standardization bodies on their responsibilities towards designing privacy compliant technology in order to enable deployers of the technology to carry out their obligations under the data protection Directive.

Besides these preoccupations, there are also worries about the risk that governments could use RFID technology to pry into the privacy sphere of individuals. For instance, passports equipped with RFID technology would allow governments to know where an identified individual travels at all times. This obviously impacts individual privacy. All this shows how necessary it is to develop systems that comply with personal data protection and privacy expectations, without preventing useful services.

Technical solutions to protect consumer privacy, more particularly in retail, are emerging though. Solutions such as the use of physical RFID tag structure that permit a consumer to disable a tag by mechanically altering the tag in such a way that the ability of a reader to interrogate the RFID tag by wireless means is inhibited. This structure is called "clipped tags".[75] These technical solutions could be complemented with appropriate legal solutions.

The Commission has anyway indicated that it intents to investigate if and to which extent the provision of the existing directives on personal data protection and privacy should be modified. Meanwhile, it has already proposed a modification of the Directive 2002/58 (e-privacy) to cover expressly RFID[76]. The

74. WP 105, January 19, 2005, pp. 21, spec. pp. 5-7.
75. G. KARJOTH and P. MOSKOWITZ, Clipped Tags – Deactivating RFID Tags with Visual Confirmation, 2005, pp. 4. See http://www.alphaworks.ibm.com/g/g.nsf/img/rfiddocs/$file/clippedtags.pdf. See also P. MOSKOWITZ et al., Privacy-Enhancing Radio Frequency Identification Tag: Implementation of the Clipped Tag, White Paper, IBM – Printronix – Marnlen, 2006, pp. 4. See http://www.alphaworks.ibm.com/g/g.nsf/img/rfidwhitepaper/$file/rfidjournallive.pdf. (accessed May 6, 2009).
76. See the proposal for a new article 3 (COM [2007] 698), as well as the compromise adopted by the European Parliament on May 6, 2009.

applicability of this directive to RFID remains contested until now[77]. What constitutes precisely personal data remains uncertain.

In an opinion of 2007, the European Data Protection Supervisor has rightly described RFID as "a fundamentally new technological development"[78]. In that context, the opinion did not generally suggest the adoption of a specific legislation. Nonetheless, it underlined the need "to prescribe that privacy and data protection safeguards must be included in the manufacturing of RFID systems, a concept that is known as 'privacy by design'"[79]. It also affirmed that "the 'opt-in principle' at the point of sale is a legal obligation that already exists under the Data Protection Directive in most situations", but that the specification of this obligation in self-regulatory agreements would be useful[80].

In 2009, the Commission has adopted a recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification[81]. This recommendation makes a strong application of the precaution principle in his field. It considers that privacy and information security features should be built into RFID applications before their widespread use (principle of 'security and privacy-bydesign'). Furthermore, an assessment of the privacy and data protection impacts carried by the operator prior to the implementation of an RFID application should provide the information required for appropriate protective measures.

4.7. EU Research Programs

Though they do not define an EU framework, EU research projects may have an influence on the development of RFID in the Member States. Different projects covering RFID are supported by the FP7. One of them is CASAGRAS (Coordination and Support Action for Global RFID-related Standardization Activities). It associates organizations from the EU, China, Japan, Korea and the USA[82]. Another project is GRIFS (Global Interoperability Forum for Standards)[83]. Both of them aim at developing and improving standards. Another one is CERP

77. See B. SCHERMER and M. DURINCK, *Privacyrechttelijke aspecten van RFID*, ECPnl, 2005.
78. OJ 2008, C 101/1.
79. § 60.
80. § 50.
81. Recommandation of 12.5.2009, C (2009) 3200.
http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf. (accessed May 13, 2009).
82. http://www.rfidglobal.eu. (accessed May 6, 2009).
83. http://www.grifs-project.eu. (accessed April 23, 2009).

(Cluster of European Research Projects on The Internet Of Things)[84]. This project aims at facilitating networking of different RFID and IoT projects in Europe and at coordinating research activities in IoT including RFID.

84. http://www.rfid-in-action.eu/cerp. (accessed April 23, 2009).

5. Next EU Steps

The European RFID regulatory environment supporting European companies in their investment efforts to deploy RFID technology as well as the general public in its call for protection of personal data and privacy, health and so on is not very consistent as we have seen. For that reason, the Commission has established an ambitious calendar for the creation of a regulatory environment that encourages the use of the RFID technology in Europe, guaranteeing at the same time the protection of personal data, effective safeguards for health and fundamental values.

In a first phase, the Commission has organized five workshops to evaluate the potential of the RFID technology for the enterprises and the society, but also to take into account the concerns about security and respect of privacy. The second phase of the debate was marked by the launch of a public consultation in 2006[85]. The results of the workshops and of the public consultation were presented at the "RFID Heading for the future" conference on 16 October 2006[86]. A communication entitled "RFID in Europe – Steps toward a policy framework"[87] was presented on 15 March 2007. This communication was accompanied by a Commission staff working document[88]. According to this communication, RFID is technologically and commercially ready, but several factors are holding back its take-up.

Concerning the data protection and privacy challenge and the security challenge, the communication is finely shaded. An important aspect of the response would be the specification and adoption of design criteria that avoid risks to privacy and security, not only at the technological but also at the organizational and business process levels. In addition, good practices should be developed to address new security threats and related countermeasures to support the widespread deployment of RFID systems. However, as RFID information systems, and related security and privacy risks are a moving target, it requires continuous monitoring, assessment, guidance, regulation and R&D. A close examination of the cost and benefits of specific security and privacy-related risks prior to the selection of RFID systems and the deployment of RFID applications is thus needed. An information campaigns towards the public should also be an essential part of the policy response.

85. http://www.rfidconsultation.eu. (accessed April 18, 2009).
86. See M. VAN DE VOORT and A. LIGTVOET, Towards an RFID policy for Europe – workshop report, 2006.
http://www.rfidconsultation.eu/docs/ficheiros/RFID_Workshop_Reports_Final.pdf (accessed April 11, 2009).
87. COM (2007) 96 final.
88. SEC (2007) 312.

The Commission indicated in a 2008 consultation that it tends to support an opt-in principle. This has been contested by various sides of the industry. They invoke that this could impose huge costs to retailers, especially SMEs, prevent interesting after-sales use projects and finally be negative for the EU's competitiveness. An increasing tension appears between the needs of protecting privacy on one side, and of preventing a loss of competitiveness of the European producers on the other side. The 2009 recommendation of the Commission on the implementation of privacy and data protection principles in applications supported by radio-frequency identification is finally more balanced on this point.

Concerning the environmental and health aspects, the communication enumerates the existing regulations. It adds that electromagnetic fields related to RFID applications are generally low in power and in such cases, and under normal operating conditions, exposure of the general public and workers to RFID-related EMF is expected to be well below the current standard limits. However, RFID take-up is expected to happen alongside a general increase in wireless applications (Mobile TV, Digital TV, Wireless broadband, etc.). For that reason, the Commission intends to monitor the respect of the legal framework at EU and/or Member State level, and to actively support research and review of scientific evidence, especially in relation to the cumulative effects of exposure to EMF from different sources.

Concerning standardization and radio spectrum, the communication indicates that the Commission will pursue on-going initiatives in co-operation and dialogue with the relevant stakeholders. International contacts with third countries administrations (particularly in USA and Asia) will also be strengthened with the objective to strive global interoperability on the basis of open, fair and transparent international standards. The Commission may also use its competence under the Radio Spectrum Decision to identify additional harmonized spectrum for RFID throughout the Community.

Finally, concerning the Internet of things, the Commission intends to initiate a series of actions as mentioned in its new action plan for Europe[89].

89. Commission's communication on the Internet of things – An action plan for Europe [COM (2009) 278].

6. Conclusion

Is RFID the new ICT "killer application" or the new "big brother" (though maybe the too small brother could seem more accurate?). RFID is in any case an old technology, which, thanks to its rising efficiency and diminishing costs, offers now many new perspectives. Its deployment during the last years has been impressive, though it has also revealed the existence of substantial technical and regulatory problems. Its deployment during the next years should be impressive, though probably not as much as various stakeholders have promised.

Enterprises must be careful to assess correctly and reasonably the productivity potential, the required technologies, the required adaptations of the production process, and the long term costs of RFID. This is no easy assessment. RFID is but the prominent member of a family of wireless technologies. It is thus useful to develop a strategy based on the global vision of the family. RFID itself is a broad family, with various sophistication levels, various costs, various potentialities. Business and administrations thus need to have a serious reflection on their real long term needs.

The Internet of Things is linked to RFID, since RFID is presently the most important illustration of electronic connections between objects. This said, the Internet of Things is a concept much more complex and much less defined. One forgets often in this context to think firstly about added value rather than about the network design.

The development of RFID in Europe requires a delicate regulatory balance in different domains. The most important one concerns the protection of privacy. The technology's potential to reduce the scope of privacy is enormous. This challenge will only grow in time. The European Union will most probably need to define new protective barriers in the future. Meanwhile, it will have to apply seriously the existing regulations, which is in itself a challenge considering their present very weak efficiency. A second challenge concerns the balancing of standardisation requirements. Too little standardisation can be a problem, too much standardisation also. Most probably, the solution lies in the defining of common standards, but with as much free access resources as possible. The use of too many intellectual property rights could appear extremely costly in the long term. From both points of view, the consultation process opened by the European Commission in 2006 was certainly timely. A continued balanced approach in the next years will most likely help RFID to become the new "killer application" in the ICT world… without becoming the new "big brother".