REPORT

Client: Chiara Giovannini
ANEC
European Association for the Co-ordination of Consumer Representation in Standardisation.

Av. De Tervueren 32,
Box 27,
B- 1040 Brussels

Report issued by:

Intertek ETL SEMKO
Research & Performance Testing

Davy Avenue
Knowlhill
Milton Keynes
MK5 8NL

Tel. +44 (0)1908 857777
Fax. +44 (0)1908 857830

AUTHORISED FOR ISSUE: ..... Wendy Brown
Operations Manager

DATE: October 2007

REPORT AUTHOR: Colin Meek

R64564 Issue 1

Consumer requirements for RFID standardisation

CONTENTS

SECTION		PAGE
1.	Introduction	4
2.	Review Of Work By Consumer Organisations	8
2.1	The Netherlands	8
2.2	UK	10
2.3	Germany	11
2.4	Other activity	11
2.5	Consumer organisations that have not carried out any work on RFID	11
2.6	Consumer Organisations outside Europe	12
2.7	Civil Rights Organisations	12
3.	Priority Applications	13
3.1	Introduction	13
3.2	RFID tags in the retail environment	15
3.3	The use of RFID in transport ticketing	17
3.4	The use of RFID systems to deter counterfeiting and improve traceability	19
3.5	European Biometric Passports	20
3.6	Themes	21
3.7	Comment on issues related to specific applications	26
4.	Privacy	28
4.1	Introduction	28
4.2	Threats to privacy	29
4.3	Potential solutions	32
5.	Security	43
5.1	Introduction	43

5.2 The risks to consumers 45

5.3 Risks in specific environments 46

5.4 'Back office' attacks 48

5.5 Potential solutions 49

5.6 Non-technical solutions 50

5.7 Application-specific guidelines 51

6. Health 53

6.1 RFID in healthcare 53

6.2 Potential risks 53

6.3 RFID and health 53

7. Standards And Best Practice Guidance 55

7.1 Introduction 55

7.2 The ICTSB Overview 57

7.3 Technical standards. 57

7.4 Guidelines and other RFID standardisation initiatives 59

8. Recommendations 67

8.1 Privacy 67

8.2 Security 71

8.3 Conclusion 73

APPENDIX I EPCGlobal Guidelines

APPENDIX II NIST – Recommended Practices

APPENDIX III Glossary

1. Introduction

Radio Frequency Identification (RFID) is the term used to describe the technology that allows 'readers' to capture information from devices called 'tags' that are placed on objects, animals, people or documents. Many different tags have been, or are being, developed with many functionalities that can be used in an infinite number of applications. Key to the technology is the ability of the system deployed to identify objects without making contact. Typically tags can be read at a distance of a few centimetres and up to a few metres.

Another feature of RFID technology is that the tags can be either 'passive' or 'active.' Passive tags require high-powered readers to both charge the capacitor to power the tag and to pick up its signal and read the information. Passive tags usually have an unlimited lifespan and can be extremely small. Active tags have their own independent power supply usually in the form of a battery that has a limited lifespan. These active tags can store more information than passive tags and that information can be rewritten. Active tags are normally used where a longer read range is needed.

RFID is not a new technology, but there has been a dramatic increase in RFID system deployment in recent years. Until relatively recently the technology was mainly been used for military purposes and within specific supply chains to monitor the location of valuable machine parts for example. RFID systems are still commonly used in similar environments but are now also frequently deployed at an item level to monitor stock in retail settings but are also being deployed in many other consumer applications.

While consumer awareness of RFID technology is relatively low, RFID has been the subject of extraordinary business to business media scrutiny and there is a wide expectation that RFID use will become common and perhaps ubiquitous.[1] It is difficult to assess the growth of RFID use and forecast trends for many reasons,[2] but two recent analyses have suggested that the market will achieve an annual growth rate of between 30 and 50 per cent until the year 2010. The number of RFID patents

[1] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Page: 94.
[2] Federal Office for Information Security. *Security Aspects and Prospective Applications of RFID Systems.* 2004. Page: 62.

registered has also jumped by 65 per cent every year for the past few years indicating the growth of interest in this technology by developers.[3]

Although awareness of RFID technology in the general population growing, it is surprisingly low given the number and extraordinary variety of applications already deployed that have a direct impact on consumers. For example:

- Rubbish bins in parts of Germany have been RFID enabled and linked to specific households. Readers on rubbish collection lorries record how often the bins are emptied. The data is used for waste management plans and billing by weight.

- RFID systems are being used in Taiwan to combat Severely Acute Respiratory Syndrome (SARS). Patients wear RFID tags and the data is used for the precise tracking of infection paths.[4]

- RFID systems are being used in new passports to improve document security.

- Michelin has already embedded tags in tyres to counter the threat from counterfeit goods and to make consumer recalls easier.

- RFID schemes have been introduced in ski resorts to allow visitors to access lifts, gondolas and other services such as ski rental automatically.

- Consumer deployments also include RFID enabled travel passes and payment systems.

Some of those applications are described in more detail in **chapter 4** but this variety indicates how pervasive RFID technology is likely to become in the next decade. Many of these examples demonstrate that RFID technology has the potential to help improve healthcare, improve services and, perhaps, improve public safety. Applications in hospital, for example, may allow for more accurate delivery of drugs with fewer mistakes. In 2000 more than 14 million Firestone tyres were recalled after they were discovered to be faulty following a production error. In the future these kind

[3] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Page: 95 and 99.

of recalls may be made easier if all tyres can be individually identified and linked to their owners. RFID systems are also being used to help improve the traceability of animals to help fight infections such as Bovine Spongiform Encephalopathy (BSE).

There is no doubt that specific applications may be beneficial for individuals and society, but any technology that makes it possible to link the physical world with private data that can reveal information about who we are, where we live, how we spend our money and where we move around is bound to raise legitimate concerns about privacy and security.

RFID systems have inherent characteristics that mean privacy cannot be protected through security measures alone. Solving the security problems will not prevent a company from potentially being able to use an RFID system to profile a consumer and from passing that information on to a third party. Nor does it prevent a travel card provider from tracking the movements of an individual within a city. These characteristics of RFID raise important questions about privacy and consent. The launch of the PayPass credit card service in the UK (see **chapter 3**) means that individuals may now be able to purchase food items using an RFID enabled credit card as they travel to a football stadium using an RFID enabled e-ticket and gain access to the stadium using an RFID enabled loyalty card. The mass deployment of RFID is now well underway.

Despite the growth in the number of consumer RFID systems the European Commission and member states are only just beginning to put in place mechanisms that can construct an appropriate regulatory response.

This report will:

- explore the work undertaken by consumer groups on the subject of RFID (**chapter 2**);

- describe a range of consumer RFID applications (focusing on the use of RFID on consumer goods in retail, in transport tickets and in the healthcare setting) (**chapter 3**);

[4] Federal Office for Information Security. *Security Aspects and Prospective Applications of RFID Systems.* 2004.

- examine the threats and benefits of RFID applications to consumers' privacy (**chapter 4**), security (**chapter 5**) and health (**chapter 6**);

- describe the formal and informal standards (and guidelines) for RFID that exist at European and International level (**chapter 7**);

- explore options for further standards and guidelines to protect the consumer interest (**chapter 8**).

The desk research for this report was carried out from May 2007 to September 2007. Key experts from a range of stakeholders were contacted for their views and interviews conducted by phone or email. Nearly 20 consumer applications are described and several consumer organisations in Europe were contacted for information about their work on RFID issues and applications. A detailed examination of existing RFID standards, guidelines and codes of practice was also undertaken. This survey focused on *non-technical* standards and guidelines designed to protect the consumer interest or improve RFID security.

2. Review of Work by Consumer Organisations

Twelve consumer organisations based mostly in Europe were contacted for information about their policy development on issues related to RFID and for details of any testing carried out on RFID applications or Privacy Enhancing Technologies (PETs). Given the nature and scale of RFID deployment now in operation, surprisingly few of the organisations contacted have developed any kind of policy response. None have 'tested' consumer RFID applications or PETs.

This section summarises the responses from those organisations that have developed policy.

2.1 The Netherlands

2.1.1 Policy Development

- A representative of Consumentenbond spoke at the European Commission workshop on RFID in May 2007. In the speech 'RFID: Let's not spoil a beautiful future' Koen Dupon focused on the potential benefits of RFID and how these may be undermined by threats to privacy and security.

- Consumentenbond contributed to the development of the Trans Atlantic Consumer Dialogue (TACD) resolution (see **chapter 7**) and wrote to the Trade and Industry Minister for the Netherlands describing the organisation's main concerns regarding RFID consumer applications; for example, the threat of discrimination, the lack of data on health impact and the threat to privacy.

- Consumentenbond argues that security and privacy should be brought into the standardisation process and that choice should be guaranteed through 'opt in' systems of RFID deployment. Under these systems companies would have to clearly explain the consumer benefits so that consumers had an explicit choice. Consumentenbond also states that the covert deployment of RFID should be made an offence.[5]

[5] Interview. Koen Dupon, Consumentenbond. July 2007.

2.1.2 Research

Consumentenbond recently published results from a major study on RFID awareness among consumers. The study also looked at consumer attitudes towards RFID. More than 2,000 consumers completed an internet survey and others took part in focus groups. The results were made available in October 2007.[6] This summary of the findings covers the most relevant results:

- 25% of those surveyed said they had heard of RFID and were aware of some applications. 14% said they knew what RFID is and were aware of some applications. 62% of respondents said they were not familiar with the term RFID but were aware of some applications.

- 21% of those surveyed had experience of RFID in the workplace.

- Two-thirds of those surveyed said they worry about public transport companies using personally identifiable data for marketing purposes. 72% said they had no problem with the concept of using travel data to trace witnesses and suspects of crime. 60% agreed with the statement: 'everyone should have a personal public transport card so that people who misbehave can be kept out of public transport.' More than a third of those who do not yet have a card said they would opt for an anonymous card.

- 23% said they already had a biometric passport or ID card. 66% said they support the central storage of digital fingerprint data in a central database that is accessible by national or foreign intelligence agencies. 20% were opposed. 56% support the storage of facial scans or photographs, while 26% are opposed.

- 62% of people surveyed said they expect prices in shops to rise through RFID technology. 70% said they would welcome paying for all goods at the same time at a counter, while 51% said they would miss the personal contact if this was automated.

[6] Interview. Koen Dupon, Consumentenbond. July 2007.

- At least 85% said they wanted RFID use on products to be transparent; support default deactivation of chips; and, want the final say on whether a chip stays active.

- 25% agreed with the statement: 'it doesn't matter to me if RFID generated data about me is being collected, "they" already know so much about me.' 47% disagreed with that statement. 41% said they have confidence that the data will only be used for the stated purpose. 37% did not believe that position to be true. 57% think unauthorised people will gain access to databases.

- Those surveyed rated the 'pros' and 'cons' of RFID in order of importance. The most important pros were: 1. the fight against crime; 2. ease; 3. a better determination of ID; 4. possibly fewer cards; 5. theft prevention. The most important cons were: 1. difficult to make a correction when the system makes a mistake; 2. data being used for other purposes; 3. possible misuse of RFID data and/or databases; 4. criminals know a way to get round the system; 5. use of data for personal commercial messages (like spam in public spaces, etc.).[7]

2.2 UK

2.2.1 Policy Development

- The UK's National Consumer Council (NCC) organised a 'summit' in 2004 to explore the future of RFID technology in retail. Twenty people attended representing several stakeholders including consumers, civil liberty groups, retailers, technologists and government officials.[8]

- The NCC developed themes discussed at the summit in its publication the *Glass Consumer*.

- The NCC helped to draft the Transatlantic Consumer Dialogue (TACD) resolution on RFID.[9]

[7] Koen Dupon. Personal Communication. Oct 2nd, 2007. Summary of Results (English)
[8] The National Consumer Council. Calling in the chips? Dr Susanne Lace. Seminar Report. May 2004.
[9] Interview. Anna Fielder, NCC. July, 2007.

2.3 Germany

The Federation of German Consumer Organisations (VZBV) helped draft the TACD resolution on RFID and gave a key presentation at the conference 'RFID: Towards the Internet of Things' in Berlin in June 2007.[10] [11]

In 2006 the Federation publicly criticised industry attempts (in Germany) to introduce a best practice code for consumer application RFID deployment. Specifically, VZBV condemned the draft code for failing to state that tags should be automatically deactivated at the cash-out. The industry initiative was coordinated by GS1 Germany.[12]

2.4 Other activity

2.4.1 Denmark

A representative of the Danish Consumer Council spoke at the European Commission workshop on RFID in May. The speech, given by Anette Høyrup and titled 'Consumer concerns can be solved', listed five important RFID principles: consumer control; data protection directive; consumer-friendly technique; interoperability; and sustainability. She also argued that the principles of the Data Protection Directive should be met.

2.4.2 Other consumer organisations known to have carried out work on RFID but failed to respond to requests for interview:

Forbrukerradet (The Consumer Council of Norway) – Norway

2.5 Consumer organisations that have not carried out any work on RFID

The following organisations were contacted and confirmed that no work has been carried out on RFID:

[10] Presentation at the conference 'RFID: Towards the Internet of Things.' June 2007, Berlin. Patrick von Braummuhl.
[11] Personal Communication with Roland Stuhr, VSBV. July 25th, 2007.
[12] VZBV Press release. June 29th, 2007.

Stiftung-Warentest (Germany)[13]

VKI (Austria)[14]

Edideco (Portugal)[15]

Association Belge des Consummateurs (Association of Belgium Consumers)[16]

Que Choisir (France) was contacted but did not respond.

2.6 Consumer Organisations outside Europe

2.6.1 Consumers Union – USA

In May 2006 the Consumers Union reported that consumers were barely aware of RFID technology but that the RFID tags were being used in credit cards, prescription-medicine packaging, computer equipment, TVs, clothing, cell phones, and the workplace. Consumers Union also said it was concerned about the prospect of RFID enabled e-Passports. At the time a CU spokesman stated: 'It's essential to develop the proper framework to protect consumers from the unprecedented privacy and identity theft risks that come with RFID.'[17]

Australian Consumers Association was contacted but did not respond.

2.7 Civil Rights Organisations

A range of other civil and privacy rights groups have voiced concerns about the deployment of consumer RFID applications. For example, European Digital Rights (EDRI) is an association of 25 privacy and civil rights organisations from 16 countries in Europe and a member of the European Commission's RFID Expert Working Group. It has published its contributions to the group in which it has raised several key concerns about privacy and user control[18]. Another influential group is the Electronic Frontier Foundation (EFF) in the US. EFF is a non-profit campaigning membership organisation.

[13] Bernd Schwenke. Personal communication. July 31st, 2007.
[14] Paul Srna. Personal communication. July 30, 2007.
[15] Personal Communication with Antonio Alves. August 15, 2007.
[16] Phone interview with Jorge Peeters. Aug 8th, 2007.

3. Priority Applications

3.1 Introduction

In a relatively short time RFID technology has jumped from being an expensive tool for supply chain management used by the largest multi-national companies to being viable system to improve retail efficiency at the item level and, it is claimed, a way for service sector companies to better tailor their products for their customers.

In 2006 LogicaCMG was commissioned by GS1 (see glossary) to forecast the market for passive RFID in Europe for 2007 up to 2022. It surveyed more than 80 companies and concluded that more than 7600 readers would be deployed in 2750 locations in order to process 144 million passive tags in 2007. Within just five years the report predicted that 175,000 readers would be deployed in 30,000 locations to process more than 3 billion tags. The report forecasts that by 2012 2% of all retail items will be tagged and by 2022 25% of all non-food and 5% of all food items will be tagged. It also found that the best single prospect for market growth was the tagging of high-value retail items.[19]

The growth of RFID deployments and the scale of those in use mean that the number of consumers coming into direct contact with RFID enabled systems is growing rapidly. RFID systems are now used in several European public transport systems, they have been used to defeat counterfeiting of tickets for sports tournaments, used to monitor consumer movements in theme-parks and as systems for item-level identification in retail. In the near future it is hoped that the systems will be used more widely within healthcare. For example, as systems to help pharmaceutical companies deter drug counterfeiting and to keep track of items in operating theatres. RFID consumer applications go far further than experimental or 'pilot' projects. In September 2007 Mastercard launched its 'PayPass' system in the UK that will allow consumers with 'PayPass' enabled credit cards to pay for low-cost items by touching their cards on a reader. Major banks in the UK have already announced their backing

[17] Consumers Union. Press Release. May 4, 2006.
[18] http://www.edri.org/issues/technology/rfid
[19] European passive RFID Market Sizing 2007-2022, February 2007.

for the new RFID enabled system and are replacing expired cards with the new PayPass enabled versions.[20]

Tables 3.2 to 3.4 explore RFID deployments in three key environments identified by ANEC as priority areas:

- the use of RFID tags to replace bar-codes in the retail sector and as alternative methods of payment;
- the use of RFID in transport ticketing and passports; and,
- the use of RFID systems to deter counterfeiting and improve traceability (in food chain and drug packaging in particular).

Section 3.5 describes the European biometric passport application.

Section 3.6 examines a range of themes that cut across several application areas.

Section 3.7 highlights other consumer issues related to specific application types.

[20] http://www.mastercard.com/uk/personal/en/paypass/faq.html accessed September, 2007

3.2 RFID tags in the retail environment

Deployment	Location	System	Issues	Other observations
Metro Group Future Store	Rheinberg, Germany and to be extended to Real branded store soon[21]	Pilot uses UHF passive tags in labels attached to packs. [22]	One of the most controversial RFID deployments. While pilot was widely advertised, store customers were not warned about RFID enabled loyalty cards. Also, technology used to disable tags found to be defective.[23]	The project is a partnership between METRO, Intel, IBM, T-Systems and around 60 other companies from the IT and consumer goods and service sector industries.
Marks & Spencer in partnership with Intellident Ltd.	More than 40 stores in the UK and soon to be extended to 100 more.	Tags added to garments by suppliers. Used for efficient stock taking.[24]	M&S consulted widely before deployment in order to avoid a backlash and its trial was public. It also acted on recommendations made by consumer groups vocal on the RFID issue.[25]	One of the largest deployments of item-level RFID in the world.
Boekhandels Groep Nederland (BGN) using software by Progress Sofware Corporation	Book stores in Almere and Maastrict in the Netherlands.	UHF tags applied to all books to allow tracking at item-level. Crucial to the system is the communication about inventory to the third party bulk supplier. Both customers and staff can search inventory to search for book locations.[26]	Some concerns about privacy but little information on this available. Reports state that the company kept customers informed and decided not to link book purchase information with individual customer information. RFID tags can be removed or killed at the till.[27] [28]	

[21] RFID and identity management in everyday life. Scientific Technology Options Assessment. June 2007.
[22] http://www.future-store.org accessed September, 2007.
[23] http://networks.silicon.com/lans/0,39024663,39118760,00.htm accessed September, 2007.
[24] http://www.intellident.co.uk/en/3.00/ge_newsarticle.php?storyid=07060401 accessed September, 2007
[25] http://www.rfidjournal.com/article/articleview/623/1/1/
[26] http://investors.progress.com/phoenix.zhtml?c=86919&p=irol-newsArticle&ID=843825&highlight= accessed September, 2007.
[27] http://www.rfidupdate.com/articles/index.php?id=1103 accessed September, 2007.
[28] RFID and identity management in everyday life. Scientific Technology Options Assessment. June 2007.

Deployment	Location	System	Issues	Other observations
ExxonMobile Speedpass developed by Texas instruments	US, Canada, Singapore, Japan	RFID passive chip carried in a case on, usually, a keyring. This enables users to pay for petrol and retail items in Exxon stations.	The speedpass is also used for marketing which means the data collected can be passed on to third parties. This includes profile information. When customers use the pass they are deemed to have opted into the scheme's privacy policy. Customers have access to their own transaction data.[29]	
RFID equipped libraries. Several companies involved including Bibliotheca RFID Library Systems	Multiple locations including: Vienna, Stuttgart, Leuven and Dresden.	Tagged books, terminals for checking in and checking out books and sensor gates to prevent theft.[30]	Concerns about the privacy of library users have been voiced by the Electronic Frontier Foundation in the US. EFF has opposed the introduction of RFID systems in libraries in the US for that reason. [31]	
Mastercard PayPass	UK	Consumers are issued with RFID enabled credit cards that allow 'contactless' for low-value items. Extra security is built into the system as consumers will be asked for a PIN number after a set number of contactless transactions.	Launched in September 2007, this system has only just gone live and the UK roll-out is the first in Europe. The PayPass scheme is already operational in the US, Canada and 11 other countries.[32]	More than 1,000 retailers have signed up to accept the PayPass payments.[33]

[29] Cusomters have access to their own transaction data.
[30] http://www.researchinformation.info/rimayjun04radiotagged.html accessed September 2007.
[31] http://www.eff.org/Privacy/Surveillance/RFID/20031002_sfpl_comments.php accessed September 2007.
[32] http://www.mastercard.com/uk/personal/en/paypass/faq.html#9
[33] http://money.guardian.co.uk/creditanddebt/creditcards/story/0,,2162262,00.html accessed September 2007.

3.3 The use of RFID in transport ticketing

For information on RFID in passports see section 3.5.

Deployment	Location	System	Issues	Other observations
OV-chip Kaart deployed by public transport companies including Trans Link Systems and Connexxion. System built and maintained by East West.	Public transport system throughout the Netherlands	Passengers use ID cards with passive re-writable tags. The system is based on the 'Octopus' RFID enabled e-ticketing in Hong Kong.	The system has provoked concern about privacy as users can be profiled while travelling or opt for a card that allows for anonymous travelling – but is not as flexible. [34]	
Oyster Card deployed by Transport for London in partnership with the consortium TranSys	Public transport in London, UK	Contactless smartcard technology supplied by MIFARE. 16,500 remote readers installed to track cards that can be 'reloaded' via ticket offices, machines and online. [35]	Serious privacy concerns have emerged over the past few years. Passengers must surrender personal information to obtain an Oyster card. Statistics obtained under Freedom of Information legislation revealed that the Metropolitan police used powers to trace people's use of public transport only 7 times in 2004, but this jumped to 61 in just one month in 2006. [36]	Concern also emerged in 2006 about the security of the online system used by passengers to login to their Oyster accounts. It was claimed that it was far too easy for family members or friends to access the journey data of people with Oyster cards.[37] A significant discount was used to promote the Oyster option.

[34] RFID and identity management in everyday life. Scientific Technology Options Assessment. June 2007.
[35] http://mifare.net/showcases/ accessed September, 2007
[36] http://www.guardian.co.uk/crime/article/0,,1729998,00.html, accessed September, 2007
[37] http://www.theregister.co.uk/2006/02/20/oyster_security_flaws/ accessed September, 2007

Deployment	Location	System	Issues	Other observations
The Torino SI-PASS for Società Italiana Traforo Autostrade del Frejus	Public transport and highway tolls in Torino, Italy	A single contactless card that enables travel on public transport and road toll payment. Uses the ASK contactless smart card technology. Users get automatic access to toll roads, parking and transport.[38]	Customers surrender personal data when applying for the SI-PASS. It is not clear how personal data is linked to the journey information and in what circumstances the personal data is passed on to third parties. [39]	
Liber-T toll payment system owned by the Federation of French Motorway and Toll Facility Companies	Toll roads in France	RFID enabled cards installed in vehicles for entry to and exit from toll roads.	The system does collect information about subscribers' journeys but how this is linked to personal information is not known.[40]	
Verkehrsverbund Rhein-Ruhr (VRR) and Verkehrsverbund Rhein-Sieg (VRS)	Public transport in Germany	ASK contactless smart card technology.	The system does collect information about subscribers' journeys but how this is linked to personal information is not known.[41]	

[38] http://www.ask.fr/uk/news/news_article.php4?id=8 accessed September, 2007
[39] RFID and identity management in everyday life. Scientific Technology Options Assessment. June 2007.
[40] RFID and identity management in everyday life. Scientific Technology Options Assessment. June 2007.
[41] RFID and identity management in everyday life. Scientific Technology Options Assessment. June 2007.

3.4 The use of RFID systems to deter counterfeiting and improve traceability

Deployment	Location	System	Issues	Other observations
FIFA World Cup 2006	Germany	UHF Passive RFID chips used in tickets for the World Cup matches.	Controversy focused on lack of choice for consumers. It was also widely reported that fans had to apply by giving a name, address, nationality, supported team and bank details.	The system was condemned by the German organisation the Independent Center of Data Protection in Schleswig-Holstein.
RFID tracing of surgical material	Hospital settings	RFID tracking of surgical instruments and sponges to prevent errors during operations	Objects left in patients undergoing operations is estimated to cause around 50 deaths a year. Stanford University is pioneering research in this field.[42]	In June 2007 ClearCount Medical Solutions in the US announced that it had received clearance in the US to market its SmartSponge system of RFID enabled surgical sponges.[43]
Prescription tracking	Hospital setting – Jena University Hospital, Germany	Pilot project to track medication from hospital pharmacy to patients in intensive care using RFID tags to prevent dispensing errors	Information is stored on patients' wristbands.[44]	
Blood transfusion monitoring	San Raffaele Hospital, Milan	RFID projects designed to reduce errors in blood transfusion handling	80% of blood transfusion errors are due to bedside or labelling errors. Patient information is stored on wristbands.[45]	

[42] http://med.stanford.edu/news_releases/2006/july/sponge.html accessed September 2007.
[43] http://www.rfidjournal.com/article/articleview/3446/1/1/ accessed September 2007.
[44] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Section:11.2. 2007.
[45] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Section:11.3. 2007.

Deployment	Location	System	Issues	Other observations
Tissue sample tracking	North Middlesex Hospital, UK	RFID tags in a system designed by 3M are used to track tissue samples and reduce the error rate[46]		
RFID labelling of the pharmaceuticals Viagra and OxyContin	US	The pharma company Pfizer now puts RFID enabled tags on all shipments of Viagra and Purdue Pharma now RFID tag Oxycontin	It is often predicted that RFID take-up in the pharma industry is likely to be strong because of the risk of counterfeit products. Both of these drugs are among brands most often counterfeited.[47]	Pharma trade bodies strongly support the increased utilisation of RFID in the sector.

3.5 European Biometric Passports

Governments have been quick to identify RFID as a technology that can help improve security and aid in strategies for curbing international terrorism. And the deployment of RFID in passports is pivotal to this development as they can store personal information as well as biometric data in the form of iris attributes and fingerprints or both.

By their nature, however, e-passports must be secure and overcome a range of threats explored more fully in **chapter 5**. These include: clandestine scanning and tracking; skimming and cloning; eavesdropping; data-leakage; and cryptographic weakness.

RFID enabled biometric passports have already been issued in the USA where they have provoked widespread concern over the possibility that data may be covertly read in public places. In Europe key aims were set out in the Council Regulation 2252/2004/EC that laid down standards for security features and biometrics in passports issued by member states. This regulation does not apply to the identity cards that member states may also want to issue as a parallel measure. European developments include:

[46] The Electronic Tags that can Save Lives on Wards. Observer, June 24, 2007.
[47] http://www.rfidnews.org/library/2006/03/21/viagra-and-oxycontin-tagged-but-future-still-uncertain-for-rfid-in-pharma/ accessed September 2007.

- The introduction of biometric passports in the UK (one million issued by July 2006).

- The cracking of the encryption scheme designed to protect the flow of information between the Dutch biometric passport and the reader in July 2005.

The new French e-passport will enable passengers to travel to the USA without the need for a visa. [48]

3.6 Themes

The specific issues of privacy, security and health in relation to RFID are addressed in detail in **chapters 4,5 and 6**. There are, however, a number of themes that cut across several applications identified in the tables above. The following section examines those themes in relation to those applications before the general concepts of privacy, security and health are discussed in more depth in the following chapters.

3.6.1 Privacy

Some of the applications included in the above tables were described in the European Parliament Scientific Technology Options Assessment (STOA) report: RFID and Identity Management in Everyday Life published in June 2007.

Through studying a number of case studies of RFID consumer deployment, the authors described the concept of Identity Management (IM) which they define 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.' In other words, IM describes how much control an individual has over that information.[49]

Interestingly, the authors of the STOA report conclude that although RFID in retail dominates the current debate about privacy in relation to RFID, this is not the consumer environment where conflicts over identity management are likely to emerge. The authors say this is partly because RFID in retail is not yet widespread and therefore consumers can choose not to shop where RFID is deployed.

The authors argue, however, that the 'power balance goes more in the direction of the maintainer [of the RFID system]' in public transport systems as operators are much more likely to persuade consumers to: personalise their cards; track travel patterns; offer price differentiation; and, use the information for direct marketing. RFID use in leisure settings was also found to be imposed on consumers without consent. The report found that the highest level of 'force' is evident with the introduction of RFID passports as citizens must comply with new initiatives (see European Biometric Passports in 3.5 above).

Overall, the report found that a more comprehensive survey would need to be undertaken to draw definite conclusions, the evidence shows that: 'relative to the scale of implementation, few Identity Management issues actually occur since both consumers and operators of the RFID systems 'perceive RFID merely as an electronic key or wallet.' The report describes two reasons why this may be the case. Firstly, in all of the cases the report examined it was clear who had to comply with data protection rules. Secondly, many of the deployed systems were small and ran in parallel to 'legacy' (non-RFID) systems.

The STOA report argues that this situation may change over time because consumers may be forced to use RFID systems and therefore maintainers will find it easier to analyse data on the whole user level. Additionally, different RFID systems may be connected making it much easier for operators to profile consumers (this issue is explored in much more detail in **chapter 4)**.

3.6.2 Lack of consultation

The use of RFID in the METRO Group Future Store is one of the most controversial deployments in Europe. Although the use of RFID was widely advertised in the trade press prior to the launch, several sources report that consumers were not informed that loyalty cards would be RFID enabled. Furthermore, it was claimed that the technology employed to permanently disable the tags at the till was found to be

[48] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Page: 220.
[49] RFID and identity management in everyday life. Scientific Technology Options Assessment. June 2007.

unreliable raising fears that the tags could be tracked outside the store.[50] METRO has attempted to reassure consumers by issuing the following statement:

'The Smart Chip cannot be used by METRO Group outside of the store, as there is no longer a link to the database. At no point is a connection made to personal data via RFID in the context of the METRO Group Future Store Initiative.'[51]

The controversy surrounding the deployment of RFID by METRO in Germany can be contrasted with RFID system introduced by Marks & Spencer (clothing) in the UK and by BGN (books) in the Netherlands. Both operators consulted widely and took steps to disconnect item level information from personal information.

3.6.3 Information demands

Many consumer groups opposed the deployment of the 2006 FIFA World Cup RFID system stating that the amount of information demanded by FIFA was against German law. While the organisers claimed they consulted widely on the issue (with the German Ministry of the Interior and the European Commission for example) the ticketing arrangements provoked widespread controversy. The organisers justified the approach by saying that it had to deal with sensitive security issues and they wanted to defeat the black market and counterfeit sales. They also claimed that the RFID information would only be matched with the personal data collected at random and in suspicious cases.[52]

Again, this deployment reveals a conflict between consumer expectations and the operators' justification for choosing to implement the RFID solution in a way that clearly linked the RFID tag and personal information.

3.6.4 People tracking

Applications that track people at leisure venues and in other environments raise serious questions about privacy and choice. It is important to note that RFID makes people tracking possible in a number of ways and these application types can be deployed in covert ways. People tracking is often considered as one specific

[50] http://networks.silicon.com/lans/0,39024663,39118760,00.htm accessed September, 2007.
[51] Metro Group Statement. Position Paper: Data protection aspects of RFID deployment at METRO. February 14, 2007.
[52] http://www.theregister.co.uk/2005/02/08/world_cup_2006_big_brother_charges/ accessed September 2007.

application, yet the ability to trace the movement of people is made possible using other RFID consumer applications such as road toll systems and e-ticketing.

The Kidspotter child-tracking application was introduced in Legoland in March 2004. The system allows parents to track children using wristbands detected by location receivers which track movement. Parents are kept informed via mobile text message alerts.[53] Similar systems are used in other leisure venues and one covert system uses tags sown into bags that were given to visitors. This system is used to analyse visitor movements and flow.[54] Both these systems are designed to monitor the movement of people at specific locations.

But people tracking is also possible through journey tracking and this has provoked some of the fiercest criticism of consumer RFID applications. The Metropolitan Police in London frequently use the Oyster RFID system deployed by Transport for London to trace the movements of people within the transport network.

In response to concern about the jump in police requests for data on travel Transport for London released this statement: 'Transport for London complies fully with the Data Protection Act. Information on individual travel is kept for a maximum of eight weeks and is only used for customer service purposes, to check charges for particular journeys or for refund inquiries.'

As table 3.3 reveals, the Police used their power to look at this data more than 60 times in just one month in 2006. In response to press enquiries about this police access to passenger data Transport for London said:

"A very few authorised individuals can access this data and there is no bulk disclosure of personal data to third parties for any commercial purposes. There is no bulk disclosure of personal data to any law enforcement agency. If information is disclosed, it is always done so in accordance with the Data Protection Act after a case-by-case evaluation. Police requests must be made under Association of Chief Police Officers guidance."

---

[53] http://www.kidspotter.com/kidspotter_solutions.php accessed September 2007.

[54] RFID and identity management in everyday life. Scientific Technology Options Assessment. June 2007. Page: 75.

There is, however, no consensus about how the Data Protection Act can be interpreted in relation to an RFID system of this kind. This subject is explored in more detail in **chapter 4**.

3.6.5 Data access and control

There is some evidence to suggest that services that give consumers access to their own data collected through RFID deployment amount to marketing or public relations strategies rather than attempts to give consumers genuine control over their own information.

Transport for London's Oyster card system gives users easy internet access to view their own historical journey data. But doubts about the security of this data were voiced in 2006 when it was reported that it was too easy for friends and family members to 'snoop' on the owners of Oyster cards. Commenting on this issue the IT journal the Register said: 'Giving individuals access to their own journey data seems of doubtful utility, considering most of them will have a fair idea of where they've been, and you can probably view this feature as a marketing tool intended (as will be the case with respect to allowing individuals access to their National Identity Register entry) to give the user the erroneous impression that they are the ones controlling their own data.'[55]

The Exxon Mobil Speedpass enables consumers to pay for petrol and other retail items using a RFID enabled key. The system also allows consumers to access their own transaction data online and to receive receipts. In this case the European Parliament STOA report suggests that a potential privacy issue could arise if people use this online information to trace family members. While consumers can access their transaction data they have no real control over it. Instead, the Speedpass 'privacy policy' states that: 'Speedpass and its affiliates may disclose any of the information that we collect to affiliates and non-affiliated third parties …We may disclose the information whether you are a current customer or former customer.' Use of the Speedpass is deemed as an act of opting in to the privacy policy.[56]

[55] http://www.theregister.co.uk/2006/02/20/oyster_security_flaws/ accessed September, 2007
[56] RFID and identity management in everyday life. Scientific Technology Options Assessment. June 2007. Page 77.

3.7 Comment on issues related to specific applications

3.7.1 Stadium, school and campus management

The use of RFID in the FIFA world cup tickets has highlighted the issue of choice in the deployment of RFID for stadium ticketing and in other leisure settings. Consumers who want to purchase the tickets or visit specific attractions *must* comply with the RFID system. The STOA report also describes an RFID enabled supporters membership scheme for Reading Football Club in England. Describing this project the authors state: 'It seems that the loyalty of the supporter surpasses the will to remain completely anonymous, all for the sake of the game.'[57] The RFID provider at Reading FC is FortressGB and this company lists a range of other UK and European clients including: Aalesund FC, Leeds Rhinos, Liverpool FC, Maccabi Haifa, Norwich FC, Sanderfjord FK, Viking Stavanger FC, Arsenal FC, London Irish RFC, Manchester City FC, San Siro Stadium (Milan) and West Ham FC.

The company also offers a 'smart school solution' and 'smart campus solution' for colleges and universities using radio-frequency smartcards for pupils, students and staff. These allow access control, cashless cafeteria, 'reduced truancy' and management of access rights to the school's networks. The company lists five school or campus clients. [58]

3.7.2 RFID on pharmaceutical packaging

One application that is often used to illustrate how RFID can be used positively to help deter or defeat counterfeiting is through deployment of systems for the tracking of pharmaceuticals. Table 3.4 lists two examples. There is, however, a growing debate about how useful RFID will prove to be in this market as some sources argue that the uptake by pharmaceutical companies is much slower than predicted.

A recent analysis (May 2007) in the business technology magazine CIO argued that RFID technology has an unproven track-record in protecting against counterfeiting and while many pharmaceutical manufacturers are carrying out research into RFID, few have decided that it is the best way to ensure authentication. The article questions the assumption that tags make effective anti-counterfeiting devices and

[57] RFID and identity management in everyday life. Scientific Technology Options Assessment. June 2007. Page 65.

points out that some companies have found RFID systems to be unreliable in the pharmaceutical setting. Industry sources say that RFID systems can only authenticate the packaging - not the contents. One source argues that changing the rules that govern how legitimate drugs are distributed may be a more effective way to defeat counterfeit drugs than RFID technology.[59]

Perhaps most importantly from the consumers' point of view, the article cites those who question the assertion that RFID technology will allow consumers to verify pharmaceutical products as authentic. In reality, it is argued, an RFID tag on a product does not give individual consumers a new way to assess authenticity. Instead, it is argued that trust will remain the basis of the transaction between the pharmacist and the consumer even where tagged items are sold.

In 2004 the US Food and Drug Administration, one of the main advocates of RFID, predicted that the technology would be deployed at item level for all drugs at risk of counterfeiting by 2006 and at item level for all drugs in 2007. With deployment falling far short of these predictions, however, the FDA has abandoned its plan to set a target date for the industry in the USA to convert to RFID. Instead it now recommends that stakeholders work together to 'implement widespread use'.[60] [61]

Recent research has also found that RFID deployment by pharmaceutical companies is likely to be much slower than predicted by the FDA. In April this year Health Industry Insights surveyed 143 life sciences industry leaders and found that a lack of demonstrated return on investment (ROI) as the main 'roadblock' to RFID adoption. It found that fewer than 1 in 5 companies were even evaluating RFID and fewer still (15%) were planning any kind of deployment.[62]

---

[58] http://www.fortressgb.com/clients.cfm accessed September 2007.
[59] http://www.cio.com/article/print/108903
[60] http://www.rfidjournal.com/article/articleview/2420/1/1/ accessed September 2007.
[61] FDA counterfeit drug task force report. 2006 Update.
http://www.fda.gov/oc/initiatives/counterfeit/report6_06.html accessed September 2007.
[62] http://www.healthindustry-insights.com/HII/getdoc.jsp?containerId=prUS20653507 accessed September 2007.

4. Privacy

4.1 Introduction

> *"RFID is a means for identification. The identification can be of products, services or persons. In most cases, RFID-tags will be related to products. When however, a person is correlated to specific products by means of a token, an index or another pointer, the identified information becomes personal information (or information that enables the identification of a person). Due to the 'enabling' characteristics of RFID-tags – they can be used everywhere, in any situation for any purpose – the threat to privacy is a major concern, for the public, companies and governments alike (albeit for different reasons)."*

This observation by the Institute for Prospective Technological Studies[63] sums up the privacy concerns that exist regarding RFID. It is sometimes argued that privacy can be ensured through improved security of RFID systems. As we will see, however, these systems have inherent characteristics that mean privacy cannot be protected through security measures alone. As is explained in **chapter 3**, it is not only conceivable but likely that people living in London are already paying for items using an RFID enabled credit card on the same day that they travel using an RFID enabled travel card to a sports stadium where they gain entry using an RFID enabled season ticket or loyalty card. All of these applications carry their own privacy risks, but there is a fear that commercial agreements may mean that data of this kind is shared leading to a loss of privacy in unpredictable ways.

Survey evidence reveals that privacy is the dominant concern consumers have about RFID. The European online consultation in 2006 that gathered responses from more than 2000 stakeholders found that privacy was the headline issue for most. A study carried out by Capgemini found that Europeans put privacy issues 'at the top of the list, leaving no doubt that companies must address these concerns as they communicate with their customers about the technology.' As a result, several organisations (including the OECD) have concluded that consumer backlash is either

[63] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. 2007. Page 135.

inevitable or likely if adequate measures are not put in place to defend consumer privacy in an appropriate way.[64]

4.1.1 Benefits

In comparison with the other priority areas of 'security' and 'health' it is extremely difficult to assess whether RFID has potential benefits in relation to privacy. While several surveys have found that 'privacy' is the top concern among consumers regarding RFID, consumers have either not listed 'privacy' as a potential benefit or that question has not been asked.[65]

Surveys have found that consumers list 'better determination of identity' as a potential benefit. In this context it can be argued that RFID may be able to help protect privacy by making it more difficult for criminals or any other unauthorised person to access private information. This potential benefit is discussed in the next chapter on security. While it can also be argued that some of the applications examined in this report were deployed with the objective of improving consumer security, none of them appear to have been deployed with the aim of enhancing consumer privacy specifically.

4.2 Threats to privacy

Chapter 3 identified a range of issues and themes directly associated with examples of RFID consumer applications. Several of those fall within one or more of the privacy threats identified below.

4.2.1 People tracking and behaviour monitoring

People can be tracked using RFID through the monitoring of their journeys made using RFID enabled travel cards, tickets and loyalty cards. Examples cited in **chapter 3** reveal that this kind of tracking already occurs. But tracking can also take place when RFID tag numbers are linked in some way to personal information. In other words: 'it is possible to track the movements of this person by surveying the

[64] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. 2007. Section 7.
[65] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Page: 112

movement of the object for which the tag data are known.'[66] Data can be used to track a person's movement through a store and, theoretically, tagged items can be used to trace someone's movements in a wider geographical area.[67] [68] Furthermore, while monitoring can occur in real time, data can also be analysed to detect patterns of behaviour over time.

4.2.2 The aggregation of personal information

Another fear is that as RFID systems become widespread then this mesh of interconnected technology becomes capable of delivering detailed 'profiles' of people. In his paper RFID and Privacy: A Difficult Marriage?, Patrick Van Eecke states: 'Merging these fragmental information could basically create a quite complete profile for each individual about his private sphere or the social and cultural values he shares in society.'[69] Patrick Van Eecke is Counsel to the law firm DLA Piper and a specialist in legal issues of ecommerce, e-government and data protection. [70]

As the number of RFID systems grow then information may be used in unpredictable ways. For example, it may be able to deduce social links between people if they make similar journeys at similar times. An RFID system created for one purpose (as a payment method) may be used for another purpose such as social networking. The Institute for Prospective Technological Studies has suggested that the monitoring or detection of social networks 'may be especially interesting for intelligence agencies' who may attempt to detect criminal networks.'[71]

4.2.3 Unauthorised reading

Some surveys have found that the unauthorised reading of data stored on RFID tags is the top privacy concern for consumers[72]. Unauthorised reading means that

---

[66] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Page: 138.
[67] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Page 7.2
[68] Position Statement on the Use of RFID on Consumer Products. Nov 14, 2003. EFF.
[69] RFID and Privacy: A Difficult Marriage?. Journal of Computer, Media and Telecommunications law, 2005, nr. 3, 84-90. Patrick Van Eecke, Georgia Skouma.
[70] http://www.dlapiper.com/patrick_van_eecke/
[71] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Section: 7.5
[72] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Page: 133

confidentiality and security can be violated enabling a third party to obtain personal information. This issue is discussed in more detail in the next chapter on security.

4.2.4 Function creep

This occurs when the system is used for a purpose that was not originally intended or specified. For example, if an RFID enabled credit card is deployed to allow easier payment transactions, function creep will occur if the system is then used to profile individual consumers using information about what they buy. The authors of *A Report on the Surveillance Society* argue that the police demands for data collected as part of the Oyster card travel scheme in London is an example of 'function creep' that has already occurred. [73]

4.2.5 Sharing data with third parties

The report by the Institute for Prospective Technological Studies makes a distinction between 'closed' and 'open' RFID systems. Closed systems are confined to one function and that company or organisation uses the data for only one pre-defined purpose. The term 'open system' describes an application where the data may be shared.

'Keeping track of the collected data becomes more problematic in an open situation; relations may exist with third parties outside the system who use the information collected for other purposes. This in the end will lead to a complicated mix of intertwined systems in which it becomes increasingly difficult to disentangle the various purpose specifications of each of the systems and see whether they are in line with each other. Issues as "informed consent", "purpose specification", "use limitation" and the like will have become problematic.'[74]

4.2.6 Covert use

One of the most serious threats to consumer privacy is the covert use of RFID which can take place in an infinite number of ways. At one extreme a whole RFID application can be introduced without the knowledge of end users. Tags can be attached to, or embedded in, objects or documents and used to monitor movement or

[73] A Report on the Surveillance Society. For the information commissioner. Summary Report. September 2006. Edited by Kirstie Ball and David Murakami Wood.
[74] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Section: 7.6

use. The recent Scientific Technology Options Assessment report RFID and Identity Management described one covert RFID system deployed at a leisure park used tags sown into bags that were given to consumers. The data was then used to analyse visitor movements and flow. In this case no link was made between the data collected and personal information about the visitors but it does reveal how easy it is to deploy a covert system. [75]

RFID readers can also be hidden and have been successfully incorporated into flooring, retail shelving and doorways making it impossible for consumers to know whether the objects they are carrying are being monitored. [76]

4.3 Potential solutions

A detailed examination of the laws that protect consumers and how they are enforced in relation to RFID is beyond the scope of this report. This section will however summarise the most important themes from the consumers' perspective in relation to the possible strategies that exist to confront the threats to privacy: protection through the law, through self-regulation or through technical solutions.

4.3.1 The law

It is widely understood that the European Data Protection Directive, EU Directive 95/46/EC, is the 'cornerstone' of European law on data protection[77] and this is underpinned by eight principles that were set out in the OECD guidelines upon which the EU Directive was based.[78] These state, for example, that: data should be obtained by lawful and fair means and, where appropriate, with consent; any personal data collected should be relevant to the purposes for which they are to be used; and that data subjects have certain rights to access the data held.

[75] RFID and identity management in everyday life. Scientific Technology Options Assessment. June 2007. Page:75.
[76] RFID and Privacy: A Difficult Marriage?. Journal of Computer, Media and Telecommunications law, 2005, nr. 3, 84-90. Patrick Van Eecke, Georgia Skouma.
[77] RFID and Privacy: A Difficult Marriage?. Journal of Computer, Media and Telecommunications law, 2005, nr. 3, 84-90. Patrick Van Eecke, Georgia Skouma.
[78] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Paragraph: 7.8

While it is often argued that the existing directive provides adequate privacy protection in relation to RFID[79] there is still no consensus and a lack of clarity over exactly how the Directive will be applied in relation to RFID. Patrick Van Eecke (see **4.2.2**) argues that: 'If the technical deployment of RFID is rapidly evolving, its legal repercussions are not so obvious to implementers and the users of RFID technologies.' Likewise the Commission has pointed out: 'RFID devices raise fundamental issues on the scope of the data protection rules and the concept of personal data.'[80] This section will explore some of those themes in relation to the consumer interest.

4.3.1.1 When is data 'personal'?

The concept of 'personal data' is key to understanding why RFID technology has an impact on the notion of privacy. RFID systems identify objects but those objects may also directly or indirectly, intentionally or unintentionally identify people. The question about whether RFID does or does not represent a significant threat to privacy is inseparable from debate focused on the definition of 'personal data.' This section describes that debate and the significant lack of consensus.

As outlined in **chapter 3** Marks & Spencer deployed an item-level RFID application in 53 stores in the UK. The company consulted with privacy groups about the system and stated that the tags do not have batteries, are harmless, can be thrown away after purchase without any affect on a claim for a refund and are not scanned at the checkout. This system makes no link between the purchased item and the individual. [81]

At the other extreme, the data collected by the operators of the Oyster travel card deployed in London is clearly linked to personal data. Police are currently using this information to trace the movements of suspects.

These two examples reveal how the data captured via RFID systems vary and why there is confusion and debate about how the European Data Protection Directive 95/46/EC should be enforced in relation to RFID systems. Consultations with

[79] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Paragraph: 7.8
[80] COM(2007) 87 final

stakeholders have found that those representing commercial interests do not consider all RFID data to be related to a person and also disagree with the statement made by the Article 29 Working Party that personal data is 'any information relating to an identified or identifiable person.' [82]

In this context it is useful to turn to the UK Information Commissioner's Office technical guidelines on RFID implementation.

Those guidelines place RFID systems in three categories:

1. those where the tags store personal data;

2. those that do not store personal data but individuals are identified by the data stored; and,

3. those that do not store any data that can identify individuals.[83]

According to the UK Information Commissioner, the UK Data Protection Act 1998 applies in the first two categories but does *not* apply in the third. Others argue that, in reality, it is much harder to define an RFID system than these guidelines imply. For example, Patrick Van Eecke states: 'At the time of implementation of an RFID solution, it may not be immediately obvious whether there is a risk to affect personal information. Such a risk may occur, for example, where the solution is integrated or interacts with(in) a wider system. In other situations, RFID-identifiers may not be associated with personal information at the kick-off stage of the deployment. However, such a possibility may not be excluded in the future, given the solution's potential for upgrades or plans to enhance its interoperability with other systems.' [84]

A similar point is made in the recent German Federal Office for Information Security report *Security Aspects and Prospective Applications of RFID Systems:* 'Assuming that tags will remain in the possession of the same person over long periods of time,

---

[81] RFID and identity management in everyday life. Scientific Technology Options Assessment. June 2007. Page: 8.
[82] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Section: 7.8
[83] Information Commissioner. Data Protection Technical Guidance. Radio Frequency Identification. 09.08.06.
[84] RFID and Privacy: A Difficult Marriage?. Journal of Computer, Media and Telecommunications law, 2005, nr. 3, 84-90. Patrick Van Eecke, Georgia Skouma. Paragraph: 4.2

repeated reading of IDs (serial numbers) allows movement profiles (tracking) to be generated. This possibility becomes a threat to privacy, if and when RFID systems become a ubiquitous part of everyday life.' (see 'Security' for more on this).[85]

Hewlett Packard is involved in the development and implementation of RFID systems on behalf of clients. Its European and Middle East and Africa Customer Privacy Manager, Daniel Pradelles, states that the technology moves so fast that it does not make sense to make a distinction between personal and non-personal (or object only) data because systems can mutate or change in ways that mean the information they store can identify individuals.[86]

The National Institute of Standards and Technology in the US has published a comprehensive set of guidelines for securing RFID systems described in detail in section **7.4.4**. In those guidelines NIST makes the point that information gathered through RFID can become personally identifiable through *indirect inference*. It states that pieces of information that are not considered personally identifiable on their own may 'still uniquely identify a person when combined.' (see **7.4.4**)

The Article 29 Working Party has published further opinion on the concept of personal data[87] but this work is ongoing in relation to RFID. The opinion concluded by stating: 'The Working Party intends to contribute to a further analysis of the way in which data protection rules may impact on the use of RFIDs and of the possible need for additional measures that may be necessary in order to ensure a proper respect of data protection rights and interests in that context.'

The Commission is therefore still seeking a solution and assessing the need for additional safeguards to defend privacy. Part of this process also involves the RFID Expert Group that will assist in the drafting of the Commission's future RFID strategy.

Given the confusion that exists about the definition of 'personal data' it remains unclear how the European Data Protection Directive can be used to defend consumers. The evidence suggests, however, that the boundary between 'item data'

[85] Federal Office for Information Security. *Security Aspects and Prospective Applications of RFIDSystems.* 2004. Section: 7.6.2
[86] Interview. Daniel Pradelles. Hewlett Packard.
[87] Article 29 Data Protection Working Party Opinion 4/2007 on the concept of personal data. June 2007.

and 'personal' information may become increasingly blurred. This may happen when data harvested from RFID applications is shared between companies and organisations in particular. From the consumer's perspective, therefore, it is important that the concept of 'personal information' is not defined too narrowly. See **8.2.2** in **Recommendations**.

4.3.1.2 Transparency

Another issue where there is confusion involves the principle of 'consent' – should it be transparent to consumers that RFID systems are deployed? Again, there appears to be a lack of clarity and confusion about when consumers should be told and an inconsistent approach across the EU.

The Commission analysis of RFID states that the issue of consent is 'another major challenge' and notes that the Article 29 Working Party has stated that 'consent should be freely given, should be specific, should entail an indication of the individuals effective will, should be informed and should be unambiguous.' It is clearly the case however, that specific RFID applications are currently being deployed that do not comply with that Article 29 Working Party statement. The Commission's analysis bluntly concludes that: 'The practice of informed consent around RFID will have to be sorted out, especially in circumstances when third parties may use the data collected.'[88]

In this context the UK Information Commissioner again makes a distinction between systems that collect *personal data* and those that don't. Those guidelines state: 'In order to comply with the fair processing requirements of the Act, those collecting personal data with RFID will have to give notice of the presence of RFID tags on products and of readers, and explain the implications.'[89]

But there is no consensus on this point. Hewlett Packard is involved in the development and implementation of RFID systems on behalf of clients and does not support any covert introduction of RFID system irrespective of the data collected. As outlined above, its European privacy officer Daniel Pradelles states that the

[88] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Section: 7.8

[89] Information Commissioner. Data Protection Technical Guidance. Radio Frequency Identification. 09.08.06.

technology moves so fast that it does not make sense to make a distinction between personal and non-personal (or object only) data.[90]

Patrick Van Eecke stresses the need to look elsewhere for guidance about how the Directive should be applied in relation to RFID and he points to two sources. Firstly, he refers to rules detailed in the Resolution on Radio-Frequency Identification adopted in 2003 by the International Conference of Data Protection and Privacy Commissioners. Secondly, he cites further analysis of those rules in the Working Document on Data Protection issues related to RFID technology prepared by the Article 29 Data Protection Working Party.

When the Directive is assessed in the light of this guidance, he says, then there is a clear requirement that 'any use of RFIDs must be explicitly conveyed to data subjects' and that this requirement is even more relevant where RFID is used for tracking. Furthermore, data subjects should also be:

- Fully informed about the characteristics of the RFID technology (such as the type of information being collected).

- Made aware of their rights in relation to the deployment. For example (as is the case with any other data processing system) they should always be entitled to withdraw consent, access stored data *and be able to amend that data.*

According to Patrick Van Eecke's analysis, a further consequence of these rules is that: 'human "tracking" through RFID technology cannot be unlimited in time and space.' Furthermore: 'A constituent of this principle is that the data subject is and must remain the sole owner and *de facto* controller of his personal data.'

It is clear that at least some RFID deployments do not comply with this assessment. For example, the covert system described in **chapter 3** above. But perhaps more importantly it is also likely that major deployments such as the Oyster card system in London do not comply with this interpretation of the Directive as not only is there a coupling between their personal information and the collected data, it is not made

[90] Interview. Daniel Pradelles. Hewlett Packard.

sufficiently clear to the data subjects that the RFID system is deployed and nor do the data subjects have control over their data.[91]

The UK Information Commissioner takes a different view of the Oyster card. Those guidelines state that the Oyster card collects information about journeys that is stored on a 'linked' database. It also states that people's movements should not be tracked 'without legitimate reason'. On the question of transparency, however, the guidelines only refer to those people *who are subject to tracking*: "Anyone who is subject to such tracking with RFID should be informed of this, and consent will be needed for any tracking that goes beyond what people would expect for a given legitimate purpose." In other words, these guidelines do not state that all Oyster users should be told about the RFID system.

Given the potential for RFID technology to be used to profile and track and for that data to be passed on to third parties, it is clear from this analysis that it is in the consumers' interest that the deployment of RFID systems should be made perfectly transparent. Furthermore, as Patrick Van Eeck points out, a corollary of this interpretation is that, as with any other data processing system, data subjects must also be aware of their rights to withdraw their consent and have control over their own data. This means that there is an obligation on system owners to provide the necessary information to allow for tag deactivation and to allow consumers to have meaningful access to control and amend that data collected through tracking.

4.3.1.3 Purpose-specification

Linked to the above theme on transparency is the need for the planned purpose of the deployment to be clearly defined. According to the rules described by Patrick Van Eecke a consequence of the principle of purpose-specification is that hidden deployments are, in fact, prohibited by the Directive because the rationale behind a planned deployment must be described accurately and in detail. Furthermore, as Patrick Van Eecke states:

'If processing of personal information collected through RFIDs may be extended to other purposes at a later stage of the system's roll-out, these additional purposes must be defined and made known to data subjects before the extension takes place.

[91] Interview. Patrick Van Eecke.

In the majority of these cases, data subjects need to re-confirm their consent to the extended processing activities planned.'[92]

4.3.1.4 Justification

The rule on justification of data processing has a number of ramifications in relation to RFID according to Patrick Van Eecke. Where a data processing technology entails major risks for human dignity and privacy, as is certainly the case with the deployment of some RFID systems, then alternative ways to meet the objectives of the project should be examined. This rule also covers the way RFID tags are used. For example, if tags are deployed at item level on retail shelves for stock control purposes, but are not de-activated after purchase, then this may not comply with the proportionality test.

4.3.2 Self regulation

Various initiatives such as the guidelines developed by the Centre for Democracy and Technology attempt to put in place mechanisms to defend the privacy of data subjects. For example, these state that consumers should be informed about when they have a choice about the use of RFID technology and should be informed about RFID deployment when information collected using that system is linked to personal information. These are described in **chapter 7.** Interestingly, according to Patrick Van Eecke the interpretation of the Directive described in his paper[93] places a legal obligation on those deploying RFID to seek information on the legal and standards-setting frameworks that exist before the system is put in place. Those that do not carry out a conformity assessment must not only ensure that the system complies with national laws on data protection but they must also closely monitor developments on standardisation 'especially in the area of security measures and PETs.'

4.3.3 Technology

The European Commission's pivotal statement on RFID, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, stresses the need for 'privacy by design'. 'Privacy and security should be built into the RFID information

[92] RFID and Privacy: A Difficult Marriage?. Journal of Computer, Media and Telecommunications law, 2005, nr. 3, 84-90. Patrick Van Eecke, Georgia Skouma. Section 4.2.

[93] RFID and Privacy: A Difficult Marriage?. Journal of Computer, Media and Telecommunications law, 2005, nr. 3, 84-90. Patrick Van Eecke, Georgia Skouma.

systems before their widespread deployment, rather than having to deal with it afterwards.' The importance of this statement is underlined by the response to that framework document drafted by the European Committee for Standardisation (CEN) described in **chapter 7.** In response to the concept of 'privacy-by-design' it stated: 'This presents some interesting technological challenges, because few RFID technologies have privacy by design in their original or current state-of-the-art solutions. The extent that privacy is designed-in varies between technologies, some of which have been well established for 15 years or more, and are in reasonably widespread use.'

CEN's proposal for a 'total system' approach to 'privacy-by-design' awaits a decision from the European Commission. Even so, other stakeholders have made suggestions for technical solutions to the privacy threats.

4.3.3.1 Privacy enhancing technologies (PETs)

The European Commission report RFID *Technologies: Emerging Issues, Challenges and Policy Options* suggests that all technical solutions for tackling privacy issues should be considered as privacy enhancing technologies (PETs). These minimise data collection of personal data and have the following functionalities:

- Anonymity: they enable consumers to get services without revealing their identities.
- Pseudo-identity: they enable consumers to get services by giving them pseudo-identities. Real identities are linked to the pseudo-identities in databases that can only be accessed by those authorised to do so.
- Unlinkability: information in databases for various services accessed by consumers are not linked.
- Unobservability: consumers can access services unnoticed by third parties.

While these functionalities may be of value, the report suggests that they don't necessarily address all RFID privacy issues as they address more generic privacy concerns in dealing with stored data. The report states that solutions that are more

directly related to RFID are those that attempt to keep control over the data flow. For example, through killer or blocker tags, those that allow an 'opt in' choice and those that allow consumers to permanently disable them by, for example, ripping off the antenna (clipped tags).[94] [95]

Patrick Van Eecke suggests that the involvement of PETs may become crucial if systems are to be fully compliant with the Directive on Data Protection. 'The tags imminent capacity to store various types of data and to transmit them over considerable distances to (an undetermined) number of users or databases reflects a realistic threat.' To avoid this, he suggests, relevant PETs should be promoted.[96] [97]

4.3.3.2 System intelligence

Other stakeholders argue that efforts to safeguard privacy should shift away from the readers and tags to the 'intelligence' at the level of the system software. Privacy threats, it is argued, arise when there is an automated link between the personal and object data. Similarly, the concept of choice suffers because consent for one individual transaction does not necessarily imply consent for a broader profile to be built through various RFID systems that may be meshed together.

The Chief Executive of Open Source Innovation, Humberto Moran, has described how his organisation has worked on the development of privacy-friendly software where the relationship between the personal and object data is never established. Furthermore, 'linking trails' such as timestamps and transaction IDs are blurred or removed. He states that his work has so far proven that most RFID applications can be based on this approach.[98] [99]

An analysis of the possible opportunities to safeguard privacy by focusing on system intelligence and the 'back office' is beyond the scope of this report. There may however, be scope for exploring how qualified third parties may have a role in

---

[94] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Page: 146.
[95] Privacy Enhancing Technologies for RFID. Dr Gunter Karjoth. RFID Workshops, Brussels, Session 1. May 16, 2006.
[96] RFID and Privacy: A Difficult Marriage?. Journal of Computer, Media and Telecommunications law, 2005, nr. 3, 84-90. Patrick Van Eecke, Georgia Skouma. Section: 4.2
[97] Interview. Patrick Van Eecke
[98] Humberto Moran. Speech. RFID Workshops, Brussels, May 16, 2006.
[99] Interview. Humberto Moran.

monitoring and auditing of system intelligence to assess for compliance with data protection and security standards. As explained in **4.3.2**, one interpretation of the Directive[100] finds that there is a legal obligation on those deploying RFID to seek information on the legal and standards-setting frameworks that exist before the system is put in place. Those that do not carry out a conformity assessment must not only ensure that the system complies with national laws on data protection but they must also closely monitor developments on standardisation 'especially in the area of security measures and PETs.' This third party auditing would clearly not deter criminal deployment, but it may be a mechanism that mainstream companies can adopt. From the consumers' perspective, this mechanism would be particularly helpful if the auditing principles applied were transparent and robust.

[100] RFID and Privacy: A Difficult Marriage?. Journal of Computer, Media and Telecommunications law, 2005, nr. 3, 84-90. Patrick Van Eecke, Georgia Skouma.

5. Security

5.1 Introduction

In its recent study the German Federal Office for Information Security noted that the integrity of RFID systems depend on the relationships between:

- The data and the tag. The tag must store a unique number.
- The tag and the tagged item. The tag must not be assigned to different items.
- The tag and the reader (the air interface). Authorised readers must have access while access from unauthorised readers is barred.

These relationships can be harmed in some way for several purposes: spying, deception, denial of service or protection of privacy. Attacks fall into the following broad categories:

- Eavesdropping on the communication between the tag and the reader. The larger the read range of the reader, the greater the risk.
- Unauthorised reading. This is one of the most serious threats because it is so easy without great outlay or technical difficulty.
- Unauthorised write access or falsification of contents. This attack is relevant where tags are rewritable and where the tag carries information other than the serial number and security information.
- Cloning and emulation. This can be carried out using a device that can emulate a tag or produce a new tag as a duplicate. This attack results in several tags circulating with the same identity.
- Detaching the tag. As a means of protecting privacy or as a malicious attack. Tags can also be swapped in the same way that price tags can be swapped with fraudulent intent.
- Destruction. Either maliciously or as part of the normal sales process. In the latter case, this is normally done using an electromagnetic field.

- Deactivation. This can occur with the unauthorised use of delete or kill commands.

- Blocking. This occurs when 'blocker tags' are used to prevent the normal communication between readers and target tags.

- Jamming. Prevents the normal communication between tags and readers. This is normally difficult as it requires a powerful transmitter.

- Shielding and frequency detuning. This breaks or influences the signal by putting a physical barrier between the tag and the reader.

- Relay attack. A device is placed between the reader and the tag making both think they are communicating with each other normally. In a retail environment this could be used to divert a charge to the wrong card. [101] [102] [103]

Other attacks are possible targeted at falsifying the reader ID in order to read tags and yet more aimed at other parts of the RFID system such as the 'back office.' The RFID back office refers to the database of information, the software used and the user interface (system management) maintained by the RFID operator.

Back-office attacks are possible using corrupted tags and a team from the Netherlands has shown that it is possible to do this using RFID worms and viruses. Furthermore, the drivers that are used by RFID readers to communicate with the middleware and the communication between the reader and the back office have been found to be vulnerable. Unauthorised access to the system management is the most basic, but one of the most significant threats to the back office.[104]

5.1.1 Benefits

There are clear security benefits associated with RFID technology. Consumers consistently refer to these benefits in surveys on attitudes to RFID. For example,

[101] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Page 8.3
[102] Federal Office for Information Security. Security Aspects and Prospective Applications of RFIDSystems. 2004.
[103] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Page 7.4.1
[104] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. 8.4

reliable surveys have found that consumers rate improved security as important when asked about potential benefits of RFID. The analysis of RFID carried out by the Institute for Prospective Technological Studies for the European Commission has also identified improved security and authenticity of prescription drugs as a benefit identified by some consumer protection groups. That analysis also found that RFID has the potential to reduce crime if deployed in the following application areas: libraries; parts for aircraft and other machinery; blood bags and samples; book retail; drugs prescriptions; cigarettes; post; and, other consumer packaged goods.

In addition to these potential benefits RFID may also clearly provide many consumer advantages but only if the technology can be proven to be more robust than existing forms of identification for payment, travel and access.

5.2 The risks to consumers

The German Federal Office for Information Security analysis *Security Aspects and Prospective Applications of RFID Systems* describes a range of threats posed by security attacks for the 'passive party' – the consumer or employee data subject. The report uses the term 'passive party' because this data subject has no control over the data stored on the tags. The authors note that privacy can be threatened by the active party (the RFID operator) and by third party attacks. This occurs in the case of the active party if data protection rules are broken and sensitive data is passed on.

This analysis concludes that the data privacy of the passive party is threatened because:

- Attackers have new ways to gain unauthorised access to data via eavesdropping.

- Both person-specific and potentially person-specific data may increasingly become targets for attack. Anonymised data may be deanonymised.

- "The resulting high degree of congruence between the virtual and the real world, which is a declared goal of using RFID systems, may give rise to the urge on the part of active parties as well as third parties (eg also state regulatory bodies) to perform evaluations which may not necessarily be in the

interest of the passive parties. **As the data become more easily accessible, the risk increases that databases will sooner or later be evaluated for purposes other than those originally intended, without the knowledge of the persons affected**."[105]

- RFID systems threaten location privacy through tracking and therefore any leakage of that data is a risk. Furthermore, the report notes that tracking more than one person allows contact profiles to be established. [106]

As described in **chapter 4** above, if and when tags become ubiquitous then there is a real possibility that movement profiles will be generated by the repeated reading of tags carried by people over long periods even if nothing more than the tag ID is transmitted. "The more tags there are in circulation, the better the chances that tracking can be carried out. Tracking more than one person also allows contact profiles to be established."[107]

The above analysis demonstrates again the difficulty there is in making a distinction between personally identifiable information and 'object' or non-personally identifiable information.

5.3 Risks in specific environments

The Institute for Prospective Technological Studies has examined the security risks of RFID in relation to five theoretical systems – four of those are consumer applications. Each application was assessed in relation to nine attack types including unauthorised modification of data, eavesdropping and jamming. The most significant threats are summarised below.

5.3.1 Healthcare

The unauthorised tampering of tag numbers on items such as medicines or blood bags in the healthcare or identity card settings is an obvious 'high impact' threat. While seen as a low probability, the potential harm justifies adequate measures to

[105] Federal Office for Information Security. Security Aspects and Prospective Applications of RFIDSystems. 2004. 7.6.1
[106] Federal Office for Information Security. Security Aspects and Prospective Applications of RFIDSystems. 2004. 7.6.2

prevent it. While the detachment or destruction of tags in this setting are possible, these are less significant problems. Other threats such as eavesdropping, blocking and jamming are possible but unrealistic in this setting.

5.3.2 Public transport

Again, the unauthorised modification of data is a significant threat because incorrect journey or charging information may be logged. Clear procedures should be put in place to deal with the accidental or deliberate destruction of tags. Invalid tickets may be formed through eavesdropping at gates or through the use of an illegal RFID reader. Blocking and jamming would probably not lead to free tickets but could 'severely frustrate (or even shut down) the public transport system'.

5.3.3 ID cards

The unauthorised modification of data is a severe threat 'therefore, in the design of the ID card, sophisticated measures are taken to reduce the risk of such an attack.' Eavesdropping is also a serious threat as, for example, a potential attacker may seek to identify passports of a specific nationality for terrorist purposes. Attackers may try to sabotage an ID system by blocking or jamming.

5.3.4 Smart shops

The unauthorised modification of data on tags attached to high value items may cause significant problems with pricing and extended warranties. Deactivation of tags by consumers is seen as desirable by some organisations while companies argue that tags left activated allows them to offer more services. The question as to whether consumers must opt in or opt out of RFID systems left active after purchase is still unresolved. Unauthorised people may be able to obtain private information through eavesdropping on a reader or by faking a legitimate reader ID. Blocking and jamming are techniques that could be used to frustrate readers and sabotage the use of the tags.[108]

---

[107] Federal Office for Information Security. Security Aspects and Prospective Applications of RFIDSystems. 2004. 7.6.2

[108] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. 8.10

5.4 'Back office' attacks

Overall, however, the German Federal Office for Information Security analysis concludes that attacks on the back office of RFID systems probably pose a greater threat to the passive party than those targeting the air interface. Obtained information 'makes it possible to create personalised movement and contact profiles, even when the data were originally in pseudonymised or anonymised form,' the report states. To put this security threat into perspective it adds: 'Compared to the use of mobile telephones, the use of RFID tags generates more precise data traces, because not only the geographical location, but also the concrete interaction with existing firms and infrastructures can be determined.'[109]

Attacks on the system backend are executed using techniques that are not unique to RFID systems and this is partly why RFID applications are probably more vulnerable to them – the techniques are already well established. The security threats are based on the fact that 'all intranet and internet connections run the risk of being subject to eavesdropping, and all computers connected to the internet are threatened by intrusion (hacking and cracking) and the introduction of software anomalies (mainly viruses and worms).'[110] While applications can be protected from these threats using the normal IT security precautions the German Federal Office for Information Security analysis adds this note of caution:

> *"One must, however, remember that, for the very first time, thanks to RFID systems, large portions of the physical world can be represented in the virtual world in near-real time. Databases are being generated from which, in particular, movement profiles of objects and information derivable from them can be extracted which previously were not available in the same density. This means that the motivation of attackers as well as the potential extent of the damage following successful attacks could attain a new order of magnitude."*[111]

[109] Federal Office for Information Security. Security Aspects and Prospective Applications of RFIDSystems. 2004. 7.6.2
[110] Federal Office for Information Security. Security Aspects and Prospective Applications of RFIDSystems. 2004. 7.4
[111] Federal Office for Information Security. Security Aspects and Prospective Applications of RFIDSystems. 2004. 7.4

5.5 Potential solutions

A detailed assessment of the numerous technical solutions that exist to counter the threats described above is beyond the scope of this report. They mainly fall within the categories of authentication, encryption, anti-collision protocols that are safe from eavesdropping, pseudonymisation and tag readout prevention. Counter-measures that can be deployed to help prevent the attacks described above are detailed in the German Federal Office for Information Security analysis.

That analysis, which took the form of a consultation with relevant experts, included an 'overall evaluation' of how relevant security questions are in the case of RFID applications. The following points emerged:

- At the present time, any threat caused by attacks on RFID systems is very minor compared to the technical difficulties involved in using these systems in practice.

- The threat potential might increase if RFID systems were employed on a massive scale. Their widespread use might trigger temptations to attack the systems or to evaluate the information in a way that compromises privacy.

- Wherever RFID systems have repercussions on physical safety (hospitals, safety-critical spare parts, personal identification), IT security is of particular importance.

- On the whole, privacy is threatened less by attacks on RFID systems than by their normal operation.

- Opinions differ regarding the additional risks to privacy caused by RFID; they range from zero risk (everything is already possible using existing systems) to very high risk (tracking through RFID as a new kind of surveillance).

- Security measures increase not only the fixed costs but also the variable costs of RFID systems. In the case of security procedures, too, costs can only be reduced through high-volume use.

It is worth noting here that this source was published in 2004, before mass deployment of consumer applications gathered pace. The second bullet is therefore an important consumer concern.

It remains to be seen how effective the technical solutions to security threats will be. Researchers in the Netherlands have already broken the security of e-passports developed in the Netherlands and have created the first RFID virus[112].

5.6 Non-technical solutions

From the consumers' perspective, however, the *non-technical solutions* will be just as important as the technical solutions described above. The German Federal Office for Information Security analysis constructed a range of 'fictive' RFID applications in use in 2010. These were not intended as forecasts but, instead, they were designed to make visible the possible risks of RFID technology in the future in order to 'motivate decision makers to analyse and protect information technology systems in companies and organisations in an appropriate way.'[113] They also demonstrate how security failures can emerge in unpredictable ways. For example, the fictive case studies suggest that in 2010:

- There may be widespread use of products that only accept replacement parts with correct authorisation codes. This benefits consumers by forcing cheap fake parts off the market but consumer rights to choice are eroded as people can only buy specific parts (such as ink for printers) from specific makers. The security issue here is that as tag use becomes ubiquitous manufacturers start to view them as essential for monitoring the age of parts in goods such as cars and parts accepted only from licensed manufacturers. Customers will not be able to verify these actions and tags may become traded on the black market in an attempt to legitimise counterfeit products or out-of-date products.

- The police make growing use of RFID logfiles to trace the activities of suspects. 'As a matter of course, data sets from service stations, toll bridges,

[112] Amsterdam University Press Release 'Digital vermin poses a real threat to RFID tags' 2006. http://www.rfidvirus.org/papers/press_release.pdf Accessed 9 October 2007.
[113] Federal Office for Information Security. Security Aspects and Prospective Applications of RFIDSystems. 2004. 10.1.1

etc. are used as part of terrorism defence.' Through changes in the law nearly all operators of RFID systems are obliged to store logfiles of all RFID transactions for a specific period and are obliged to make these available to the police when required. The development of the police information systems cannot keep pace with the technical RIFD developments and become less accessible to effective monitoring.

- Soccer fans are increasingly allocated RFID enabled tickets that allow automatic entry to stadiums. These tickets are linked to personal information on a database. All people can be traced at all times in the stadium and blocks of fans becoming conspicuous can be identified quickly and remotely without the need for confrontational person checks by the police. Readers monitoring the event may identify innocent ticket holders by mistake.[114]

5.7 Application-specific guidelines

Despite the fact that the mass deployment of consumer RFID applications is now underway, the development of non-technical solutions in the form of guidelines or regulations at a European level, has only just started. The cornerstone of European policy on RFID (*Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*) stresses the importance of 'security and privacy-by-design' where these two principles are built into RFID systems before they are deployed rather retrospectively. To this end the Commission has proposed 'the development of a set of application-specific guidelines (codes of conduct, good practices) by a core group of experts representing all parties.' [115]

The Commission also states that these security-related activities and initiatives will be conducted in line with the strategy for a Secure Information Society set out in COM(2006)251. In response to this the European Committee for Standardisation has drafted its proposals for European standardisation in the field of RFID described in detail in **chapter 7**.

[114] Federal Office for Information Security. Security Aspects and Prospective Applications of RFID Systems. 2004. 10

[115] Radio Frequency Identification (RFID) in Europe: steps towards a policy framework. COM(2007)96 final - 4.1

This strategy of application-specific guidance is supported elsewhere. Partly in response to the conclusions contained in the analysis *Security Aspects and Prospective Applications of RFID Systems* described above, The German Federal Office for Information Security (BSI) has launched the project *Technical Guidelines RFID.* Harald Kelter from the BSI Department of Scientific Foundations and Trends has stated that this approach will consider the interests of all parties including citizens, consumers, service providers and suppliers. Technical Guidelines for the use of contactless chip technology in four major application areas will be published later in 2007:

- Event ticketing.
- Ticketing in public transport.
- Near Field Communication (NFC)-based ticketing.
- Logistics.

Describing these guidelines Harald Kelter stated: 'These Technical Guidelines will contain technical advice on how to implement a system in a functional, secure and economical way. Potential threats for the system owner and the users are depicted, discussed and countered by appropriate security measures. Remaining risks will be described. All proposed solutions are based on standards or open specifications. Gaining the acceptance from all parties is the most important project goal. An open discussion and integration of all potential contributors is a cornerstone of our concept. Therefore the Technical Guidelines are currently being drafted in close co-operations with leading companies from the respective application areas.'

He said the drafts have already been discussed in dedicated expert workshops where all relevant groups, including those critical of RFID, were present.[116]

[116] Interview. Harald Kelter.

6. Health

6.1 RFID in healthcare

This report (**chapter 1** and **chapter 3**) has described a range of examples where RFID is being used in the healthcare setting. The European Commission analysis of RFID Technologies also describes a range of applications in this sector.[117] These include applications that track hospital assets such as equipment but also items used in surgical theatres such as sponges. Other applications include the tracking of medications from hospital pharmacies to patients; tracking of patients; and, blood transfusion monitoring. Given the potential benefits RFID use in this setting is likely to expand dramatically and it has been proposed, for example, that European citizens carry an RFID enabled health card that contains relevant medical information such as blood group and details of any allergies. [118]

6.2 Potential risks

The consequences of any loss of privacy through any breach of security in the healthcare setting are probably more serious than in most other application areas. Although considered a low probability, the unauthorized tampering with RFID tag information or other successful attacks on RFID tagged blood samples or medication or on many other RFID enabled systems may result in serious injury or death. The need for robust security measures to counter potential attacks is obvious.

6.3 RFID and health

Concerns have also been raised about the potential health impact of electromagnetic fields on health generally wherever RFID systems are deployed. Limits on exposure to electromagnetic fields (EMF) are published by various national and international regulatory agencies and standards bodies that have responsibility for EMF standards. A detailed assessment of those limits and standards is beyond the scope of this report.

---

[117] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Section 11

[118] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. Section 11

EPC Global has published its own Recommended Occupational Use Best Practices for Complying with Limits on Human Exposure to Electromagnetic Fields as a guide for system installers and users. These guidelines state that the main conclusion from the World Health Organisation and results from other scientific studies show that 'EMF exposures below the limits recommended in internationally adopted guidelines are not proven to have any known negative health effects.' [119]

Both the ANEC/BEUC report and the EPC Global Guidelines refer to the International Commission on Non-Ionizing Radiation Protection (ICNRP) exposure limits but the former points out that these limits do not take into account exposure to several sources in close proximity to the body. [120] Overall, it is unlikely that the tags on items or placed within documents pose any health risk. If there is a hazard then it is likely to be associated with 'always on' readers which are high powered and several may be used in one location such as a retail space.

Recent media reports have suggested that research has linked implanted RFID chips in animals with the development of cancer. This has prompted the Food and Drug Administration in the US to defend its decision to approve RFID chip implants in humans. It has been reported that the implant manufacturer VeriChip Corp, has already implanted 2,000 chips into humans for various applications. The company has denied any link has been established and other media reports have been critical of the scientific basis for the suggested link.[121] [122]

[119] GS1 EPC global. EPCglobal Recommended Occupational Use Best Practices for Complying with Limits on Human Exposure to Electromagnetic Fields (EMF). January 2007. Point 2. RFID and Health.
[120] Consumers' scenarios for a RFID policy. Joint ANEC/BEUC Comments on the Communication on Radio Frequency Identification (RFID) in Europe:steps towards a policy framework – COM(2007)96
[121] http://blog.wired.com/gadgets/2007/09/study-rfid-impl.html accessed September 2007
[122] http://news.yahoo.com/s/ap/20070908/ap_on_re_us/chipping_america_ii;_ylt=Ap5xxm.JhEuIbTkkixdxZqIjtBAF accessed September 2007

7. Standards and Best Practice Guidance

7.1 Introduction

The European Commission communication to the European Parliament - Radio Frequency Identification (RFID) in Europe: steps towards a policy framework[123] - has stressed how important it is for standards to keep pace with the speed of the emerging RFID market. It calls for the 'streamlined adoption of international standards and the harmonisation of regional standards' to ensure the smooth take up of services and interoperability[124]. Furthermore, the Commission has called upon the European standardisation organisations (ESOs) in co-operation with relevant industry forums and consortia, to:

- ensure that international and European standards meet European requirements (in relation to privacy, security, IPR and licensing issues in particular);
- to identify standardisation gaps; and,
- to provide the appropriate framework for the development of future RFID standards.

The EC, however, has not yet made any specific recommendations for standards designed to protect privacy or ensure security. Instead, the Commission has embarked on a two-year process to 'analyse the options' through discussions with stakeholders. In relation to security, privacy 'and the other policy issues posed by the shift from RFID to the 'Internet of Things' the Commission has decided that further detailed debate between stakeholders is necessary. Key to this process is the RFID Stakeholder Group.[125]

In its policy framework for RFID the Commission has stated that privacy and security should be built into RFID information systems *before* their widespread deployment. Importantly it has also stated that the interests of those deploying RFID systems and those who are subjected to them must be considered during the design of the

[123] COM(2007)96 final
[124] COM(2007)96 final – 3.5
[125] COM(2007)96 final – 4

system. 'As end users typically are not involved at the technology design stage, the Commission will support the development of a set of application-specific guidelines (code of conduct, good practices) by a core group of experts representing all parties,' the Commission states in its policy framework. To achieve this goal the Commission states that all security related activities and initiatives will be conducted in line with its strategy for a Secure Information Society set out in COM(2006)251.

The policy framework document states that the RFID stakeholder group will be 'invited to build visions and develop position papers that define user guidelines for RFID applications taking into account longer-term issues as well as economic and societal aspects of RFID technologies.'

On the issue of privacy the Commission says it will 'set out the principles that public authorities and other stakeholders should apply in respect to RFID usage'. It says it will also consider 'including appropriate provisions' for the amendment of the ePrivacy Directive and will also take into account input from the RFID Stakeholder Group, the Article 29 Data Protection Working Party and other relevant forums. 'On this basis the Commission will assess the need for further legislative steps to safeguard data protection and privacy,' it says.[126]

Further impetus to the development of standards in relation to RFID was given by the Commission's '2007 ICT Standardisation Work Programme' published in February 2007.[127] This reported that the Commission's internal consultation identified eight priority domains and within those it concluded that preference should be given to standardisation work on RFID (the other two issues identified by the commission as a priority for standardisation work were the Single Euro Payments Area and Privacy Enhancing Technologies.).

These European Commission statements reveal that, despite the widespread deployment of consumer RFID applications, the process of assessing the need for standards, guidelines and legislative change to address issues related to privacy and security (in relation to RFID) is only now being formulated. This section of the report will briefly describe the technical standards that exist or that are under development

[126] COM(2007)96 final – 4.1
[127] 2007 ICT Standardisation Work Programme. February 2007.

and, in more detail, will describe the various initiatives and positions adopted by specific stakeholders that are likely to shape future Commission strategies designed to defend privacy and security and the wider consumer interest.

7.2 The ICTSB Overview

The Information & Communications Technologies Standards Board is a collaborative group of organisations concerned with the standardisation and related activities in information and communications technologies. The European standardisation organisations (ESO's) including CEN (the European Committee for Standardisation), CENELEC (European Committee for Electrical Standardisation) and ETSI (European Telecommunications Standards Institute) are members.

The ICTSB has published an overview of standards activities in RFID and mapped these activities[128] in relation to the European Commission policy framework document. It has decided to review standards activities in relation to a range of applications on an ongoing basis as more RFID applications are developed and as it becomes aware of other standards initiatives.[129] [130] This issue will be debated further at an ICTSB workshop that will review the issue of stakeholder involvement on the development of standards and in relation to the Commission Expert Working Group in particular. This meeting will be open to ICTSB members and other stakeholders.

7.3 Technical standards.

The ICTSB overview and other recent European Commissioned reports on RFID reveal that various organisations involved in developing a range of general technical standards for RFID and also a range of other standards to be applied to specific applications. The picture is therefore complex and incomplete with approximately 60 initiatives on technical standards already identified.[131]

---

[128] http://www.ictsb.org/RFID_standardization.htm - accessed August, 2007.
[129] Radio Frequency Identification (RFID) in Europe: Standards aspects related to the policy framework, as well as other issues. June 14, 2007.
[130] John Ketchell. CEN Director of Pre-Standards. Personal Communication, Aug 30, 2007.
[131] http://www.ictsb.org/RFID_standardization.htm - accessed August, 2007.

A detailed examination and assessment of the technical standards that have or are being developed is therefore beyond the scope of this report. This section provides a brief overview of the organisations involved and their focus of development.

7.3.1 EPCglobal

This member-driven industry organisation is dominated by companies that deploy RFID systems. This is a deliberate strategy to ensure that the standardisation process is driven by supply chain process requirements. The objective of EPCglobal is to provide standards for attaching information to products through the use of, for example, the Electronic Product Code (EPC) which gives tagged items unique numbers and the Electronic Tag. Its focus of activity is in the development of core RFID standards such as those related to the management and operational protocols for readers.

EPCglobal defines its role in this way: 'By providing open standards for tags, readers, and middleware EPCglobal has enabled the creation of a standards based industry where tags applied in one country can pass through many different organisations to their final destination and the identity of the object understood and authenticated.'[132]

7.3.2 The International Organisations for Standardisation (ISO) in partnership with the International Electrotechnical Comission (IEC)

The network of national standards bodies from 148 countries that works under the ISO umbrella has jurisdiction over the frequency spectra used for RFID transmission. In conjunction with the IEC, the ISO has also published standards on the interface between readers and tags for various frequencies and other core standards issues such as standard methods of identifying tags.

7.3.3 The European Telecommunications Standardization Institute (ETSI)

The standards published by ETSI focus on the power levels emitted by the RFID readers. They aim to avoid interference between products and ensure that exposure to non-ionising electromagnetic radiation remain below recognised safety limits.

7.3.4 Application-specific standards

Other organisations are involved in the development of standards for specific applications. For example, CEN has proposed the development of standards for

Automotive Product Authentication & Tracking Using RFID and the Organisation for the Advancement of Structured Information Standards (OASIS) is involved in developing standards for the cross-frontier movement of goods.

7.4 Guidelines and other RFID standardisation initiatives

As outlined above, as well as putting the case for the 'streamlined adoption of international standards and the harmonisation of regional standards' the European Commission's policy framework document[133] supports the development of 'application-specific guidelines' in the form of codes of conduct or good practices. It also said that privacy and security should be built into RFID information systems at the design stage. Both in response to those European Commission statements and independently of them, various organisations have published recommendations for best practice guidelines or proposals for the development of standards to protect consumers. Some take the form of voluntary guidelines while other organisations have called for measures that are enforced through regulation.

7.4.1 EPCglobal

The full EPCglobal guidelines on the Electronic Product Code for Consumer Products is in **appendix 1**. EPCglobal states that as more consumer applications are deployed then 'it is important to address privacy concerns prompted by the current state of the technology while establishing principles for dealing with its evolution and implementation.' It also states that these guidelines are intended to complement compliance with national and international legislation and regulation that deals with consumer protection, privacy and related issues.

The guidelines state that consumers should:

- be given clear notice of the presence of EPC on products or packaging and should be informed about the use of EPC technology;

- be informed about the choices that are available to discard, remove or disable tags; and,

[132] http://www.epcglobalinc.org/standards/epcis/epcis_1_0-faq-20070427.pdf - accessed August, 2007.
[133] COM(2007)96 final

- have access to accurate information about EPC and its applications from companies that use EPC tags. The guidelines state that these companies should 'help consumers understand the technology and its benefits.'[134]

The guidelines have attracted severe criticism as EPCglobal has so far failed to introduce an enforcement mechanism to ensure compliance.

7.4.2 The Center for Democracy and Technology (CDT)

The CDT in the US works to promote democratic values and constitutional liberties in the digital age and seeks to build consensus among all stakeholders in the future of the internet and other new communications media. The CDT coordinated a year-long discussion and consultation process among a range of stakeholders in the US to develop a set of industry guidelines to address privacy concerns about RFID technology. They are targeted at companies that deploy private sector consumer RFID applications. A range of global companies including Eli Lilly and Company, IBM and Microsoft signed up to the guidelines representing industry interests while other signatories included the National Consumers League and the American Library Association.

The guidelines focus on the following areas:

- Notice. – 'Consumers should be provided with clear, conspicuous and concise notice when information, including location information, is collected through an RFID system and linked, or is intended by a commercial entity to become linked, to an individual's personal information either on the RFID tag itself or through a database.' They add that this notice should be given before the transaction is completed.

- Choice and Consent. – Consistent with the above provision, consumers should be clearly notified when they have a choice about the use of RFID technology and the use of information that can be linked to 'personally identifiable information.' The guidelines state that consumers should be informed about when they have a choice to remove or destroy tags. If they

[134] Guidelines on EPC for Consumer Products. Revised 2005. http://www.epcglobalinc.org/public/ppsc_guide/ accessed on August 24, 2007.

decide to do so then the consumers' ability to return an item, benefit from a warranty, or benefit from the protections of local law should not be compromised. Where information is linked to PII to enable the purchased device to function or the service to be delivered, then the consumer should be informed about the RFID tag but the consumer's consent about the use of the PII need not be obtained. However, if the information is linked to PII for other purposes then the consumer should be notified and given the opportunity to consent to such uses.

- Onward Transfer. – 'Wherever practicable' companies that share PII with other companies should make sure it is given a level of protection that is equal to or greater than that afforded by the company collecting the information.

- Access. – Consumers should be given reasonable access to PII when it is recorded on the tag. If a person is given an adverse decision related to the availability of a good or service, or the ability to obtain credit, based on the information linked to PII that person should have reasonable access to that information. Consumers should have reasonable access to PII, including location information, if it is cost effective and efficient. Access should be given by the company interfacing with the individual.

- Security. – Companies should exercise reasonable and appropriate efforts to secure RFID tags, readers and, whenever applicable, any corollary linked information from unauthorized reading, logging and tracking, including any network or database transmitting or containing that information and radio transmissions between readers and tags.

These guidelines are voluntary and there is no means of enforcement or sanction. CDT states that: 'The participants in the drafting process believe that widespread and voluntary adoption of these guidelines, combined with a major effort at consumer education, would dramatically improve the environment for the use of RFID.'

7.4.3 The Trans Atlantic Consumer Dialogue

TACD has issued a resolution on the use of RFID which takes the form of recommendations that it has made to EU and US governments. If adopted, some of

these would take the form of minimum standards or would require legislative change. These recommendations are not consistent with the EPCglobal guidelines or the CDT best practice guidance.

- Recommendation 2 states that governments should ensure that RFID implementation should comply with existing data protection and privacy legislation. But, as we have seen, there is no consensus on how this legislation should be applied (see **chapter 4**). Recommendation 2 also states that governments should require organisations developing and using RFID to follow a set of principles. These state that personal data should only be collected in an open and transparent way and that personal data should only be used for the specific purpose for which they were first collected. These principles also state that consumers should always have the right to delete data from tags and disable tags.

- Recommendation 3 states that consumers should always have the option to pay anonymously.

- Recommendation 8 states that organisations that use RFID should automatically de-activate tags after purchase while giving consumers the option to have tags re-activated.

The TACD resolution also calls upon organisations that are deploying RFID to:

- provide evidence of real consumer benefit;

- build security and privacy protection into the technology and its applications;

- explore RFID applications that enhance consumer privacy and decision-making; and,

- reject applications that have potentially anti-competitive effects.[135]

[135] http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=274 Accessed on August 24, 2007.

7.4.4 The National Institute of Standards and Technology (US)

In April 2007 the Computer Security Resource Center of NIST published Guidelines for Securing Radio Frequency Identification (RFID) Systems. These detail the security and privacy risks that must be identified and mitigated so that the benefits of RFID can be realised. The document also makes recommendations on best practice to help organisations: 'realise productivity improvements while safeguarding sensitive information and protecting the privacy of individuals.'

The document concludes that while RFID technology enables organisations to significantly change their business processes to increase efficiency and effectiveness, those changes and the complexity of the technology generate risks. In addition to the security risks described in the report the 'privacy risk' is identified as one of the four major risks associated with RFID deployment. The report defines the privacy risk in this way:

'Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. As people possess more tagged items and networked RFID readers become ever more prevalent, organizations may have the ability to combine and correlate data across applications to infer personal identity and location and build personal profiles in ways that increase the privacy risk.'

The report describes a set of recommended security practices for the initiation, planning and design, procurement, implementation, operations/maintenance and disposition phases of deployment. While it admits that 'no one-size-fits-all approach will work across implementations' the report says organizations can benefit from these general principles to help manage RFID risks to an acceptable level.

The Security Practices recommended by NIST are detailed in **Appendix 2**.

It is important to note that the NIST Guidelines document views privacy issues as interrelated with security considerations 'in a manner that one cannot be discussed without the other.' Like other organizations, NIST makes a clear distinction between

personally identifiable information (PII) and non-personally identifiable information.[136] NIST also describes how information can become PII through *indirect inference* – pieces of information that are not considered PII on their own, but which might 'still uniquely identify a person when combined.' NIST states that privacy laws govern the management of PII inferred through both direct and indirect means.

NIST also argues, however, that many people may still consider information that is not considered PII as 'personal'. For example, someone walking down the road may remain anonymous but readers may be able to identify the books they are carrying or the contents of their handbag. Some people may consider this an invasion of privacy. NIST concludes, therefore, that 'organizations may still choose to implement privacy controls voluntarily to safeguard information its customers, business partners, employees, and other stakeholders consider personal.'[137]

As detailed in **Appendix 2** the guidelines identify a number of general good practice principles that help in the defence of personal privacy. For example, the recommendations that organizations perform risk assessments and identify suitable technical standards. Additionally, the following principles identified by NIST are the most relevant to the protection of consumer privacy:

Practice 3 – organizations should establish an RFID privacy policy.

Practice 6 – establish an RFID security and privacy training programme for operators.

Practice 8 – include security and privacy considerations in RFID system investment and budget requests.

7.4.5 The European Committee for Standardisation (CEN)

In its response to the Commission's policy framework[138] and the 2007 ICT Standardisation Work Programme[139], the European Committee for Standardization

[136] NIST Special Publication 800-98. Guidelines for Securing Radio Frequency Identification (RFID) Systems. April 2007. Section 6-1.
[137] NIST Special Publication 800-98. Guidelines for Securing Radio Frequency Identification (RFID) Systems. April 2007. Section 6-8.
[138] COM(2007)96 final
[139] European Commission, 2007 ICT Standardisation Work Programme.

has made five proposals to the Commission[140] for European standardisation in the field of RFID. One of those will focus on RFID privacy and security[141]. The rationale for this proposal states that the Commission's concept of privacy-by-design (whereby privacy and security are built into RFID systems before they are deployed) 'presents some interesting technological challenges, because few RFID technologies have privacy by design in their original or current state-of-the-art solutions.' CEN argues that because some RFID systems have been in use for many years it will be impossible to 'retro-fit' enhancements to the particular components of some systems such as the RFID chip for example). CEN therefore argues that it should follow a 'total systems' approach to the challenges of privacy and security. By doing this it says: 'it should be able to enhance even well established technology to a higher level than is possible from a basic implementation.' CEN adds: 'Within this constraint, privacy and security issues can be enhanced by adding features to some components in an RFID system, not necessarily focusing on the lowest cost component (the RFID chip), which probably has the most inflexible design constraint for backwards compatibility.'

In relation to privacy CEN intends to identify and explore all claimed threats to privacy and will provide reasoned engineering and scientific explanations to eliminate those that are impossible or improbable. The project will then identify the remaining 'probable' set of privacy threats including those that are illegal. CEN will then identify pre-existing solutions that can minimise or eliminate those threats to privacy and carry out a 'gap analysis' on systems to identify those parts that are incapable of supporting 'privacy-by-design' and will explore alternative solutions. The CEN proposal is for a similar process to be carried out in relation to security issues.[142]

Given the scope of this project CEN expects the formal vote on the draft standard to take place in 2009 and its publication at the end of that year. The work may fall under CEN's Information Society Standardisation System (ISSS) which is the name given to

[140] Gertjan Akker van den. Personal Correspondence. 24 August, 2007.
[141] European Committee for Standardization. Draft CEN proposals for European standardisation in the field of RFID. 2007-04-17
[142] Proposal 1: RFID Privacy and Security – Standardisation Issues.

CEN's ICT sector activities. The work would be carried out by the ISSS Data Protection and Privacy Workshop (WS/DPP).[143] [144]

CEN has also addressed the issue of RFID with the publication of the Network and Information Security Standards Report commissioned by CEN as part of CEN's ICT sector activity – Information Society Standardization System (ISSS). This report supports the objectives in COM(2006)251 Communication from The Commission to The Council, The European Parliament, The European Economic and Social Committee and the Committee of the Regions; A Strategy for a Secure Information Society – 'Dialogue, partnership and Empowerment.' The aim was to respond to COM(2006)251 by providing an overview of existing standards in the area of network and information security (NIS).[145] The report highlighted RFID as a new development that may have important implications for the development of information security. The report made two recommendations in relation to RFID:

- There is 'an urgent need for standardisation activities on active tags'; and,
- Privacy issues and traceability of the RFID tag users should be one of the main research issues for a successful RFID technology development.

[143] http://www.cen.eu/CENORM/BusinessDomains/businessdomains/isss/activity/wsdpp.asp - accessed on August, 2007.
[144] http://www.ictsb.org/RFID_standardization.htm - accessed August, 2007. ICTSB overview document, Excel summary.
[145] Network and Information Security Standards Report. May 2007. ICT Standards Board. http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/activity/nissg+report+table+of+content.asp accessed August 2007.

8. Recommendations

8.1 Privacy

Consumer organisations and other stakeholders have made several recommendations and published numerous guidelines on the protection of privacy in relation to RFID. Some of those, including the recommendations made by the Trans Atlantic Consumer Declaration are described in **Chapter 7**.

A number of initiatives such as the Article 29 Working Party and the Commission Expert Working Group on RFID have a remit to examine how current legislation should be interpreted to protect consumer privacy. The definition of 'personal data' is the focus of the debate but, as detailed above, a number of other issues remain to be resolved – in particular the issue of transparency. Until that work is complete it is clear that RFID systems will continue to be deployed in a context where the regulatory environment is opaque at best and may be working against the consumer interest. Given how advanced the deployment of consumer RFID applications has become it is remarkable how immature the regulatory response is.

That said, it is widely believed that a consensus has emerged which holds that the European Privacy Directive 'enables a proper treatment of privacy aspects related to RFID.'[146] Patrick Van Eecke states that: 'To the eyes of most privacy scholars, law practitioners and policy-making bodies, the legal framework to control the *excessive use or misuses* resulting from RFIDs is already in place'.[147] [148] The RFID developer Hewlett Packard agrees.[149] From the consumers' perspective, an important next step will be the debate over the precise definition of 'personal data' and how informed consent should be implemented. Just as importantly, there should also be a focus on enforcement.

It is perhaps too early to assess whether PETs or the other approaches described in section 4.3.3.1 can contribute significantly to curbing the privacy threats described. Most are still under development and it is difficult and perhaps impossible to predict

[146] RFID Technologies: Emerging Issues, Challenges and Policy Options. Institute for Prospective Technological Studies. EUR 227770 EN. 2007. 7.8
[147] Interview. Patrick Van Eecke.
[148] RFID and Privacy: A Difficult Marriage?. Journal of Computer, Media and Telecommunications law, 2005, nr. 3, 84-90. Patrick Van Eecke, Georgia Skouma. 5.0

whether consumers will be able to use them as they are intended. PETs can only function appropriately if RFID systems operate within a regulatory environment that guarantees transparency and consent.

ANEC may wish to consider the following points and recommendations on specific consumer rights. It would clearly be preferable to build agreement that these rights should be guaranteed by law and that other mechanisms (such as the development of a forum to draft application-specific *Technical Guidelines RFID* in Germany described in chapter 5) are used to construct the necessary application-specific guidelines and codes of conduct that are capable of defending the consumer interest in specific environments. These forums may be the best place to explore the introduction of suitable PETs.

8.1.1 Compliance with Data Protection Directive

The recent Communication from the Commission on the follow-up of the Work Programme for better implementation of the Data Protection Directive[150] raised the issue of erratic implementation in member states. It noted: 'One concern is respect for the requirement that data protection supervisory authorities act in complete independence and are endowed with sufficient powers and resources to exercise their tasks. These authorities are key building blocks in the system of protection conceived by the Directive, and any failure to ensure their independence and powers has a wide-ranging negative impact on the enforcement of the data protection legislation.' Despite the confusion that exists about terminology, there is evidence to indicate that some consumer RFID applications may not comply with the Directive. One potential line of investigation would be the examination of specific applications to assess their compliance with the Directive and to assess whether local data commissioners have failed to act.

8.1.2 Concept and definition of 'personal data'

As discussed in 4.3.1.1, without a clear definition of 'personal' data it remains unclear how the European Data Protection Directive can be used to defend consumers. Yet the evidence suggests that the boundary between 'item data' and 'personal'

---

[149] Interview. Daniel Pradelles.

[150] Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive. COM(2007)87 final.

information may become increasingly blurred. This may happen when data harvested from RFID applications is shared between companies and organisations in particular. **From the consumer's perspective, therefore, it is important that the concept of 'personal information' is not defined too narrowly.**

Currently the TACD resolution calls for the implementation of RFID technology to comply with existing data protection and privacy legislation. On one hand there is broad agreement that the Data Protection Directive is adequate but, on the other hand, there is no consensus on the definition of 'personal data'. ANEC may wish to explore further whether all 'object data' should be defined as personal data as many organisations and individuals consider the distinction between 'personal' and 'object' data to be increasingly irrelevant. Furthermore, it is currently difficult to interpret the TACD resolution without a clear steer as to how 'personal data' is defined.

8.1.3 Transparency of systems

Clear notice should be given on RFID implementation in line with definition detailed by the Article 29 Working party that, where consent is legally required: 'consent should be freely given, should be specific, should entail an indication of the individuals effective will, should be informed and should be unambiguous.' Further ANEC may wish to recommend that the corollary of the transparency principle is that: use must be explicitly conveyed; data subjects must be fully informed; and data subjects must be aware of their rights over RFID-tagged objects including their right to deactivate the tags.

As detailed in section **4.3.1.2**, given the potential for RFID technology to be used to profile and track and for that data to be passed on to third parties, **it is clear from this analysis that it is in the consumers' interest that the deployment of RFID systems should be made perfectly transparent**. Furthermore, as Patrick Van Eeck points out, a corollary of this interpretation is that, as with any other data processing system, data subjects must also be aware of their rights to withdraw their consent and have control over their own data. This means that there is an obligation on system owners to provide the necessary information to allow for tag deactivation and to allow consumers to have meaningful access to control and amend that data collected through tracking.

8.1.4 Deployment of covert systems

Linked to the above theme on transparency is the need for the planned purpose of the deployment to be clearly defined. Until the issue of personal data has been defined – **ANEC may wish to consider supporting an absolute moratorium on the deployment of covert systems**. According to the rules described by Patrick Van Eecke a consequence of the principle of purpose-specification is that hidden deployments are, in fact, prohibited by the Directive because the rationale behind a planned deployment must be described accurately and in detail. Furthermore, as Patrick Van Eecke states:

'If processing of personal information collected through RFIDs may be extended to other purposes at a later stage of the system's roll-out, these additional purposes must be defined and made known to data subjects before the extension takes place. In the majority of these cases, data subjects need to re-confirm their consent to the extended processing activities planned.'[151]

8.1.5 Monitoring and auditing of compliance

As explained in **4.3.3.2** an analysis of the possible opportunities to safeguard privacy by focusing on system intelligence and the 'back office' is beyond the scope of this report. Even so, as outlined in **4.3.2** under one interpretation of the Directive[152] there is a legal obligation on those deploying RFID to seek information on the legal and standards-setting frameworks that exist before the system is put in place. Those that do not carry out a conformity assessment must not only ensure that the system complies with national laws on data protection but they must also closely monitor developments on standardisation 'especially in the area of security measures and PETs.' This third party auditing would clearly not deter criminal deployment, but it may be a mechanism that mainstream companies can adopt. From the consumers' perspective, this mechanism would be particularly helpful if the auditing principles applied were transparent and robust. **ANEC may want to explore further how qualified third parties can have a role in the mandatory monitoring and auditing of system intelligence to assess for compliance with data protection and**

[151] RFID and Privacy: A Difficult Marriage?. Journal of Computer, Media and Telecommunications law, 2005, nr. 3, 84-90. Patrick Van Eecke, Georgia Skouma. 4.2.

[152] RFID and Privacy: A Difficult Marriage?. Journal of Computer, Media and Telecommunications law, 2005, nr. 3, 84-90. Patrick Van Eecke, Georgia Skouma.

security standards that may emerge from the CEN proposals described in 7.4.5 or any other initiative.

The NIST **Guidelines** document for Securing Radio Frequency Identification Systems (described in **7.4.4** above) is one example of a set of practices that can be used as the basis for a third party audit of this type.

8.1.6 CEN proposals

Of all the initiatives to develop standards for RFID deployment in Europe, the CEN proposals described in 7.4.5 above are one of the most important. **ANEC may wish to monitor the commission's response to those proposals closely. One of the most alarming prospects from the consumers' point of view is the prospect that the consumer deployments already being used may shape the standards and guidelines that are eventually adopted.** Robust and effective measures to protect consumers should not be diverted because they are difficult to 'retro-fit' to existing RFID deployments.

8.2 Security

If the threats to the passive party (the data subject) identified in **chapter 5** are viewed in the context of the privacy threats described in **chapter 4** then the implications for consumers are alarming. As outlined in **chapter 4** many expert sources suggest that the distinction made between 'personal data' or 'data that can be referenced to persons' and 'non-personal data' (object data) may become increasingly redundant. Furthermore, it may become increasingly easy for the 'context' of data to be generated 'using a variety of variables which escapes the control of data protection due to the heterogeneity and large number of components involved.'[153] Given this background *Security Aspects and Prospective Applications of RFID Systems* concludes that:

'The requirement of data economy and the requirement that data be collected only for specified purposes are to be seen as essential criteria for the future preservation of the right to privacy."

[153] Federal Office for Information Security. Security Aspects and Prospective Applications of RFIDSystems. 2004. 10

The report's summary of the Federal German Data Protection Report is worth quoting in full:

'There are in principle no objections to the use of RFID systems, as long as their introduction takes place on a legal basis and while observing the data protection regulations: It is legitimate to use the new technical developments. However at the same time technical monitoring systems and a surveillance structure are being established which, once they are in place, could be used for quite different purposes and whose legal and data protection compliant use is ultimately no longer ascertainable. Here again it becomes apparent that the sum of useful and data protection compliant applications on the whole represents a potential threat to the basic right to determine information about one's self, which is not yet being perceived as such by those affected nor in society's political discussions.' [154]

In order to realise the opportunities of RFID and minimise the threats *Security Aspects and Prospective Applications of RFID Systems* recommends the implementation of the principles of modern data protection laws, data economy and 'the most rapid possible anonymisation or pseudonymisation of personal referenced data in RFID systems early in the design process and in market introduction.'[155] The development of the *German Technical Guidelines RFID* project is part of that process.

8.2.1 Assessment of application-specific guidelines

Given the Commission has stated that application-specific codes of conduct or guidelines are its preferred method to ensure security and privacy 'by design,' **ANEC should assess the application-specific guidelines being developed in Germany and described in Chapter 4**. While consumers may benefit from specific guarantees enshrined in law, application-specific guidelines may be the best way to protect consumers in specific circumstances. But important consumer questions remain about the development of 'application-specific' standards. For example:

- how is the consumer voice involved in their development?;

[154] Federal Office for Information Security. Security Aspects and Prospective Applications of RFIDSystems. 2004. 10.

[155] Federal Office for Information Security. Security Aspects and Prospective Applications of RFIDSystems. 2004. 10.

- are the guidelines mandatory in any way?; and,

- what, if any, sanctions will be put in place to make sure companies and organisations adopt these technical guidelines?

Given this context, the points made in **8.1.5** apply equally to security as they do to privacy. ANEC may want to explore further how qualified third parties can have a role in the monitoring and auditing of system intelligence to assess for compliance with data protection and security standards that may emerge from the CEN proposals described in **7.4.5** or other initiatives such as the German Technical Guidelines project. As explained in **4.3.2**, under one interpretation of the Directive[156] there is a legal obligation on those deploying RFID to seek information on the legal and standards-setting frameworks that exist before the system is put in place. Those that do not carry out a conformity assessment must not only ensure that the system complies with national laws on data protection but they must also closely monitor developments on standardisation 'especially in the area of security measures and PETs.'

8.2.2 Auditing of system design

Given that the cornerstone of European policy on RFID (Radio Frequency Identification (RFID) in Europe: steps towards a policy framework) stresses the importance of 'security and privacy-by-design' then **one issue ANEC may want to consider is mandatory third party auditing to ensure best practice at the design stage**.

8.3 Conclusion

As explained in **7.1** the European Commission has explained how important it is for standards to keep pace with the speed of the emerging RFID market and has called upon the European standardisation organisations (ESOs), in cooperation with relevant industry forums and consortia, to :

[156] RFID and Privacy: A Difficult Marriage?. Journal of Computer, Media and Telecommunications law, 2005, nr. 3, 84-90. Patrick Van Eecke, Georgia Skouma.

- ensure that international and European standards meet European requirements (in relation to privacy, security, IPR and licensing issues in particular);

- to identify standardisation gaps; and,

- to provide the appropriate framework for the development of future RFID standards.

It is clear from this analysis and from the above recommendations, however, that consumers are now in a vulnerable position due to confusion over the application of the Data Protection Directive and the slow regulatory response. Given the speed and scale of RFID application deployment the lack of consensus regarding transparency and the definition of 'personal' data is alarming. **It may be that robust standards are needed to make RFID deployment both secure and compatible with the Directive, but a first step is ensuring that that Directive is applied to RFID systems in a way that best defends the consumer interest.**

APPENDIX I

EPCGlobal Guidelines

Appendix I

EPCglobal Guidelines

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.[157]

[157] Guidelines on EPC for Consumer Products. Revised 2005. http://www.epcglobalinc.org/public/ppsc_guide/ accessed on August 24, 2007.

APPENDIX II

NIST – Recommended Practices

Appendix II

NIST – Recommended Practices

Number	Phase	Practice
1	Initiation	Perform a risk assessment to understand RFID threats, the likelihood that those threats will be realized, and the potential impact of realized threats on the value of the organization's assets.
2	Initiation	Establish an RFID usage policy that specifies what assets should be tagged, who is authorized to use RFID technology, and for what business purposes this authorization applies.
3	Initiation	Establish an RFID privacy policy.
4	Initiation	Establish HERF[158]/HERO[159]/HERP[160] policies if applicable.
5	Initiation	Enhance the organization's information security policy to account for the presence of RFID systems.
6	Initiation	Establish an RFID security and privacy training program for operators of the RFID system.
7	Planning and design	Identify the RFID standards with which the RFID system will comly
8	Planning and design	Include security and privacy considerations in RFID system investment and budget requests.
9	Planning and design	Conduct a site survey to determine the proper location of readers and other devices given a desired coverage area.
10	Planning and design	Determine approach to RF emissions control.
11	Planning and design	Identify an approach to securing network management traffic, using dedicated networks and encryption when feasible.

[158] Hazards of electromagnetic radiation to fuel.
[159] Hazards of electromagnetic radiation to ordnance.
[160] Hazards of electromagnetic radiation to people.

12	Planning and design	Design a network firewall between the RF subsystem and the enterprise network.
13	Planning and design	Develop RFID audit processes and procedures that identify the types of security relevant events that should be captured, and determine how audit records will be securely stored for subsequent analysis.
14	Planning and design	Develop a password management system for tags that support password-protected features.
15	Planning and design	Determine approach to tag memory protection, if applicable.
16	Procurement	Procure products that use FIPS-validated cryptographic modules.
17	Procurement	Procure products that are functionally capable of supporting the organization's security and privacy policy.
18	Procurment	Procure readers, middleware, and analytic systems that log security relevant events and forward them to a remote audit server.
19	Procurment	Procure readers and server platforms that support the selected approach to securing network management traffic.
20	Procurment	Procure readers and server platforms that support Network Time Protocol (NTP).
21	Procurment	Procure an auditing tool to automate the review of RFID audit data.
22	Procurment	Procure readers that can be upgraded easily in software or firmware.
23	Implementation	Harden all platforms supporting RFID components (e.g., middleware, analytic systems and database servers).
24	Implementation	Ensure that readers that support user authentication have strong, unique administrative passwords.
25	Implementation	Secure wireless interfaces on readers.
26	Implementation	Assign unique passwords to tags.

27	Implementation	Lock tag memory.
28	Implementation	Disable all insecure and unused management protocols on readers and enterprise subsystem components. Configure remaining management protocols for least privilege.
29	Implementation	Activate logging and direct log entries to a remote audit server.
30	Implementation	If applicable, initiate a HERF/HERO/HERP compliance program to include operator training, posting of notices, and application of labels to sensitive materials.
31	Operations and maintenance	Test and deploy software patches and upgrades on a regulare basis.
32	Operations and maintenance	Review audit logs frequently.
33	Operations and maintenance	Perform comprehensive RFID security assessments at regular and/or random intervals.
34	Operations and maintenance	Designate an individual or group to track RFID product vulnerabilities and wireless security trends.
35	Disposition	When disposing of tags, disable or destroy them.
36	Disposition	When disposing of an RFID component, ensure that its audit records are retained or destroyed as needed to meet legal or other requirements.
37	Disposition	Recycle retired tags.
33	Operations and maintenance	Perform comprehensive RFID security assessments at regular and/or random intervals.

APPENDIX III

GLOSSARY

Association Belge des Consummateurs - Association of Belgium Consumers

CDT - Center for Democracy and Technology

CEN - European Committee for Standardisation

CENELEC - European Committee for Electrical Standardisation

Edideco – Editores para a Defensa do Consumidor (Portugal

EDRI – European Digital Rights

EPCglobal – The industry body that leads the development for EPC standards

EPC - Electronic Product Code

ETSI - European Telecommunications Standards Institute

ESOs - European standardisation organisations

VZBV - Federation of German Consumer Organisations

Forbrukerradet - The Consumer Council of Norway

GS1 - an industry organisation which aims to improve efficiency of global supply and demand chains by developing standards and solutions and other products.

GS1 Germany - see GS1

ICTSB - Information & Communications Technologies Standards Board

ISO - The International Organisations for Standardisation

IEC - International Electrotechnical Comission

ISSS - CEN's Information Society Standardisation System

LogicaCMG - Is a major international information technology provider and consultancy headquartered in Europe.

NFC - Near Field Communication

NIST - The National Institute of Standards and Technology (US)

PII - personally identifiable information

PETs – Privacy Enhancing Technology

STOA - European Parliament Scientific Technology Options Assessment

TACD - Trans Atlantic Consumer Dialogue

WS/DPP - ISSS Data Protection and Privacy Workshop