RADIO FREQUENCY IDENTIFICATION AND ITS EFFECT ON PRIVACY

How does the EPCglobal standard fit into the regulatory environment of the European Union?

Candidate number: 8002
Supervisor: Dr. Lee A. Bygrave
Deadline for submission: September 1, 2007

Number of words: 16,686 (max. 18.000)

19.09.2007

Content

1 INTRODUCTION 1

1.1 Research material, definitions and thesis structure 4

2 THE TECHNOLOGY 7

2.1 The Internet of Things 7

2.2 Components of an RFID system 8

2.3 Security 9

2.4 Privacy 10

2.5 Conclusion of technology discussion 13

3 PRIVACY 15

3.1 Introduction 15

3.2 *De lege lata* 16

3.2.1 Guidelines for RFID deployers and data controllers 17

3.2.2 EU Decisions regulating the radio spectrum 23

***3.3 De lege ferenda* 24**

3.4 Personal data affected by RFID technology 26

3.4.1 The concept of personal data 27

3.4.2 Personal data stored on the RFID tag 28

3.4.3 Personal data linkable to tag 28

3.4.4 Targeting, tracking and/or profiling 29

3.5 Conclusion of privacy discussion 30

4 THE ELECTRONIC PRODUCT CODE AND THE EPCGLOBAL NETWORK 32

4.1 The Electronic Product Code 33

4.2 EPC Middleware 35

4.3 EPCglobal Network Information Services 36

4.3.1 Object Naming Service (ONS) 36

4.3.2 EPC Information Services (EPCIS) 37

4.3.3 EPC Discovery Services (EPCDS) 37

4.4 How the EPCglobal Networks Works 37

4.5 Conclusion of EPC discussion 38

5 WHAT NEEDS TO BE DONE TO ENSURE THAT THE EPC STANDARD IS COMPLIANT WITH THE DATA PROTECTION DIRECTIVE AND OTHER EUROPEAN UNION REGULATION ON RFID? 41

6 CONCLUSION 49

REFERENCES 51

ANNEX: TECHNOLOGICAL DETAILS OF RFID A

The tag A

Active, Passive or Chipless tags A

Tag data C

The reader D

The middleware and information systems E

The technical means of interaction between tags and readers E

Overview of tables

Table 1 What is in an EPC number? 34

Table 2 Bit length to uniquely identify different type of objects 35

Table 3 EPCglobal Guidelines on EPC for Consumer Products 44

1 Introduction

In today's society individuals are exposed to surveillance and tracking in numerous different ways. Cameras are located on street corners, in stores, in cash machines, on public transport and even in the workplace. Most of the time, the purpose of these cameras is to prevent crime: monitor shoplifters and thugs, prevent speeding or vandalism, and ensure identifiability of anyone breaching recognised set of rules. Mobile phones can easily be located via triangulation. A payment card leaves a trail every time it is used, slowly but surely collecting all the items purchased, revealing the holder's spending patterns. Store loyalty cards give detailed information about visit frequency and spending patterns. Phone conversations are recorded in the workplace for numerous reasons, and your web browsing is tracked both on your computer and through your search entries.

Imagine a system that combines most if not all these things adds location tracking and stores the data gathered in a central database accessible over the Internet to all who contribute to it. Imagine being tracked from the moment you wake up until you fall asleep again. Think of all the things you do in-between, whether highly private or casual, being available for scrutiny of an interested party on "the other side".

If we believe all the hype surrounding RFID that is how our life will be in a not so distant future. Because RFID technology makes real-time item tracking relatively easy and it does not differentiate between human beings, animals, or things – all that is required is vast amount of computer space and readers.

RFID stands for Radio Frequency Identification, a term that describes any system of identification wherein an electronic device that uses radio frequency to communicate, is attached to an item.[1] The device, sometimes carrying a globally unique serial number, interacts with readers in the vicinity and as the technology used is radio frequency, the

[1] B Glover and H Bhatt, *RFID Essentials* (Cambridge: O'Reilly, 2006), 1

device and the reader do not need “line of sight” to communicate. As further discussed in Chapter 2 and the Annex, the device can be both small and relatively inexpensive, which gives promise to an item-level RFID tagging in the near future.

In a 2005 ITU Internet Report, the International Telecommunication Union (hereafter also ITU) predicted “The Internet of Things”[2] where all domestic and industrial devices and appliances would be globally connected and equipped with readers enabled to communicate with RFID tags. These appliances would then be able to transmit the communication for example to vendors and manufacturers giving them the ability to react.[3]

RFID generated data can be compared with Internet click-stream data, and an RFID based Internet of Things is likely to result in similarly massive amount of data, with the difference that RFID generated data is connected with “real world” items. The RFID technology is likely to dramatically increase efficiency in most business processes, and convenience for many consumers. However there is a risk of diminishing privacy in the process. Users generally perceive RFID as not more than an electronic key or wallet, while the deployers of the system use it to register movements, spending, productivity, preferences, habits and so forth.[4]

With lack of security and low cost of the RFID technology, this new flood of data has the potential to fundamentally change the way we view privacy, leading to a world in which our physical location would never be safe from the prying eye of the government, companies, or a hacker. Because as RFID technology expands, it is likely to literally

---

[2] ITU Internet Report, *The Internet of Things*. (Geneva: ITU, 2005).

[3] *Supra* n2, 3.

[4] Christian van 't Hof, *RFID and Identity Management in Everyday Life: Striking the balance between convenience, choice and control*, a study commissioned by STOA under Framework Contract IP/A/STOA/FWC/2005-28 (2007), p.iii. Available at http://www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf.

surround future consumers wherever they go and whatever they do.[5] While RFID technology is only one of many technological devices that could be abused to violate consumers' privacy, this technology has three critical differences not found in other technologies that make it a highly likely candidate for the task: low price, passivity (not requiring external power source), and very small size.[6]

This new prospective future is likely to bring an enhanced requirement for identity management, where individuals would request options to control – at least to some extent – the amount of personal data other entities gather about them.
For this context, a definition of Identity Management from Christian van 't Hof[7] is adopted:

> In this context, Identity Management is understood as how a person, interacting with an information system, defines what is known and not known about him/her to others using the system and how this relates to the information known or not known to the persons maintaining the system. It goes beyond the juridical notion of protecting personal data and emphasises an active role for users determining their identity in the digital public space.

Discussing the legal aspects of Radio Frequency Identification is an interrelated discussion of privacy, security, radio spectrum, standards and governance.[8] With a restricted size, this thesis can only touch upon these different aspects, while looking in further detail on the privacy aspects related to a specific standard created within the range of RFID technology – the EPCglobal Standard for item-level RFID tagging. As this standard is still in its infancy and little distribution has yet taken off, outside the pilot projects, the future scenario of usage will be based on plans, hypothetical examples, and visions put forward by industry stakeholders. The hypothetical examples and visions these stakeholders have put forward trigger certain privacy related

---

[5] O Kobelev, "Big Brother on a Tiny Chip: Ushering in the Age of Global Surveillance Through the Use of Radio Frequency Identification Technology and the Need for Legislative Response." *North Carolina Journal of Law & Technology*. Spring, 2005, (6 N.C. J.L. & Tech), 330-331.

[6] *Id.*

[7] *Supra* n4, 5.

[8] European Commission, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*. SEC(2007) 312. COM(2007)96 final. A communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Available at: http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf.

questions: What is personal data and when is the tag data considered to be personal data? How well does the current EU legislation address the privacy threats of this US developed technology? In addition what needs to be done to have the technology adopted? Is certain legal action required now or should we wait for further development of the technology? To what extent are those deploying tags, accountable? Who controls the data on the tag? What control does the consumer have, in particular after purchase? These are only few of the questions that any discussion about the legal aspects of RFID triggers, some might be outside the scope of this thesis, but answering most, if not all, of them is the goal.

Breach of the privacy of the individual is different between industry sectors and application domains. Thus, one of the challenges for any debate on RFID deployment is differentiation between solutions for these industry sectors and application domains. The problem this thesis aims to solve is whether regional deployment of the EPCglobal Standard for RFID systems in Europe is possible given current European data protection legislation and if not, what needs to change, either in the EPCglobal Standard, including its privacy policy, or in the legislation, in order for it to be possible.

1.1 Research material, definitions and thesis structure

There has been large amount of papers, studies, and books written about RFID in the past 5 years, and the websites touching on the technology are copious as well. When selecting what to use as a foundation for this thesis, the aim was to find different point of views as well as prominent papers and books in the field. Documents from the European Union and its institutions and working groups are a certain foundation for the legal discussion, but other sources have been used as well – in particular when looking for a different interpretation than that of EU or its institutions and working groups.

When looking at the specific material focused on the EPCglobal Standard and related networks and information systems, it is necessary to explore documentation from industry stakeholders whose focus is on efficiency with emphasis on the business case and deployment, rather than the effect it has on individuals at the receiving end. To balance that and because the industry stakeholders are (perhaps overly) lenient towards the business processes, it is important to explore literature (perhaps overly) lenient

towards protection of the privacy of individuals. One of the privacy advocate sources is *Spychips* by Katherine Albrecht and Liz McIntyre,[9] which can be described as a highly loaded and biased "doomsday prediction" based on item-level tagging deployment. Another source perhaps biased as well, refers to *Spychips* as "a poorly researched, fear-mongering diatribe against RFID".[10] When evaluating the information provided by stakeholders and privacy advocates, utmost attempt has been made to remain neutral by looking at both sides and attempting to find the golden middle ground.

This thesis puts forward a few phrases that the average reader might be unfamiliar with which requires them to be clarified – to be defined for their intended purpose. The components of the RFID system, the *tag*, the *reader*, the *middleware*, and the *information system*, will be defined in Chapter 2.2, where better explanation of their function will take place.

Information management has already been defined as how a person, interacting with an information system, defines what is known and not known about them to others using the system, and how this relates to the information known or not known to the persons maintaining the system.[11] There is further exploration of the defining parts of *personal data* in Chapter 3.4.1, but the definition in the European Union's data protection directive[12] (hereafter also DPD) is the point of departure.[13] In it, the definition of personal data is any information relating to an identified or identifiable natural person with the additional definition of an *identifiable person* as one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or

---

[9] K Albrecht and L McIntyre, *Spychips: How major corporations and government plan to track your every move with RFID* (Nashville: Nelson Current, 2005).

[10] D Brown, *infra* n16, 398. In all fairness, one of the editors of the other main technical source for this thesis, Simson Garfinkel (*infra* n16, xxxix) describes Katherine Albrecht as one of the leading activists fighting RFID. Simson says that "her amazing ability to find the industry's missteps and then heavily publicise them has earned her a reputation for truth and accuracy that her opponents have tried hard to discredit but have failed."

[11] *Supra* n7.

[12] See chapter 3.2.

[13] Article 2(a).

more factors specific to his physical, physiological, mental, economic, cultural or social identity. The DPD uses the phrase data *controllers* for the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.[14] When it comes to RFID systems, those setting them up, defining needs (including needs for data) and making decisions are named *deployers*. Deployers are the data controllers in the RFID system. Both phrases will be used throughout the thesis.

The *Electronic Product Code* (EPC) is a specialised globally unique serial number that has been developed to take over from the barcode in identifying (consumer) products. Unlike the barcode, which identifies the type of product, the EPC uniquely identifies each item within the type. The EPC is developed by the EPCglobal aiming to make this the universal standard for all products, particularly consumer products. When discussing the ability of different types of tags[15] to communicate without line of sight, the word *susceptible* or *susceptibility* is often used to describe how sensitive the radio waves are when it comes to penetration through different types of matter. The radio waves are more susceptible to metal penetration than e.g. the penetration of fabric.

Finally, looking at the structure, the thesis starts by defining and describing the RFID technology in Chapter 2 before moving on to the core aspects of privacy and how the RFID technology increases collection of personal data in Chapter 3. There most effort will be put on current regulatory instruments, definition of personal data, and identifiability, as well as the difference between regulatory effects when personal information is stored on an RFID tag and when it becomes personal data by linking tag data to personally identifiable information stored elsewhere. Chapter 4 introduces the emerging global standard of EPCglobal Inc. and the upcoming EPCglobal Network that plans on storing and sharing relevant information for a globally unique numbering system applied in the consumer market. In Chapter 5 the need for changes to this global standard in order for it to comply with European privacy regulation, will be explored, before concluding remarks of the thesis in Chapter 6.

---

[14] Article 2(d).

[15] See further chapter 2.2.

2 The technology[16]

2.1 The Internet of Things

In its 2005 Internet Report,[17] ITU speculates about the Internet users of the future. There it says that if humans will be the only Internet users, the current total user base might double, but is unlikely to go beyond two billion active users in the near future. If "things" however become active Internet users on behalf of humans, the number of active connections could be measured in terms of tens or hundreds of billions.[18] This ambitious prediction of the ITU would be reached by connecting objects and things to communication networks creating a truly ubiquitous network – "anytime, anywhere, by anyone and anything". In this context, consumer products might be tracked using tiny radio transmitters or tagged with embedded hyperlinks and sensors. Connectivity would take on an entirely new dimension, fridges would be able to communicate with grocery stores, laundry machines with clothing, implanted tags with medical equipment, and vehicles with stationary and moving objects.[19]

Such developments would make the merely static objects of today into newly dynamic things, embedding intelligence in our environment, and ITU predicts it would stimulate the creation of innovative products and entirely new services. Given that everything in our physical environment would have its own identity, the real world would be mapped in a virtual cyberspace.

---

[16] The technological portion of this chapter is partly a short version of Annex I of this paper, which explains the technological means of RFID systems in much greater details. As cited in n145 the main resources for building the technological annex are two books on this subject: D Brown: *RFID Implementation* (McGraw-Hill, 2007), and S Garfinkel and B Rosenberg (eds): *RFID: Applications, Security, and Privacy* (Addison Wesley, 2006). Other material will be further cited when referred to.

[17] *Supra* n2.

[18] *Id*, 1,3.

[19] *Id*, 3.

2.2 Components of an RFID system

RFID technology is relatively new on the commercial market. Although the technology dates back to 1948,[20] mass-market RFID applications have only been developed over the last decade.[21] An RFID system is a set of components that work together to capture, integrate, and utilize data and information. The main components in an RFID system are *tags* that are attached to or implemented into movable items; *readers* that are either movable or permanently situated and read the signals sent by tags; a *middleware* that connects to the reader; and *information systems* where the data is analysed. Usual settings of such a system means that several times per second, readers broadcast a signal, and all tags within range and on the same frequency, respond.[22] This process creates a list of all the tags in the read zone, identified by a serial number and sometimes carrying further information about the tagged item. The middleware is used to reduce the flood of raw data produced by the tags, by aggregating, sorting and filtering the information and creating meaningful data which is then acquired by the information systems. An RFID system's true benefit comes from successfully converting the raw data generated by the tags and readers into useful information[23] which will then support future strategic decisions by deployers.[24]

Tags can be passive, semi-passive or active, based on their power source and the way they are used, and can be read-only, read/write or read/write/re-write, depending on how their circuit is adjusted. Tags do not need a built-in power source, as they take the

---

[20] H Stockman, *Communication by Means of Reflected Power*, Proceedings of the IRE, (1948), 1196-1204, (via ITU's Internet Report, *supra* n2).

[21] *Supra* n2, 10.

[22] Active tags have the ability to either continuously broadcast a signal for readers to "catch" or wait for a signal from the reader to respond, cf. Annex.

[23] *Supra* n1, 2.

[24] For example, a retail store placing readers on the shelves to have accurate information about how many items of milk are left on the shelf. When quantity runs low the information system lets the store manager know that it is time to refill the shelf. This would mean that it would be less likely for the shelf to be empty and an employee of the store does not need to check the shelf quantity regularly, thus leading to better efficiency in running the store.

energy they need from the electro-magnetic field sent out by readers.[25] Tags range and ability to transmit data is dependant on energy level and passive tags require stronger signals from the reader than active tags, to be able to respond as they are without internal power source.

Read range of tags differs depending on the frequency, technology and the standards used. Generally speaking, there is a correlation between frequency and read range and technology and standards can influence the read range even further. For example, the Icelandic ePassport[26] is tuned into 13.56MHz frequency which generally would mean a read range of 1 meter and good ability to penetrate through various opaque materials as the radio waves are 22 meters long.[27] According to the manufacturer of the equipment used, the read range is only 3cm due to adherence to an ISO standard with enhanced security settings.[28] It remains to be seen whether the security measures on the passport are strong enough to restrict unauthorized access by non-standard readers with longer read reach than the vendor-standard offers.[29]

2.3 Security

There are a few options when it comes to securing the tags. The ability and effort for securing the data is restricted *inter alia* by the power source of the tag and its complexity. The better the protection, the more power, or the bigger chip, is needed. That increases the cost of tag production, which restricts the interest of mass tag deployers to utilise such technology. Interest to deploy security-enhanced tags is

---

[25] *Supra* n2, 10.

[26] A biometric passport containing a digital photo and personal data belonging to the holder of the passport.

[27] See further discussion about frequency, wavelengths and read ranges in Annex I.

[28] Integrated Engineering is the device manufacturer for the Icelandic passports and technological information was acquired from their website, see in particular Product sheet for the e-Document Reader used to read ePassports: http://www.ieprox.com/files/Datasheets%20feb.%202007/e-Document%20Reader%20.pdf. The ISO Standard in question is ISO 14443, Proximity Card, which is designed to limit read range to a few centimetres.

[29] For further discussion about the security of ePassports see A Juels, D Molnar and D Wagner, *Security and Privacy Issues in E-Passports*, IEEE SecureComm 2005, available at: http://www.cs.berkeley.edu/~dmolnar/papers/RFID-passports.pdf.

therefore limited as is clearly depicted in the latest version of the EPCglobal Standard,[30] the EPC Gen-2, which uses passwords only to limit activation of a *kill* command, which permanently shuts down a tag, or to relock a tag's memory, e.g. to re-write data to it.

RFID tags that contain personal data must have embedded technical measures to comply with European regulation.[31] Without technical measures that restrict unauthorised disclosure of the tag data, anyone with a reader could query the tag and acquire the tag data. Technical means used could e.g. be encryption of the data, authentication of the reader, or a restriction to the communication with the tag. For enhanced security which might be needed to protect the tag data, deployers should aim at using standard protocols and algorithms.[32]

When it comes to physical manipulation of the equipment, "standard rates apply." As with any other information systems, the middleware and the RFID linked information systems are prone to hacking. It is therefore necessary to take the same precautions with this equipment. In addition, a Dutch research team has successfully implanted a virus on an RFID tag,[33] presenting the danger of the tag exploiting vulnerability in the middleware, and possibly infecting the data.

2.4 Privacy

An RFID system offers certain possibilities to limit invasion into people's personal space. As item-level tagging might sometimes be outside the scope of EU data protection and privacy legislation, when there is no direct processing of personal data, it is important to ensure that these possibilities are accessible and in use, where applicable. A mandatory feature enabling to kill the RFID tag might be one of such options.[34] Restricted access to and cross-reference of the collected data is another. For

---

[30] See further discussion about the EPCglobal standard and the EPC tag in Chapter 4.

[31] Art 17 of the data protection directive, see further discussion in Chapter 3.

[32] E.g. ISO/IEC 9798 authentication protocol and RSA or ECC encryption algorithms. See *infra* n50, 17.

[33] B Crispo, MR Rieback and AS Tanenbaum, *Is Your Cat Infected with a Computer Virus?* IEEE PerCom 2006, available at http://www.rfidvirus.org/papers/percom.06.pdf.

[34] European Commission, *The RFID Revolution: Your voice on the Challenges, Opportunities and Threats*. Results of the public online consultation on future radio frequency identification technology

example, it has been suggested to keep data from RFID tags separate from consumers' personal information.[35] Physically, all it takes is a simple layer of aluminium foil to shield most low power RFID devices. The effects such actions would have will be further discussed in chapter 3, as this might clearly affect a person's ability to not be discriminated against, for opting out of using the technology.

It has been widely discussed that users should have the ability to control when, where and to what extent tag data is read and collected by data controllers. Of course, this is not always possible, given the nature of some of the tag deployment.[36] The use of Privacy Enhanced Technologies (PETs)[37] comes to mind as an answer to the data processing problem the RFID system might pose, but PETs put the burden of protection on the individual, to learn how to protect himself. Education of consumers on the pros and cons of RFID systems is clearly an important reach, as informed consumers could play an important role in enhancing fair information practices. The DPD requires that data subjects be given the possibility to opt out of previously given consent for data collection.[38] There are however a few options to give the user control over the tag usage.

It is a matter to be further explored what effect ownership of the tag has on its manipulation. If a clause in a contract for delivery of e.g. RFID enabled Access Card, says that the card is a property of the provider and not the holder, could the provider then prevent the holder from restricting access to the card at any or all times?

---

policy. SEC (2007) 312. COM (2007) zzz final. (Brussels: 2007), 5. Available at http://ec.europa.eu/information_society/policy/rfid/doc/rfidswp_en.pdf.

[35] California state senator Debra Bowen introduced a bill to that effect. See *Big Brother at the supermarket till*, 27 January 2005. Available at: http://news.bbc.co.uk/2/hi/business/4211591.stm. As to the fate of the bill see http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_1801-1850/sb_1834_bill_20041201_status.html.

[36] For example when it comes to emergency tag with vital hospital information while a patient is admitted or an ePassport with biometric information required by law.

[37] On the subject of PETs see e.g. European Commission: *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, 2 May 2007, COM/2007/0228 final.

[38] See further discussion in Chapter 3.

Sometimes the tag can be removed from the item it was previously attached to, as is the case when the tag is put on a price label of a piece of clothing. Other times the tag can be destroyed, either physically by i.e. "frying" it in a microwave, or digitally by issuing a kill command that is intended to disable access to tag data.[39] Revisiting the Access card scenario, the question arises whether a declaration of ownership by the provider would restrict the holder's permission to kill the card. What if the card is an ID card and the requirement is to have it "visible" at all times? Some sources[40] even question whether individuals should accept transference of control of the tag from the provider as that might release the provider from certain security obligations.[41]

Another angle of the deactivation of tags is when purchasing a consumer product with a return policy. What would happen to the return policy if the tag would be deactivated at sale? Does that render the return of the item impossible as the tag could not be activated again and the product thus not sold again, or, if the tag could be reactivated[42] is that suffice protection of privacy as de- and reactivation can take place without line of sight. What would stop the retailer, or anyone else with malice intent, from reactivating the product the next time it entered the premises? Similar problem arises with regard to warranty of items. Could a retail store require the tag to be kept alive for the period of a warranty? As will be further explained in chapter 3, that is not the case, but the question is whether the regulation suffices to uphold the individual's right. If the individual insists on deactivation without the ability to reactivate, would the retailer perhaps reject the sale?

---

[39] The authors of *Spychips* (*supra* n9) visited Metro Future Store, an experimental project in Germany, where they purchased certain products and put them through a deactivation process offered by the store before leaving. The authors claim to have later discovered that the serial number on the tag could still be read from up to five feet away. Cf. K Albrecht: *Spychips*, *supra* n9, 72.

[40] S Garfinkel *supra* n16.

[41] *Id*, 77.

[42] This is e.g. the case if it was deactivated on the software level. Software deactivation is not available in the EPCglobal Standard, see further Chapter 4.

2.5 Conclusion of technology discussion

RFID systems can be used for all sort of purpose and naming all would require a complete book. Christian van 't Hof's report[43] on RFID and Identity Management in everyday life outlines 24 interesting examples of real life usage of this technology. Even though I do not agree with all assumptions made in that report, I think it is a good read to get familiar with what has already been done with the RFID technology and what privacy incidents have already risen and possibly addressed.

For tags to threaten the privacy of an individual it must be readable, uniquely identifiable, and able to be read surreptitiously, which brings us to privacy discussion in next chapter.

[43] *Supra n*4.

"One California company has developed a soap dispenser capable of reading employee tags to let restaurant managers know whether their workers washed their hands while in the bathroom."

Jonathan Krim, Washington Post.[44]

[44] Jonathan Krim. *Embedding their hopes in RFID – Tagging technology promises efficiency but raises privacy issues*. Washington Post, June 23, 2004.

3 Privacy

3.1 Introduction

Privacy is a fundamental right of the individual, often classified as part of human rights.[45] On European level, it can be derived from Art 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.[46] Art 8 gives "[e]veryone … the right to respect for his private and family life, his home and his correspondence." Europe has been building a set of privacy rules for more than 50 years while at the same time, technology has advanced and threatened to tear it down again. For the first decades, the threat appeared to be the possibility of Orwellian *Big Brother* states, as governments would gather detailed personal information and use it against their citizens. Nevertheless over the last 25 years the combination of several key political, commercial and technological issues has resulted in the increase of private enterprises beyond national governments as the largest potential threat to the privacy of the individual.[47] This is mainly because private enterprises are better at data processing: they have more motivation to push the envelope of acceptable personal data use; they are subject to limited public control; and they have benefited from the free market and deregulation ethos in recent years.[48] The commercialisation of RFID, with its cheap and efficient tracking mechanisms, increased accuracy, and its ubiquity in the marketplace, has the ability to magnify even further the threat to privacy of individuals.[49]

---

[45] See e.g. C Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, (Oxford: Oxford University Press, 2007, 2nd ed), 18.[46] ETS no 5; opened for signature 4.11.1950; in force 3.9.1953 – hereafter also *European Convention of Human Rights* (ECHR).

[47] A Charlesworth, "Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual" in Edwards & Waelde (eds): *Law & the Internet: a framework for electronic commerce*. [79]-122. Oxford 2000, 80-81.

[48] *Id*.

[49] *Supra* n5, 339.

3.2 *De lege lata*

It is crucial that any implementation of an RFID system is in compliance with existing data protection and privacy legislation and guidelines. The main regulatory instrument on privacy in the European Union is Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter the data protection directive or DPD), where the collection of data is limited only if it contains personal data. Generally speaking, the data protection directive applies to the processing of all personal data.[50] This means that any processing, whether by automatic means or not, that is made to form (a part of) a filing system, is restricted should it contain processing of personal data.[51] Whether this means that, the directive applies to the data collected through RFID technology depends on the RFID application in question, particularly whether that application entails the processing of personal data as defined by the directive.[52] When assessing whether the collection of personal data is covered by the DPD, it is important to determine both the extent to which the data processed *relates* to an individual and whether such data concerns an individual who is *identifiable* or *identified*.[53] Discussion on the identifiability will be continued in 3.4.1.

Article 29 Data Protection Working Party (hereafter the Working Party) has put forward a definition providing that data "relates to an individual if it refers to the *identity*, *characteristics* or *behaviour* of an individual or if such information is used to determine or influence the way *in which that person is treated or evaluated*"[54] (emphasis mine). Additionally, the Working Party states in the same document that even "if the

---

[50] Article 29 Data Protection Working Party: *Working document on data protection issues related to RFID technology*, WP 105, January 19, 2005, 8, hereafter referred to as WP105 and available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf. In accordance with Art 3(2), the directive does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law or by a natural person in the course of a purely personal or household activity.

[51] Art 3 of the directive.

[52] Art 2(a) of the directive, cf. Chapter 3.4.1.

[53] *Supra* n50, 8.

[54] *Id*.

individual is not immediately and directly identified at the item information level, he can be identified at an associative level because of the possibility of identifying him without difficulty via the large mass of information surrounding him or stored about him."[55] This would leave it highly likely, in the Working Party's opinion that a uniquely identified tag, e.g. EPC tag, born by an individual would be considered to store personal data and all collection of that tag's data would fall under the scope of the data protection directive. Not everyone agrees with this opinion of the Working Party and in a public consultation on *WP105*, concerns were raised whether the Working Party paper was based on an overstretched definition of personal data, which would go beyond the definition contained in the DPD.[56] In June 2007 the Working Party issued an opinion on the concept of personal data,[57] where it was further defined what could make data personal. There the Working Party stresses that it is not necessary that the data *focuses* on someone in order to be considered to relate to him. After explaining the three elements (content, purpose, result) that must be considered as alternative conditions, the Working Party provided this explanatory example:

> The same information may relate to individual Titius because of the "content" element (the data is clearly about Titius), AND to Gaius because of the "purpose" element (it will be used in order to treat Gaius in a certain way) AND to Sempronius because of the "result" element (it is likely to have an impact on the rights and interests of Sempronius).[58]

It still remains to be determined on each application basis, whether the information the deployer plans to process would be considered personal data.

3.2.1 Guidelines for RFID deployers and data controllers[59]

The framework for any data processing is set out in Recital 2 of the data protection directive. It says, "data-processing systems are designed to serve man; … they must,

---

[55] *Id*, 7.

[56] Article 29 Data Protection Working Party: *Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology*, WP 111, 28 September 2005, 3, hereafter referred to as WP111 and available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf.

[57] *Infra* n81.

[58] *Id*, 11-12.

[59] This section (and its subsections) is heavily based on WP105 (*supra* n50) pages 9-17. Other material cited when used.

whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy".

In *WP105* general guidelines are put forward which application deployers and data controllers should use and adapt when designing the application, the device, and preparing their data processing. These guidelines are based on the principles and articles of the DPD and will be used to identify the regulatory requirements that RFID system deployers are forced to consider. It is beyond the scope of this thesis to explain the guidelines in detail but it is equally important to discuss the legal state, as that is the basis of the comparison in chapter 5. The guidelines are two-fold; first, the Working Party introduces guidelines regarding the data and its processing, and then also guidelines regarding technical requirements to the equipment.

3.2.1.1 Working Party guidelines on the compliance of the data protection requirements

The data processing guidelines first list the data protection principles[60] related to data quality which the data controller must comply with: The *use limitation principle (purpose principle)*,[61] the *data quality principle*,[62] and the *conservation principle*.[63] Secondly the guidelines discuss legal grounds for processing pursuant to Art 7 of DPD.

---

[60] For a discussion on core principles of data protection laws in general see e.g. L Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, (The Hague: Kluwer Law International, 2002), Chapter 3, 57-69.

[61] In L Bygrave (*id*, 61) this principle is called *purpose specification principle* and reads "that personal data [should] be collected for specified, lawful and/or legitimate purposes and *not subsequently processed in ways that are incompatible with those purposes*" (emphasis mine). This principle is partially embodied in Art 6(1)(b) of the data protection directive.

[62] Looking at L Bygrave again (*id*, 62) this principle requires personal data to be "valid with respect to what they are intended to describe, and *relevant and complete* with respect to the purposes for which they are intended to be processed" (emphasis mine). This means that any irrelevant data must not be collected and, if collected, must be discarded. This principle, which can be found in Art 6(1)(c) of the data protection directive, also requires data to be accurate and kept up-to date.

[63] In L Bygrave (*id*, 60) this is part of the *minimality principle*, requiring that "personal data [is] erased or anonymised once they are no longer required for the purposes for which they have been kept." This principle can be found in Art 6(1)(e) of the data protection directive.

According to the article, data may only be processed if such processing can be based on one of the grounds for legitimate data processing listed in Art 7. The guidelines state that "[u]nder most of the scenarios where RFID technology is used, consent from individuals [would] be the only legal ground available to data controllers to legitimise the collection of information through RFID."[64] Such consent must be freely given, specific, informed, and an indication of the individual's effective will.[65] The guidelines then address how data controllers must provide the data subjects with certain minimal information pursuant to Art 10 of DPD: the identity of the controller, the purposes of the processing, information on the recipients of the data, and the existence of a right of access. As an example a retail store, using EPC tags on every item in the store, would according to the guidelines, have to provide all store visitors with information about the presence of the EPC tags and the accompanying readers as well as the consequences of their presence. Such as what information is gathered, by whom, and how it would be used; how to disable the tags and how to gain information about data collected. The information is to be provided to the data subject in a clear and comprehensible manner.[66] A further discussion about the effect of store readers reading tags on individuals acquired from different retailers will be put forward in chapter 5.

Lastly, the guidelines address data subject's right of access and security related obligations. Right of access in Art 12 of DPD gives data subjects the possibility of checking the accuracy of the data and ensuring the data are kept up to date. For example, when an RFID tag contains personal information (i.e. ePassports and ID cards) individuals should be entitled to know the information contained in the tag and to make corrections using means easily accessible. Still adding to the Access card scenario, an Access card holder could request various information from the data collector: a printout explaining what is on the card; an overview of all the records of entries and exits from working premises; a list of all records that have been shared with third parties; and a procedural and technical documentation that would explain to the

[64] *Supra* n50, 10.

[65] Art 2(h) DPD.

[66] Cf. the principle of fair processing and Art 6(1)(a) of the data protection directive.

cardholder which readers in the wider population might be capable of reading all or parts of their card.[67]

Art 17 of DPD imposes an obligation upon data controllers to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or unauthorised disclosure. The measures can be organisational or technical. This requirement is further discussed in next chapter.

3.2.1.2 Working Party guidelines on technical and organisational requirements to ensure the adequate implementation of data protection principles

When it comes to technical and organisational requirements, the Working Party considers that technology might play a key role in ensuring compliance with the data protection principles in the context of processing personal data collected through RFID technology. The Working Party also considers that the design of RFID tags, RFID readers as well as RFID applications driven by standardization initiatives might have great impact in minimising the collection and use of personal data and also in preventing any unlawful forms of processing by making it technically impossible for unauthorised persons to access personal data.[68] Additionally the Working Party considers manufacturers of the technology and standardisation bodies to be responsible for ensuring that privacy compliant technology is available for deployers. It calls for development of mechanisms in order to ensure that such standards are followed in practical applications.

When it comes to interoperability of RFID systems, the guidelines identify its double edge, as the interoperability of RFID systems is positive from a business perspective. While "[f]rom a data protection perspective, whereas interoperability may increase the technical quality of the data and contribute to compliance with Art 6(1) (d) of the [data protection] Directive, RFID interoperability may at the same time have some negative side effects for data protection unless appropriate measures are taken."[69] As an

---

[67] S Garfinkel *supra* n16, 79.

[68] *Supra* n50, 12.

[69] *Id*, 13.

example, the guidelines mention that it might be more difficult to apply and to control the principle of purpose limitation and that management of access rights regarding privacy might become more critical with increased numbers of actors manipulating the data.

The way an RFID application is built may have a great impact on ensuring the effective implementation of access, rectification and deletion rights. For that reason, the guidelines suggest development of a pictogram standard and other standard means to more easily inform individuals of the presence, visibility and activability of RFID technology. The guidelines also discuss in detail the technical and organisational measures for exercising access, rectification and deletion rights as recognised by Art 12 of DPD. Opting out of using the technology should always be a possibility for individuals and the guidelines stress that individuals selecting deactivation or removal of a tag should not be penalised in any way for that.

For many applications, the tag itself contains only an ID whose semantics can only be accessed through a complete IT application environment. The EPC system discussed in chapter 4 is one of those RFID applications while ePassports is an example of a system, which does contain semantic information on the tag itself. Acquiring access to tag data information can therefore be a complicated process. Rectification requires a reader working with the tag protocol and an interactive IT system providing the individual with information about the content read as well as what modifications has been made to the content. Interactivity should be required in order for the individual to be able to correct processed data.

Permission to delete the tag data depends on the legal grounds that legitimize the processing of personal data. It is highly unlikely, if at all possible, that an individual would be allowed to delete the content on the tag in his ePassport, while deleting the content of a tag attached to the jeans he buys should always be available at or after purchase. Disabling the function of the tag without deleting its content is another option to consider, in particular in context with the individuals option to manage the information gathered around him. Several solutions have been proposed as to how to disable access to tag data, both permanent solutions and temporary ones. The most

popular one is an introduction of a kill command that would deactivate the tag either permanently or temporarily. A permanent solution would destroy the tag while a temporary deactivation could be done mechanically or by applying a software lock. Two problems arise with the use of a kill command: the advantage of re-using RFID capability after deactivation is lost, and the security of the software lock is likely to be low, in particular in cheap, mass-produced EPC tags, causing different type of privacy concerns. Another popular solution is a Faraday cage,[70] where the tag would be physically shielded from contact. Purses with shields can be used to prevent detection of tagged banknotes, aluminium sheets incorporated into ePassport covers could suffice for content protection while the ePassport is closed. Shielding of that type is not applicable to all applications of RFID technology, particularly not to the consumer industry. Shielding the jeans and shoes a person is wearing is a bit more difficult than shielding the passport in their pocket. The use of labelling, killing, and Faraday cages does not address the biggest problem facing individual privacy when it comes to RFID deployment: consumers are likely to want live, readable RFID tags for the benefits and convenience it will bring to them.

Remembering that consent is the most common legal ground available to data controllers highlights even further the requirement for availability of tag disablers as individuals can always withdraw their consent to the processing of personal data. A lack of a device to disable the tag prevents the individual from exercising this right.

The last topic of the Working Party guidelines is data security. As discussed earlier, unrestricted use of RFID tags triggers a potential privacy threat greater than the much-feared "sneak-and-peak" provisions of the USA PATRIOT Act and has been predicted by MIT[71] researchers to become the most pervasive computer technology in history.[72] Tags containing personal data must have embedded technical measures to prevent unauthorised disclosure of the data, according to Art 17 of DPD. This is to ensure that

---

[70] See e.g. http://en.wikipedia.org/wiki/Faraday_cage for information about Faraday cages.

[71] Massachusetts Institute of Technology.

[72] *Supra* n5, 325-326. Kobelev's footnote cites *Sanjay E. Sarma et al., Radio Frequency Identification: Security Risks and Challenges, 6 RSA Laboratories Cryptobites 2 (2003)* as reference. Sanjay Sarma was one of the driving forces behind the Auto-ID Center at MIT which will be further discussed in Chapter 4.

only the intended data processor could query the tag for its information. Such measures are also necessary to ensure the integrity of the data stored on the tag, as required by Art 6(1)(d). When the tag itself does not contain personal data and the tag data can only be considered personal with a link to externally stored information, this becomes a vaguer requirement which deployers might attempt to bypass.[73]

3.2.2 EU Decisions regulating the radio spectrum

There are two European Community decisions regulating the radio spectrum. The framework decision is Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (in short the Radio Spectrum Decision).[74] The second one is a decision specifying further the use of the UHF[75] band: Commission Decision 2006/804/EC of 23 November 2006 on harmonisation of the radio spectrum for radio frequency identification (RFID) devices operating in the UHF band.[76] In short, what these decisions do is to harmonise the use of radio spectrum in the European Union and European Economic Area. The relevant portion of these decisions for this thesis is the annex to the UHF band decision put in force with Art 3(1) of that decision. There it is stated that the frequency bands for RFID devices running on UHF band frequency[77] in the European Union are 865-868 MHz divided into three sub-bands with different maximum power and field strengths. What this means is that the UHF band, the band that the EPCglobal's standard is utilizing, is running on a different frequency range in the European Union than the rest of the world, apart from New Zealand and India.[78] As one of the first tasks of defining tags is deciding which frequency it will run on, this generally means that tags manufactured to function in the United States are not using

---

[73] In WP111 (*supra* n56, 3) the Working Party cites this as a very controversial issue. That consumers and think tanks/universities are prone to believing that processing of EPCglobal standardised tags would most of the time entail a processing of personal data, while most industry stakeholders consider that it will not.

[74] Official Journal L 108, 24/04/2002 P. 0001 – 0006.

[75] Ultra high frequency.

[76] Official Journal L 329, 25/11/2006 P. 0064 – 0066.

[77] See Annex for further explanation regarding the difference of frequencies.

[78] See D Brown *supra* n16, 11 for overview of the UHF frequency allocations in selected regions of the world: e.g. North America (902-928 MHz), Singapore (923-925 MHz), Australia (918-926 MHz), New Zealand (864-929 MHz) and India (865-867 MHz).

the correct frequency for Europe. This could be particularly troublesome as the EPCglobal's standard readers are designed to read the whole range (860-960 MHz). Using those readers in the European Union could thus violate against the Radio Spectrum decision and the UHF band decision mentioned above, depending on the frequency the responding tag has been tuned to.

3.3 De lege ferenda

There have been different opinions aired when it comes to the discussion of whether the data protection directive suffices as a protection for the privacy of individuals in the context of RFID systems. In *WP111*[79] lines were drawn between consumers and think tanks/universities, and industry stakeholders, where the former group tended to state that current legislation did not suffice and the latter disagreed. Consumers and some think tanks/universities applauded the initiative of the Working Party by introducing the working document and thought that a stronger regulation would be required to secure sufficient protection of personal data. Industry stakeholders disagreed with certain parts of the working document and questioned whether all examples and scenarios described therein would entail processing of personal data.[80] The difference between these two groups and their opinion on the matter of personal data clearly indicates a friction in interpretation that needs to be addressed. Recent work of the Working Party is a step along that way.[81]

There are other sources who also call for a better regulation of the technology.[82] The data protection directive does leave room for the use of code of conduct, but those calling for better regulation usually doubt that codes of conduct will suffice to protect the privacy of individuals. Another aspect of better regulation is the need for a region wide standard, preferably even global standard. As was mentioned in chapter 3.2.2,

---

[79] *Supra* n56.

[80] *Id*, 3.

[81] Article 29 Data Protection *Working Party, Opinion 4/2007 on the concept of personal data*, WP136, 20 June 2007, hereafter referred to as WP136 and available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[82] See e.g. *supra* n4.

Europe e.g. uses a different frequency range in the UHF band[83] than other regions meaning that products imported from other areas require different tags than they would, had they been sold locally.

Yet another aspect is better clarification on key terms in the data protection directive. While the Working party recently put forward an important document on defining personal data,[84] there is still lacking a clear and concise clarification as to what constitutes *consent* and *legitimate interest*. Not to mention that even with a better definition on personal data, deployers might still argue that tags containing only an EPC could never be construed as personal data, thus stripping them of a requirement to comply with the data protection directive.

It might be argued that with the advent of commercial use of RFID technology, a shift in aim of the data protection directive could be needed. While current principles and articles aim at restricting possible collection of data and minimising the collection of personal data, the *de facto* setting of any RFID system is a mass gathering of all data, which then needs to be filtered to become accessible. It would be rather difficult to eliminate a collection of data while using an RFID system with little or no technological security measures, in particular when considering that it will not become personal data until certain linking in the information system has taken place or is at least possible. In RFID, data collection is a rule rather than the exception.

It is put forward in the data protection principles and implemented in the data protection directive[85] that explicit consent is required before the data controller can utilise the previously processed data differently than for which it was collected. The question then becomes whether the punitive provisions in member states' legislation will suffice to prevent the data collector from manipulating a data set he has acquired on any given data subject. It is possible that stronger punitive provisions are required to secure the

[83] See further discussion about frequency range in the Annex.

[84] *Supra* n81.

[85] Article 6(1)(b) and 7(a).

right of the data subject in that matter. With the introduction of RFID and a possible explosion of data processed, this is an emerging problem to be addressed.

3.4 Personal data affected by RFID technology

The most problematic thing concerning RFID and personal data is how to recognise whether the data on the tag should be considered personal or not. This is because when considering the processing of personal data with the RFID technology, one needs to focus more on the information systems than the tags themselves. The power of the technology lies in the (possibly globally) uniquely identifiable serial number each RFID tag manufactured can and often does contain. If security settings are too low, this unique ID number quickly becomes as connected to an individual's persona as a national identification number.[86] The privacy concerns will focus on the extent of linking of this serial number to personally identifiable profiles in information systems that might create behavioural profiles beyond what is necessity to confirm with the desired usage of the technology.

Even though most RFID tags do not carry personal data *per se*, the same cannot be said for the attached information systems. The data collected by the readers from RFID tags are usually of little use, until imported into the information system the collector uses. Take employee's access card for example. The card itself usually carries on it, an identifiable serial number that is assigned to the personal profile of the employee within the company's information system. Each time that employee opens a door with that access card; the action is recorded and registered into the same database as holds the personnel profile. Processing of location data in that context is a particularly sensitive matter as it is involving the key issue of the freedom to come and go anonymously.[87]

---

[86] E.g. the US Social Security Number or the Icelandic ID number.

[87] Article 29 Data Protection Working Party, *Working Party 29 Opinion on the use of location data with a view to providing value-added services*, WP115, November 2005, 3, hereafter referred to as WP115, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf.

3.4.1 The concept of personal data[88]

Art 2(a) of DPD defines personal data as any information relating to an identified or identifiable natural person. It also defines an identifiable person to be one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Data is therefore considered personal whether the collector can make the link or not[89] and is considered personally identifiable when a person can be distinguished from all other members of a group.[90] How detailed the identification needs to be, depends on the surroundings of the individual, the descriptive comments, and the size of the group. Indirect identification could also be based on many smaller titbits none precise enough to identify anyone, while combined will allow the individual to be distinguished from others.[91]

When assessing whether information concerns an identifiable person, it is important to apply recital 26 of DPD. Recital 26 limits the amount of time and money spent on analyzing the data before the data is considered to be personal or not. It says that when determining whether a person is identifiable, "account should be taken of all the means *likely reasonably* to be used either by the controller or by any other person to identify the said person." The Working Party has nevertheless expressed in *WP105* that given the computer memory and processing capacity of computers today, individual movements tracked by the use of RFID technology are, if not identified, identifiable.[92]

In any case, identifiability of a person will almost always depend on the data gathered in addition to event data[93] from the tag itself. The use of an RFID system in an amusement park, for example, might generate personal data and then it might not. There have been rumours that Legoland in Billund, Denmark provides parents with reusable

---

[88] For in-depth discussion on the definition of personal data see WP136, *supra* n81.

[89] As long as someone can make the link.

[90] *Supra* n81, 12.

[91] *Id*, 13.

[92] *Supra* n50, 8.

[93] Each record of registration by a reader from a tag is called an event.

RFID tags in order to find a lost child,[94] here a link is necessary between the child's profile and the tag's ID, for the effective recovery of the child. This would render the tag data personal while the tag was attached to the child, but dependant on the storage of the data; it is possible that as soon as the tag has been returned, the data would become impersonal.

3.4.2 Personal data stored on the RFID tag

Regardless of the discussion above, there are known cases where personal information is stored on the tag itself. The best known usage for RFID tags that include personal data are ePassports.[95] The tag embedded in the passport stores a digitized photograph, name, gender, date of birth and nationality of the passport holder as well as the passport number and the passport expiry date.[96] In the future, there are plans to have the ePassport carry a digitized version of ones fingerprint or other biometrics data. Another example of RFID tags including personal data is some implementations of transport ticketing.[97]

3.4.3 Personal data linkable to tag

It has been briefly touched upon before that the most common type of collection and processing of personal data in RFID systems is when tag data is linked to personal information in a database. This is much vaguer category than the one where personal data is placed on the tag itself, as here the debate will always be whether the link between the tag data and the personal data is sufficient enough to render the tag data as personal as defined by the data protection directive.

---

[94] *Supra* n4,15. This source speculates whether Legoland also uses the device to track movement of people through the park.

[95] The Australian Department of Foreign Affairs and Trade, *The Australian ePassport*, available at http://www.dfat.gov.au/dept/passports/. The International Civil Aviation Organization (ICAO) a body run by the United Nations have issued guidelines for Machine Readable Travel Documents. Document 9303. See further http://mrtd.icao.int/content/view/33/202/. See also discussion on the Icelandic ePassport in chapter 2.2.

[96] *Id*.

[97] See e.g. an example of a Dutch implementation of travelling documents with identifiable RFID tags in *supra* n4.

WP105, the Working Party's working document on RFID, lists two scenarios possible under this category, all a part of the retail sector. The first one arises when the tag data is linked to the record of the customer who bought it, for e.g. guarantee purposes. The second one is a case where supermarket tags loyalty cards or similar devices which identify individuals by their names to learn and record consumer habits while consumers are in the store. In both examples above, the privacy implications are obvious. The technology strengthens existing ability of learning consumer habits, but also increases the potential for direct marketing, as individuals could be recognised on entering a store and their habits in store monitored.[98]

3.4.4 Targeting, tracking and/or profiling

There are many different ways for targeting, tracking and profiling people in today's society. Introduction of RFID as a means for such methods is nothing new, but brings these abilities to the foreground as an affordable, feasible, and efficient way to enhance knowledge e.g. about consumer behaviour, in particular if linked with other means used today. A foreseeable scenario was set forward in an US patent application by IBM:

> Previous purchase records for each person who shops at a retail store are collected by [cash register systems] and stored in a transaction database. When a person carrying or wearing items having RFID tags enters the store or other designated area, a RFID tag scanner located therein scans the RFID tags on that person and reads the RFID tag information. The RFID tag information collected from the person is correlated with transaction records stored in the transaction database according to known correlation algorithms. Based on the results of the correlation, the exact identity of the person or certain characteristics about the person can be determined. This information is used to monitor the movement of the person through the store or other areas.[99]

Here, the IBM anticipates that retail stores would be interested in realising how different individuals behave while browsing through their store. The Working Party anticipated similar scenarios in *WP105*[100] and considered these scenarios to be likely to be processing of personal data. The Working party reaches even further with a scenario where an unidentified person carrying tagged items enters a store and is traced and profiled based on those items each time he enters the premises. It was this assumption

---

[98] *Supra* n50, 6.

[99] J R Hind: *Identification and tracking of persons using RFID-tagged items*. US patent application #20020165758. Filed 05/03/2001. Available at http://www.freepatentsonline.com/20020165758.html

[100] *Supra* n50, 6-7.

of the Working Party that raised the most disputes by industry stakeholders in *WP111* as discussed earlier, but the Working Party is not alone in this opinion. A similar scenario was drawn in van 't Hof's report where systems were foreseen registering movements, spending, preferences, and so forth, giving data collectors a means of providing feedback according to these identities and control over their data subjects.[101]

3.5 Conclusion of privacy discussion

The chapters before show that it is not the data that the RFID tags carry that are causing a worry; it is the linking that can be done and the profiles that can be created by analyzing all the records collected when a tag-carrying item is in the vicinity of a reader. This is why limited access to tags is vital for protection of the privacy of individuals in the foreseen future of RFID deployment in the consumer market.

As the example of the access card in the previous chapter indicated, the potential threat of the RFID technology to the privacy of individuals is there. Studies show that while RFID access cards are primarily used to open doors, companies are using the records collected in both a personally identifiable form (e.g. to understand the movements of an individual) and in aggregate form (e.g. to describe the behaviour of many individuals without identifying any of them). Personally identifiable use of collected records have included investigating allegations of work rule violations (e.g., misreporting time spent working) and monitoring former employees of an acquired company to ensure they adopted enterprise norms for work hours.[102]

---

[101] *Supra* n4, 6.

[102] RAND Corporation, Privacy in the Workplace, a research brief available at: http://www.rand.org/pubs/research_briefs/RB9107/index1.html.

"[T]he widespread use of RFID tags on merchandise such as clothing would make it possible for the locations of people, animals, and objects to be tracked on a global scale—a privacy invasion of Orwellian proportions."

IBM U.S. patent application 20020116274.[103]

[103] A quote from John R. Hind, *Method to Address Security and Privacy Issues of the Use of RFID Systems to Track Consumer Products*, U.S. patent application #20020116274, assigned to International Business Machines, filed 21 February 2001. (via K Albrecht: *Spychips*, supra n9 p37). Available at: http://www.freepatentsonline.com/20020116274.html. The patent application claims to limit these Orwellian proportions.

4 The Electronic Product Code and the EPCglobal Network[104]

The EPCglobal Network is a platform to enable identification, tracking and tracing of objects in global commerce. It is planned to have the capabilities to uniquely identify trillions of items and be able to record every significant change in location, status, or ownership. According to its developers, the network will make baggage tracking in airlines efficient and safe; pharmaceuticals and other products harder to counterfeit; food will be delivered fresher; airplanes will be safer; and automobiles will be repaired more efficiently. This network is intended to have a wide range of positive impacts on industry, commerce, and our personal lives.

The EPCglobal Network started as the Auto-ID Research Center at MIT, where the Uniform Code Council, Gillette and Procter & Gamble funded the first research for the successor technology to replace the barcode. The breakthrough idea was the combination of low-cost microchips and ubiquitous networks.[105] The chips would only need to store a globally unique serial number that would serve as a pointer to the data stored on servers accessible via the network. The Auto-ID Center created the original concepts for implementing an *Internet of Things* to parallel the *Internet of Information* we have now.

In four years, the Auto-ID Center outgrew its university roots, and its research became less theoretical and more applied, and commercial demands increased with over hundred corporate sponsors. Thus, it was decided to commercialise the project by

---

[104] The basis for this chapter comes from D Brown *supra* n16 and Verisign, *The EPCglobal Network: Enhancing the Supply Chain*, (2005), available at http://www.verisign.com/stellent/groups/public/documents/white_paper/002109.pdf. Other resources cited when used.

[105] One of the aims of the centre was to minimise cost of RFID tag production. That was done by stripping as much off the existing RFID tags as possible – including any encryption "because there was no memory to protect." S Sarma, "A history of the EPC" in S Garfinkel, *supra* n16, 44.

founding an organisation, EPCglobal,[106] to develop and administer standards for RFID technology.

EPCglobal has developed a standard for UHF tags named EPC, currently in its second generation.[107] The organisation claims that the standard opens the door for a number of manufacturers to make interoperable, compatible products quickly. EPCglobal envisions that collaborating businesses and industries will set up a network of EPC Information Services (EPCIS) servers[108] to provide an on-demand repository of information related to individual EPC numbers. Information made available by EPCIS servers could include e.g. the last observed location of an item carrying an EPC, as well as pricing information and product manuals.[109]

The EPCglobal Network is comprised of several different standards and specifications. The Electronic Product Code (EPC) data format, the air interface specification,[110] and Network Information Services that share data between different parts and different enterprises in the supply chain. The EPCglobal Network intends to leverage the existing Internet infrastructure to create a low-cost, standards-based set of services for trading partners to discover information associated with each EPC. It is made up of three main elements: the Object Naming Service (ONS), the EPC Information Services, and the EPC Discovery Service. Before completing the discussion on the EPCglobal Network, it is therefore practical to explore the different parts of it.

4.1 The Electronic Product Code

Similar to the barcode, the Electronic Product Code (EPC) is a standardised identification number structured to differentiate between products *and* product items.

---

[106] A joint venture between EAN International and the Uniform Code Council (which have now merged into GS1). EPCglobal's Board of Governors is composed of leading companies in the consumer market.

[107] Thus usually referred to as EPC UHF Gen-2.

[108] See further discussion on EPCIS in chapter 4.3.2.

[109] *Supra* n1, 45.

[110] The specification for frequency and other aspects of communication between the reader and the tag.

Unlike the barcode, the EPC number is large enough to uniquely identify all items produced on earth for a very long time.[111]

Table 1: What is in an EPC number?

	Header[112]	**Company prefix[113]**	**Item reference**	**Serial number**
SGTIN-96 (bits)	14 bits	40-20 bits[114]	4-24 bits	38 bits
Unique items:[115]	specifies which numbering scheme	1 trillion – 1 million	16-16 million	274 billion

In *Verisign*,[116] EPC numbers are said to be able to uniquely identify up to 268 million unique manufacturers, each with 16 million types of products and that each unique product could include up to 68 billion individual items, meaning the format could be used to identify hundreds of trillions of unique items.[117] The *Verisign* numbers do not add up to the SGTIN standard normally used for item tracking, but it might be based on some other numbering scheme. Regardless, this requires the EPC code to be at least 96 bit long and with it, each item of a product produced, can be uniquely identified. Each

---

[111] In *Spychips* K Albrecht and L McIntyre claim that the EPC system could uniquely identify all items produced on earth for the next thousand years – including human beings, see K Albrecht, *supra* n9, 26.

[112] 8 bits used to reference the numbering scheme and 6 bits for other specification based on the numbering scheme used, e.g. SGTIN (Standardised Global Trading Number) or SSCC, (Serial Shipping Container Code), SGTIN is inter alia used for item level tagging of consumer products. When using the SGTIN the 6 bits are split up: 3 bits for a filter value (which will be further discussed in chapter 5), and 3 bits for a partition value, which gives further detailed description of tag setup.

[113] The Company prefix and Item reference fields are SGTIN fields that combined are 44 bit long. Using other numbering schemes, these fields could be either split up differently or used as one.

[114] As the Company prefix can be from 20-40 bits long the Item reference will range between 4 and 24 bits. When the Company prefix is 40 bits, the Item reference is 4 bits. A small Company prefix leaves room for more unique item references.

[115] The calculations of unique items displayed in the numbering scheme are mine, based on the formula that *n* bits have the highest possible value of 2^n-1, thus e.g. 24 bits are equivalent to 2^{24}-1.

[116] *Supra*, n104.

[117] Different sources read for this thesis gave different indications as to how many items a 96-bit code would track. The numbers in the text come from the Verisign document (*supra* n104). D Brown (*supra* n16) refers to "several thousand trillion items" (32), while K Albrecht (*supra* n9) quotes an Auto-ID white paper for "80 thousand trillion trillion objects" (26).

six-pack of canned Coke would have seven EPC numbers – one for each can and one for the six-pack combined.[118] The structure of the EPC code enables most currently available numbering schemes to be built into it. This means that EPC compliant RFID readers could be useful across all but the most obscure application areas without forcing these industries to change their identification schemes.

Table 2: Bit length to uniquely identify different type of objects.[119]

Bits	**Unique number**	**Objects**
23	6.0×10^6 per annum	Automobiles
29	5.6×10^8 in use	Computers
33	6.0×10^9 total	Humans
34	2.0×10^{10} per annum	Razor blades
54	1.3×10^{16} per annum	Grains of rice

No information beyond the number itself is conveyed in the EPC and the standard does not allow any extra information to be stored on the RFID tag carrying the EPC. The information associated with an EPC, such as company name, product information, history, shipment date, expiration date, and so on, is meant to be accessible via specific EPC information systems (EPCIS)[120] only to authorized users, such as other members of a given supply chain. Without access to that secure information, the EPC is said to be meaningless, which again raises the question as to how restrict the access control can be, in a global commerce of intertwined suppliers and retailers.

4.2 EPC Middleware

The Middleware, also known as event manager, serves four functions in the EPCglobal Network. To resolve the EPC numbers into useful information by querying the ONS and accessing EPCIS;[121] to filter raw data into useful information by processing it so

---

[118] Although, canned products are the items least likely to be tagged today, as the susceptibility of the UHF radio waves towards the metal is very high. See further Annex.

[119] D Brock, *The electronic Product Code (EPC): A naming scheme for physical objects*, Auto-ID Center White Paper (via K Albrecht, *supra* n9, 26).

[120] See further section 4.3 below.

[121] See further section 4.3.1 below.

any application sees only relevant, significant events;[122] to manage a disparate group of readers through a common interface; and to transform data into usable formats and communicate it to the correct applications.

4.3 EPCglobal Network Information Services

The EPCglobal Network Information Services is a mechanism to acquire, secure and deliver real-time data about individual items as they move through the supply chain. It is conceived as the globally recognized and universally available mechanism to provide a pedigree of product identification and movements accessible to authorised users but secured behind firewalls, encoding and other security measures.

The EPC serves as a database lookup key that enables the server to locate and serve the information about the item. The database information itself is provided by the EPC Manager, the organisation responsible for the item, and possibly by others as the item makes its way through the supply chain. EPCglobal Network Information Services is divided functionally into three parts that each plays a unique role in enabling the secure discovery and sharing of detailed, real-time product information:

4.3.1 Object Naming Service (ONS)

Object Naming Service (ONS) is the authoritative directory of information sources available to describe EPCs in the supply chain. It is designed to be a central service to avoid fragmentation of information about EPCs. Similar to DNS,[123] ONS contains an entry for every registered EPC, and it has pointers to all of the recognised sources of information about that EPC. The root ONS is provided by EPCglobal and managed by Verisign, the company that manages the root DNS for the Internet. ONS may be implemented with a local cache for any company location. This local cache is used to reduce the need to query the global ONS for each object seen by a reader, since frequently sought or recently sought values can be stored locally. The local cache may also manage lookup of private internal EPCs for asset tracking.

[122] Where each record of a tag passing by a reader is considered an event.

[123] Domain Name System, the glue that holds the Internet together.

ONS points to two types of information: static information and dynamic information. Static information describes the item and gives its permanent characteristics (name, weight, source, maintenance instruction etc.). Dynamic information may be spread physically across several databases. It may describe, for instance, the date and time of its arrival at a given dock or warehouse. The dynamic information is posted by various organisations as they receive and distribute the item and sharing that dynamic information is what EPCglobal claims to be the efficiency factor of the system.

4.3.2 EPC Information Services (EPCIS)

EPC Information Services (EPCIS) are the set of data repositories that store information about unique item in the supply chain. The structure of EPCIS is distributed; different parts are controlled, owned and operated by different companies. EPCIS are hosted by different enterprises in the supply chain which are also the managers of access to the data. Each company is pursuing its own business model, and they are writing and reading data to and from EPCIS in a standardised way. EPCIS makes it easy to secure, find, and share information as needed. For example, it may give location information or the physical properties of an item, or it may describe the number of units in the lot or crate or pallet or dates of manufacture or expiration. The middleware, having acquired the EPC from the tag, queries the ONS to find the location of the right EPCIS servers for the information it needs. It then downloads the descriptive information from the servers.

4.3.3 EPC Discovery Services (EPCDS)

Discovery services is a chain-of-custody registration service, it tells the middleware where the relevant information is stored. The EPCDS provides a directory of all EPCIS servers that have read and contain dynamic information about a particular item. Although each of these three components is critical, according to EPCglobal the EPC Discovery Service is the most valuable component of all, enabling many applications of the enhanced product data set.

4.4 How the EPCglobal Networks Works

Looking at a process of the movement of one item tagged with an EPC tag throughout the supply chain would yield a result similar to the following:

- The item is tagged, the tag commissioned and then the tag's EPC is registered with the ONS. The tag remains with the product as it moves through the supply chain.
- The information associated with this particular item is added to the manufacturer's EPCIS.
- A pointer to this information is stored in the EPCDS.
- When the item is shipped, the shipment information is registered with the EPCIS.
- When the product is received at the next point in the supply chain, it is automatically read by acquiring the relevant information from the manufacturer's EPCIS via a lookup in the EPCDS. The item's arrival is registered in the distributor's EPCIS and a pointer to this information stored in the EPCDS.

As products make their way across multiple points throughout the supply chain, this process of products being scanned, and the knowledge of their data within EPC Information Services being passed on, repeats itself. The registration of this product knowledge by each EPC Information Service into the EPC Discovery Service enables full supply-chain visibility.

4.5 Conclusion of EPC discussion

The EPC standard is already being used for both retail chains and other sectors, but the EPC Network as such is still in its infancy and sharing information via EPCIS is not yet underway. Reports, that both the United States' Department of Defence[124] and Washington State's Department of Licensing[125] are utilising this standard for their asset management and other projects, have been seen by the RFID industry as an indicator that the EPC Standard will be the reigning standard for use of the UHF band.

Looking back at the reference that product information would only be accessible via secured network raised several questions. With a wide distribution of this standard

[124] See e.g. http://www.rfidjournal.com/article/articleview/1460/1/1/.

[125] See e.g. http://www.rfidjournal.com/article/articleview/3514/1/1/.

where possibly thousands of different manufacturers, suppliers and retailers share this distribution information, reference information to the static details of any product will be easily acquired. What more does anyone with interest to track or monitor an individual need? Do they even need that info? Considering what would be the most common lookup queries of any middleware filing recorded events, it would probably be what product is this? Is it in my stock? And, has it been sold? With a query like that, the middleware has possibly recorded the location of a person at any given time.

The EPCglobal Network has mainly been developed as an US based standard, although intention is to distribute it globally. The Working Party addresses this in *WP105*[126] where it says that EU concerns had been under-represented in the standardisation initiatives of EPCglobal. The Working Party derives this mainly from the fact that the participating stakeholders are most US based.[127] With such a widely distributed standard already, it is rather likely that this will become the RFID standard for consumer products, at least in the Western parts of the world. It is therefore important for the European Union to evaluate the standard and try to influence the changes required for the standard to be viable for use in the EU. These changes are the topic of next chapter.

[126] *Supra* n50

[127] *Id*, 13.

"You may need to read the following sentence twice: Aluminum foil hats will block the signals emitted by the radio tags that will replace bar-code labels on consumer goods.

That is, of course, if you place your tin-foil hat between the radio tag and the device trying to read its signal."

Mark Baard, Wired News, 18 November 2003.[128]

[128]M Baard, "Is RFID Technology Easy to Foil?" *Wired News*, 18 November 2003, available at http://www.wired.com/politics/security/news/2003/11/61264. (via S Garfinkel *supra* n16).

5 What needs to be done to ensure that the EPC standard is compliant with the data protection directive and other European Union regulation on RFID?

After having looked at basic information about the RFID technology as such, as well as looked at the specific characteristics of the EPC standard system, and touched upon the European legislation that governs the sphere, it is now time to see how the EPC standard fits into the European regulatory environment.

It is an ongoing mantra of the EPCglobal that the EPC tag does not carry personally identifiable information.[129] This is an assumption which EPCglobal is unable to support. When looking at an EPC tag in isolation, with no regard to the databases it might be linked or linkable to, that statement might be true, as the number-code on the tag relates to a product and not a purchaser. However, as has been depicted in chapter 3, this is not necessarily true when the EPC tag standard is used in the European market. This is because a serial number like that of the EPC tag can be considered personal data as defined by the data protection directive, if it is linked to an identified or identifiable person.[130] Any determination of such identifiable link needs to be done on an application by application basis. It is therefore necessary to look at what, if any, changes need to be done on both the EPCglobal's public policy and guidelines for consumer products, as well as the tag characteristics, to ensure compliance with European data protection regulation.

Addressing first the characteristics of the tag standard, it is designed to communicate on the frequency range between 860 MHz and 960 MHz, which does comply with the EC decision on that matter.[131] It is however clear that because the European Union does provide a different frequency range than the United States and many other regions, tags

[129] See e.g. http://www.epcglobalinc.org/public/ppsc_factsheets/epc_overview.

[130] See further discussion in chapter 3.

[131] See further chapter 3.2.2 where the content of the frequency decision is discussed.

need to be specially adapted for communication in the European Union for it to take place on a legitimate frequency. Additionally because frequency and range are determined before an antenna is selected (and thus the tag compiled) North-American manufacturers exporting to the European Union will need to use two different sets of EPC tags on their products, one for the home market and one for the European market. It is the opinion of this author that the European Union should consider revising the frequency range allocated to UHF RFID tags to allow for communication on the same frequency as the rest of the Western world.

As quoted in footnote 105 before, it was the belief of the developers of the EPC tag that there was nothing on the tag to protect. This resulted in removal of all encryption that was a "standard" in RFID tags before the development of the EPC tag. As a result, the EPC tag has no defences against communication from anyone, legitimate or not. The only protection the tag has is a password request that is required to kill or re-program the tag. This is in clear violation of Art 17 of DPD as portrayed in the requirements gathered by the Working Party in *WP105*[132] and discussed in chapter 3.2.1.2. There it says that technology might play a big role in ensuring compliance with the data protection principles, and that the design of the RFID tags, readers and other parts of an RFID system, might have great impact in minimising the collection and use of personal data. The Working Party considers manufacturers of the technology and standardisation bodies to be responsible for ensuring that privacy compliant technology is available for deployers.

The EPC, by design, does none of these things. The EPC is a simple RFID tag and the tendency of simple RFID tags to communicate their data indiscriminately is not an inherent characteristic of the technology, it is a choice of the designer. One could design the tags so that tag information remained inaccessible until the reader established a connection with it through a cryptographic handshake. That, however, would result in bigger and more complicated and thus more expensive tags. The business case for RFID in the retail supply chain depends on keeping the tags inexpensive – the dumber the tag, the cheaper it becomes to produce. As a result, there must be stricter requirements put

[132] *Supra* n50.

forth regarding the processing of data that is inevitable to be collected from the EPC tags. Owners and maintainers of readers need to ensure that the middleware filters through what the readers have picked up and only send through to the information system what they are scheduled to and not just all passing data. Mechanisms to limit collection could include screening out transmissions from non-targeted tags, and removing identifiers to render data impersonal.

Additionally the ability to kill EPC tags must be further developed and implemented. Based on information published on EPCglobal's website,[133] there are no means available to disable the EPC tag today,[134] but EPCglobal *supports the objective*. An ability to kill the EPC tag, should in this author's opinion, be present and active before any tag deployment takes place within the European Union and by extension, the European Economic Area. In *WP111*, the summary paper released after the consultation period given for document *WP105*, the Working Party duly notes that while consumers, security industry and universities all agree on the need for a kill command, for consumer products at the exit of stores, retailers and standard bodies for retailers strongly disagree.[135]

Furthermore, as discussed previously, there is a difference of opinion drawn roughly between the same groups, whether item level tagging based on EPCglobal standards will normally entail processing of personal data. This is extremely important because if EPC tag data is not considered personal data, retailers have no obligation to comply with the data protection directive. Meaning that, there would be no obligation to inform individuals on the presence of EPC tags or readers, nor any need to deactivate them.[136] It is for that reason that requests to generally define the EPC as indirect personal data do not sound preposterous.

---

[133] http://epcglobalinc.org.

[134] "Although not available today, development of efficient, affordable and reliable technology to disable EPC tags is an objective supported by EPCglobal." http://www.epcglobalinc.org/public/ppsc_faq/.

[135] *Supra* n56, 3.

[136] *Id.*

Looking next at the requirements of the data protection directive which are outlined in the Working Party guidelines and comparing them with the guidelines the EPCglobal has put forward regarding EPC for consumer products,[137] there is a world of difference between the two. The EPCglobal guidelines, portrayed in table 3, are binding for all the members of EPCglobal.

Table 3: EPCglobal Guidelines on EPC for Consumer Products.

The purpose of these Guidelines is to provide a responsible basis for the use of Electronic Product Code™ (EPC) technology for consumer items. Under the auspices of EPCglobal Inc, these Guidelines have been followed since January 1, 2005 and will continue to evolve as advances in EPC and its applications are made and consumer research is conducted. As EPC evolves, so too will new issues. EPC participants are committed to addressing these issues and engaging in a dialogue about them with interested parties. **1. Consumer Notice** Consumers will be given clear notice of the presence of EPC on products or their packaging and will be informed of the use of EPC technology. This notice will be given through the use of an EPC logo or identifier on the products or packaging. **2. Consumer Choice** Consumers will be informed of the choices that are available to discard or remove or in the future disable EPC tags from the products they acquire. It is anticipated that for most products, the EPC tags would be part of disposable packaging or would be otherwise discardable. EPCglobal, among other supporters of the technology, is committed to finding additional efficient, cost effective and reliable alternatives to further enable customer choice. **3. Consumer Education** Consumers will have the opportunity easily to obtain accurate information about EPC and its applications, as well as information about advances in the technology. Companies using EPC tags at the consumer level will cooperate in appropriate ways to familiarise consumers with the EPC logo and to help consumers understand the technology and its benefits. EPCglobal would also act as a forum for both companies and consumers to learn of and address any uses of EPC technology in a manner inconsistent with these Guidelines. **4. Record Use, Retention and Security** The Electronic Product Code does not contain, collect or store any personally identifiable information. As with conventional barcode technology, data which is associated with EPC will be collected, used, maintained, stored and protected by the EPCglobal member companies in compliance with applicable laws. Companies will publish, in compliance with all applicable laws, information on their policies regarding the retention, use and protection of any personally identifiable information associated with EPC use. Revised September 2005

[137] Available at http://www.epcglobalinc.org/public/ppsc_guide/ (accessed 15 August 2007).

These EPC guidelines call for the labelling of products containing RFID, for informing consumers on the use of the technology and whether the possibility to deactivate RFID tags at the point of sale is available. Instead of giving consumers the right to have a tag removed or deactivated (killed), the guidelines give the retailers the option to make the decision and inform the consumers about their decision. Instead of giving consumers a right to know what the RFID information is being used for, the policy simply calls for companies to publish their policies regarding "record use, retention, and security", not to mention that these guidelines are just that – guidelines – and without a regulation to support them, compliance is a decision to be made by the company.

There is a clear lack of informed contractual relation between the retailers and their consumers, which is considered by the Working Party to probably be the only legal ground available to data controllers to legitimise the collection of the information that the EPC tags freely offer to readers. For that informed contract to become binding, e.g. at the cashier's register, quite an amount of education and information mediation needs to take place from data controller to data subjects. Notices such as those suggested in the EPCglobal guidelines to be given in consumer products only fulfil one of several requirements that the DPD puts forward. While the guidelines request that consumers should be informed of the use of EPC technology, that request does not include informing consumers on the consequences of tag presence in terms of information gathering. This is somewhat solved by section 3, regarding consumer education; however there only lies an *opportunity* for consumers to easily obtain accurate information about EPC and its application. The EPC guidelines completely miss to request of data controllers to inform their data subjects of the effects that has on their privacy, including that the tags broadcast unique serial numbers to any active reader in the vicinity of the data subject's whereabouts.

Additionally, the EPC guidelines are failing to require deployers using EPC tags, to inform consumers on who is collecting the data as well as the purpose for which the information is intended to be used, including the type of data with which the EPC tag data will be associated and whether the information will be made available to third parties.

After publication of some criticism,[138] the EPCglobal guidelines were changed, adding an extra clause in the first sentence of the first item.[139] The second sentence however limits the scope of this addition; by only requiring information to be provided on the product itself. The guidelines could easily be interpreted to not include demand to inform about presence of readers in a store or other public place.

As was described in chapter 4, the EPC is a globally unique numbering system standard, where tags and readers manufactured to function with it all communicate using the same air interface protocol. Generally this means that a soap manufactured by A and sold to both B and C can be read by all readers of both B and C. Should D purchase the soap at B before entering C, the readers at C would pick up the tag's signal whether C planned for it or not. This leads to inadvertent collection of data and dependant on the filter settings of the middleware the record of D moving through C's premises with the soap, might end up in the records amongst other movement tracking inside C. This brings up considerations like whether it would be possible to adjust filter settings to restrict such data from being entered into the information system and whether that should be a requirement put forward by authorities in order to prevent excess data processing of what could be identifiable data.

The filter value is a part of the header of an EPC tag[140] and is used when judged necessary to enable effective and efficient reading of the EPC tags. This is done to improve accuracy of tag reading in a "crowded" area, where many tags respond to a reader communication. This value has already been specified to differentiate between small items boxed together on a pallet and larger items that ship separately. The smaller items' filter values are set to indicate item-level tags and the pallet and larger items receive their own values. This enables the middleware to filter out unwanted data for the level the readers are working on. For example a pallet with 12 boxes of soap only needs one tag value (the pallet value) recorded when it enters into a warehouse centre,

---

[138] E.g. in WP105 *supra* n50 and S Garfinkel *supra* n16.

[139] Item 1: Consumer Notice. The clause added was "and will be informed of the use of EPC technology"

[140] See table in chapter 4.1.

while the items in the boxes need to be read when the pallet is emptied and items further handled (the item-level value). By utilising this filter value already available, item level tags could be rewritten at checkout where the only change of the tag would be adjusting the filter value to indicate "sold" status. EPC middleware would then be required to ignore and remove all event data from tags with filter value set to "sold". The only exception would be those specified readers handling after-sale service at the retailer, and possibly a few other well defined types of readers.[141] This way, retailers would maintain the benefits of after-sale use of the tag data, while consumers would be protected from most unauthorized access to tag post-sale. Such use of the filter value would also eliminate all accidental tag reads that are prone to happen with the use of unprotected tags, like the EPC tags.[142] The only unauthorised read this would not prevent is when someone intentionally decides to breach legitimate protection means, by circumventing the request to remove event data from middleware before sending it to the information system. Such acts would probably happen regardless of the technological measure utilised to protect the tag data.

Other suggested solutions to protect the privacy of consumers without killing the tag, have included: removing or destroying the antenna without touching the chip; having tag status visibly indicated; and probably the most realistically, readers could be made to rewrite the tags at sale, eliminating the serial number portion of the tag. That would render the tag with the benefits of covert reading abilities while at the same time not threatening the privacy of the individual carrying the tagged item. It is that re-write possibility that is available in the EPC tag that enables the change of filter value status.

In the meantime, using blocker tags to disrupt any dialog between tagged item and readers in the vicinity is a solution any person caring for their privacy should consider.[143]

---

[141] Automatic recycling readers come to mind.

[142] Accidental reads like when a person moves from retailer A to retailer B with a bag filled with tagged items purchased at A. As the tags are without protection, the middleware would need to be adjusted to prevent it from processing such event data generated.

[143] For further information on blocker tags see S Garfinkel *supra* n16, 332.

By utilising the filter value in that way, there would be no need to interfere further with data manipulation after accumulation of event data into the information systems, and data controllers would be able to use the data gathered in accordance with any requirements they have presented to the data subjects. Utilisation of the filter value would also arguably increase data quality, as the only data gathered would be the data from tags still for sale.

By not utilising the filter value in EPC tags, or a similar technological measure to prevent a collection of possibly identifiable data, consumers would be prone to the possibility of numerous unknown and unidentified different data collectors. Incidentally it is the fear of such situation that is the biggest hurdle to consumer acceptance of using RFID tags on item level.

6 Conclusion

This thesis began by posing several questions regarding the privacy of individuals and the affect of possible use of personal data in RFID system deployment. Biggest of which was whether regional deployment of the EPCglobal Standard for RFID system in Europe would be possible given current European data protection legislation. Additionally if it would not be, what would need to change, either in the EPCglobal Standard, including its privacy policy or in the European legislation, in order for it to be possible?

The answer to that problem was brought into light by discussing the RFID technology in general as well as the specifics of the EPCglobal Standard system, identifying the legal requirements that the data protection directive does define and measuring the EPC system and its privacy policy against the directive requirements.

Reading the guidelines put forward in *WP105* should be the starting point for anyone considering an implementation of an RFID system on European level or in any of the EU/EEA member states. Nevertheless it requires more than that. It is clear to this author that the EPC standard is a long way from being able to be used for deployment of RFID systems in Europe. This is only partly the designer's fault for stripping the tag of all abilities to secure it self. Another cause is the vague definition of what constitutes personal data[144] in particular through linking and the limits of reasonable likelihood, which gives EPC deployers the chance to ignore the situation and reject any adherence to data protection legislation on the basis that the tag data does not constitute personally identifiable information. This is also caused by inconsistencies in frequency allocations, between Europe and other Western countries. As EPC tag deployment is underway in Europe it is vital for the EU authorities to react quickly and further define the notion of personal data in RFID systems, before unsophisticated EPC tags make it onto the streets, because those tags will incorporate no useful privacy protections.

[144] Which for a framework regulation is a good thing, but for this technology seemingly a bad thing.

There has been little as no discussion in this thesis about real manipulation of data collectors in the face of widely distributed EPC tag deployment. Notions like that the tags could theoretically be used to facilitate dynamic pricing or for retailers to realise how to design their stores by tracking how consumers scan them. This is because such manipulation might be prevented by adhering to the technical and informational requirements already found in the data protection directive and gathered together by the Working Party in *WP105*. Such manipulation is in this author's opinion not the first tier to solve, but should be further explored after rectifying the imminent problems of lack of technological security measures to restrict a pickup of tag data by all EPC readers.

How the problems will be solved is beyond the scope of this thesis, but one of the solutions could be to make use of the filter value discussed in chapter 5 by altering readers to have them rewrite the tag at sale, adjusting the filter value to a "sold" status which would then be required to be ignored by readers in general. The only readers allowed to access such tags would be specified readers used in connection with warranty, returning of items, recalling them and lastly but certainly not least, when selecting process for recycling the tagged items.

Whatever the solution becomes, it must be remembered that the data collected by use of EPC tag systems should be considered personally identifiable even though the collector would not be able to make that link, if a link is reasonably likely to be made.

What is reasonably likely in tomorrow's data warehousing thus remains the key to the solution.

References

List of Judgements/Decisions

Treaties/Statutes

Commission Decision 2006/804/EC of 23 November 2006 on harmonisation of the radio spectrum for radio frequency identification (RFID) devices operating in the UHF band. (Official Journal L 329, 25/11/2006 P. 0064 – 0066.)

Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (in short the Radio Spectrum Decision). (Official Journal L 108, 24/04/2002 P. 0001 – 0006)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, 31).

European Convention for the Protection of Human Rights and Fundamental Freedoms, ETS no 5.

Secondary Literature

K Albrecht and L McIntyre: *Spychips: How major corporations and government plan to track your every move with RFID* (Nashville: Nelson Current, 2005)

Article 29 Data Protection Working Party: Working document on data protection issues related to RFID technology, WP 105, 19 January 2005, available at:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

Article 29 Data Protection Working Party: *Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology*, WP 111, 28 September 2005, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf

Article 29 Data Protection Working Party, *Working Party 29 Opinion on the use of location data with a view to providing value-added services*, WP115, November 2005, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf

Article 29 Data Protection *Working Party, Opinion 4/2007 on the concept of personal data*, WP136, 20 June 2007, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

The Australian Department of Foreign Affairs and Trade, *The Australian ePassport*, available at: http://www.dfat.gov.au/dept/passports/.

M Baard, "Is RFID Technology Easy to Foil?" *Wired News*, 18 November 2003, available at http://www.wired.com/politics/security/news/2003/11/61264.

D Brock: *The electronic Product Code (EPC): A naming scheme for physical objects* Auto-ID Center White Paper. 1 January 2001. Available at http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH-002.pdf

D Brown: *RFID Implementation* (McGraw-Hill, 2007)

L Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, (The Hague: Kluwer Law International, 2002), Chapter 3, 57-69.

A Charlesworth: “Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual” in Edwards & Waelde (eds): *Law & the Internet: a framework for electronic commerce*. pp [79]-122. Oxford 2000.

J Collins, “DOD Awards Contracts for EPC Tag”, *RFID Journal*, 22 March 2005, available at: http://www.rfidjournal.com/article/articleview/1460/1/1/.

B Crispo, MR Rieback and AS Tanenbaum, *Is Your Cat Infected with a Computer Virus?* IEEE PerCom 2006, available at http://www.rfidvirus.org/papers/percom.06.pdf

EPCglobal Inc., *Electronic Product Code (EPC): An overview*, available at: http://www.epcglobalinc.org/public/ppsc_factsheets/epc_overview

EPCglobal Inc., *EPCglobal, Inc. Public Policy Steering Committee (PPSC) Frequently Asked Questions on Guidelines on EPC for Consumer Products*, available at: http://www.epcglobalinc.org/public/ppsc_faq/.

EPCglobal Inc., *Guidelines on EPC for Consumer Products*, available at: http://www.epcglobalinc.org/public/ppsc_guide/.

European Commission, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*. SEC(2007) 312. COM(2007)96 final. A communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Available at: http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf

European Commission, *The RFID Revolution: Your voice on the Challenges, Opportunities and Threats*. Results of the public online consultation on future radio frequency identification technology policy. SEC (2007) 312. COM (2007) zzz final. (Brussels: 2007), 5. Available at http://ec.europa.eu/information_society/policy/rfid/doc/rfidswp_en.pdf

S Garfinkel and B Rosenberg (eds): *RFID: Applications, Security, and Privacy* (Addison Wesley, 2006)

B Glover and H Bhatt, *RFID Essentials* (Cambridge: O'Reilly, 2006)

J R Hind: *Identification and tracking of persons using RFID-tagged items*. US patent application #20020165758. Assigned to … Filed 05/03/2001. Available at http://www.freepatentsonline.com/20020165758.html

J R Hind: *Method to Address Security and Privacy Issues of the Use of RFID Systems to Track Consumer Products*, U.S. patent application #20020116274, assigned to International Business Machines, filed 21 February 2001. Available at: http://www.freepatentsonline.com/20020116274.html.

C van 't Hof, *RFID and Identity Management in Everyday Life: Striking the balance between convenience, choice and control*, a study commissioned by STOA under Framework Contract IP/A/STOA/FWC/2005-28 (2007). Available at http://www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf

Integrated Engineering *Product sheet* for the e-Document Reader used to read ePassports: http://www.ieprox.com/files/Datasheets%20feb.%202007/e-Document%20Reader%20.pdf.

ITU Internet Report 2005: *The Internet of things* (Geneva: ITU, 2005)

A Juels, D Molnar and D Wagner, *Security and Privacy Issues in E-Passports*, IEEE SecureComm 2005, available at: http://www.cs.berkeley.edu/~dmolnar/papers/RFID-passports.pdf.

O Kobelev: "Big Brother on a Tiny Chip: Ushering in the Age of Global Surveillance Through the Use of Radio Frequency Identification Technology and the Need for Legislative Response" in *North Carolina Journal of Law & Technology* Spring, 2005. (6 N.C. J.L. & Tech, 325-342.

J Krim. *Embedding their hopes in RFID – Tagging technology promises efficiency but raises privacy issues*. Washington Post, June 23, 2004.

C Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, (Oxford: Oxford University Press, 2007, 2nd ed)

MC O'Connor, "Washington Driver's Licenses to Carry EPC Gen 2 Inlays", *RFID Journal*, 30 July 2007, available at: http://www.rfidjournal.com/article/articleview/3514/1/1/.

RAND Corporation, *Privacy in the Workplace*, a research brief describing work done for RAND Infrastructure, Safety, and Environment and documented in 9 to 5: Do You Know If Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace by Edward Balkovich, Tora K. Bikson, and Gordon Bitko, TR-197-RC, 2005, 36 pp., ISBN: 0-8330-3719-6. The research brief is available at: http://www.rand.org/pubs/research_briefs/RB9107/index1.html.

H Stockman: *Communication by Means of Reflected Power*, proceedings of the IRE, (1948), 1196-1204.

Verisign, *The EPCglobal Network: Enhancing the Supply Chain*, (2005), available at http://www.verisign.com/stellent/groups/public/documents/white_paper/002109.pdf.

B Wilson: "Big Brother at the supermarket till", *BBC News*, 27 January 2005, available at: http://news.bbc.co.uk/2/hi/business/4211591.stm

Annex: Technological details of RFID[145]

Radio frequency technology is somewhat complicated, including several components and many different usable solutions. This Annex is compiled to further explain the technological means of the system, which is required to some extend, to understand both the scope and the limits of the technology.

The tag

An RFID tag, also known as a transponder, is a small device that can be attached or built into an item, case, container or pallet, for identification and tracking. The tag is composed of a microchip and an antenna.

The microchip may be half the size of a grain of rice, but the antenna must be large enough to pick up the radio signal from the reader and to transmit back. Tags come in a variety of shapes, sizes, formats and characteristics. The intended uses, as well as the size of the antenna, are therefore the factors that determine the tag's size.

Active, Passive or Chipless tags

There are two types of RFID tags, active and passive with the third type, chipless tags, emerging. Passive tags receive a message from the reader and broadcast a reply. They have no source of energy of their own but derive it from the reader's radio wave. Active tags may broadcast continuously, and beacons may broadcast intermittently. Active tags have a transmitter for sending signals to the reader and normally their power comes from an onboard battery, but it may come from other sources.

Active tags have greater range, data capacity, and processing power. They can work with extremely weak reader signals. They can also incorporate sensors that record and

[145] This Annex is first and foremost based on technical descriptions in two books. D Brown: *RFID Implementation* (McGraw-Hill, 2007) and S Garfinkel and B Rosenberg (eds): *RFID: Applications, Security, and Privacy* (Addison Wesley, 2006). Other material will be cited when used.

timestamp such telemetry data as temperature, location via GPS, shock events, tampering events, moisture levels, and radiation. Active tags typically cost more than USD 20 each, reaching to over USD 100 each in some cases. Active tags also require maintenance of their power source.

Passive tags, since they draw their power from the reader, require a strong signal from the reader in order to function. In turn, they produce a weak signal back to the reader. Active tags, on the other hand, can work with weak signal levels from the reader, and they can produce strong signals back, driven by their own power source. Additionally, the active tag is continuously powered, always functioning. It can record data even when no reader is present. The passive tag functions only when in the presence of a reader.

Active tags can be viewed as miniature computers, capable of operating sensors and performing calculations and logic operations, encryption and decryption, and sophisticated two-way wireless communication over substantial distances. Active tag systems can monitor a large area and thousands of tags with only a few readers. The active tags are costly as compared with passive tags, so their use is limited to high-value items and processes. If an active tag has a battery, it has to be maintained and, ultimately, replaced. Active tags may last as long as ten years, but eventually the battery runs out.

Active tags are available on most frequencies where RFID is used, but for many applications, the preferable frequency is in the amateur radio band, right at 433 MHz. At this frequency, the wavelength is about one meter, which enables it to propagate around many obstacles that would halt the shorter UHF radio waves. Active tag read ranges at 433 MHz can reach as long as 300 feet (90 meters)

Passive tags transmit only when they are in the field of a reader. Otherwise, they are silent. As they have no internal power supply, they can waken decades after manufacturing.[146] Passive tags are much less costly than active tags. Experts generally

[146] *Supra* n50, 3.

believe that UHF passive tags will reach a cost of 5 US cents per tag when purchased in large quantities before the end of 2008. By comparison, a bar code label, including the cost of application, costs less than 1 US cent. Passive tags are best used where the movement of tags is highly consistent and controlled, and little security, sensing capability, and data storage is required.

Both active and passive tags discussed so far work with an integrated circuit chip inside them to store their data and to perform the processing logic. By contrast, a few innovative companies have developed what are called “chipless tags”, which use different technologies to store and transmit their data. They have no integrated circuit. Instead, they encode unique patterns on the surface of various materials. These patterns encode the data reflected back to readers. Chipless tags are read-only; the data is permanent. However, chipless tags are significant in that they appear to offer a much lower price point for the tags. The drawback is that no international standards for chipless tags have been established. Nonetheless, it has been estimated that chipless tags will comprise up to 30 percent of RFID tags in just a few years.

At least one company manufacturing chipless cards appears to solve many of the common problems that arise in RFID pilots and deployments. Read ranges extend up to 30 meters, the tag is not sensitive to metal or liquid and is smaller than active or passive tags. The tags operate at 2.45 GHz, which is a frequency internationally recognized and generally available for RFID.

Tag data

Tags acquire their data in a variety of ways. *Pre-encoded* tags are commissioned[147] by the manufacturer when the chip is made. Customers who intend to use these tags may order the chips with customized numbers, but they cannot change them themselves.

Unlike pre-encoded tags, *write-once-read-many* (WORM) tags are commissioned by the customer, usually when they are first put into service. The first write definitively establishes the data contents of the tag and then it cannot be changed. Commissioning is

[147] The initial entry of data into the tag is called commissioning the tag.

typically done when the identity of the object to be tagged first becomes known. WORM tags enable you to put your own number or other information into the tag at any single point in the production and distribution process, and that permanently establishes it.

Electronically erasable programmable read-only memory (EEPROM) tags can be written many times by a qualified piece of equipment. This enables the tag to be rewritten with new information at different points in the work process or to be reused. EEPROM tags will hold their data values for up to about ten years without accessing a power supply. The oxide layer of the EEPROM deteriorates after that.

Data can be added to read-write tags by a simple reader at any point in their lifetime. This type of tag brings important capabilities to your application; it enables the tag to acquire information as it moves through a business process, store it, and provide it back to readers later on. A work-in-process application is a good example where read-write tags are useful. The tags can collect and record data such as date, time, who worked on it, what machines were used, and environmental conditions as the unit proceeds through the production process. When the process is complete, the tag contains a complete record of every step taken, and the record can be downloaded at the end.

Active read-write tags may be manufactured with sensors. They meet users' needs to continuously monitor the contents and the environment for conditions that might indicate tampering, spoilage, theft, or other forms of deterioration. Passive read-write tags are also available.

The reader

A reader, also known as tracker, uses its antennas to stimulate tags, read their data, and transmit it via a network to a host computer. Readers can also commission a tag and write data to its memory. In the simplest case, the reader transmits a simple query, and any tags within its field transmit their contents. In today's more sophisticated cases, the reader sends authentication information and commands coded in the radio waves.

The middleware and information systems

The middleware is the brain behind the operation. The raw data that the reader generates is analysed and filtered in the middleware before it is integrated into other information systems. This is done to ensure that only useful, meaningful information is entered into the information system. The middleware interfaces with warehouse management systems, CRM systems and supply chain partners' systems, to name a few, all depending on the RFID application in place and how it's data is to be used. It is the middleware that manages bar code scanners, printers, scales, sensors, validation stations, employee badge readers or whatever device the system has in place.

The payoff for the RFID system lies in the generation of new data and putting it to use through the integration of RFID into an organization's information systems, asset tracking systems and ultimately, its purchasing, logistics and stocking decisions and sharing it with trading partners.

The technical means of interaction between tags and readers

Radio waves pass through air, but they can also pass through many other materials such as plastic, cardboard, wood, cloth and so on. Radio waves are less efficient at passing through opaque materials like metal and liquids.

Different wave frequencies differ in their ability to penetrate opaque materials. Low frequency and high frequency tags are able to penetrate or circumvent opaque materials while ultra-high-frequency, the industry standard for item-level tagging, is absorbed by water and reflected by metals. This difference between the behaviour of the different frequencies is important to consider, as it might affect the methods used for security and disabling of the technology. Additionally low and high frequency tags are more expensive to manufacture than UHF tags.

Radio waves have three characteristics that are of interest from a privacy standpoint: frequency, wavelength and read range. Frequency and wavelength control the distance from which the tag can be read (along with the ability to travel through opaque materials). Frequency and wavelength have negative correlations meaning that a higher

frequency corresponds to a shorter wavelength. Every frequency has a unique corresponding wavelength.

Table 1: Frequency characteristics[148]

	LF[149]	**HF[150]**	**Amateur Band[151]**	**UHF[152]**	**Microwave**
Frequency	9-135 KHz	13.553-15.567 MHz	430-440 MHz	860-930 MHz	2.4-2.4835 and 5.8 GHz
Wavelength[153]	2300 meters	22 meters	69 cm	33 cm	12 cm
Opaque materials	Not susceptible	Somewhat susceptible	Somewhat susceptible	Very susceptible	Very susceptible
Read rates	Slow		Fast	Fast	Very fast
Read range	50 cm	1 meter	30 meters	4-5 meters	10 meters

Table 1 shows amongst other things, the wavelengths associated with the five frequency ranges commonly used by RFID systems. Low-frequency waves are much longer than others are. These longer waves can go around obstacles that would stop shorter ones, but they take more power to traverse the same difference. Opaque materials will obstruct shorter waves, but if they are unimpeded, they can go significant distances using very low energy resources.

---

[148] D Brown, *supra* 1, p7 and p13. See also further explanation of the difference between these frequency options *id*, 9-12. An example of specific wavelength is the technology used in the Icelandic RFID passport. The frequency used is 13.56 MHz which has waves about 22 meters long, see D Brown *supra* n1, p10. It is however important to note that the Icelandic RFID passport is developed using an ISO standard that limits the read range (ISO 14443, Proximity Card).

[149] Low frequency.

[150] High frequency.

[151] Amateur radio band.

[152] Ultra-high frequency.

[153] Approximated wavelength.

The antenna and its associated electronics determine the frequency of a radio wave. The length of the antenna limits it to a range of frequencies and the size of the antenna is proportional to the wavelength.

There is inconsistency in UHF frequency applications around the world. Europe has allocated 865-868 MHz while North America has allocated 902-928 and Australia 918-926 MHz, to name a few areas around the world. This could mean that a tag applied to a product manufactured in North America but imported to Europe, would require to be communicated with on a frequency outside of the allocated range in Europe.

Read rates for multiple UHF tags are different in different countries because of an interaction between bandwidth and the methods utilized to communicate between tags and readers. The wider the bandwidth is, the faster a large group of tags in a read zone can be read. Therefore in the United States (which has 26 MHz bandwidth) UHF tag read rates are rated at about 1600 tags per second while in Europe (which has 3 MHz bandwidth) they are rated about 600 tags per second. This means that readers will operate faster in North America than in Europe leading to a probability of better privacy protection in Europe than North America.