EUROPEAN PARLIAMENT

Scientific Technology Options Assessment

S T O A

RFID and Identity Management in Everyday Life

Striking the balance between convenience, choice and control

STUDY

IPOL/A/STOA/2006-22 **PE 383.219**

This study is the outcome of the project "RFID and Identity Management" commissioned by STOA under Framework Contract IP/A/STOA/FWC/2005-28.

Only published in English.

Authors:

ETAG
European Technology Assessment Group:
Institute for Technology Assessment and Systems Analysis (ITAS), Karlsruhe
Danish Board of Technology (DBT), Copenhagen
Flemish Institute for Science and Technology Assessment (viWTA), Brussels
Parliamentary Office of Science and Technology (POST), London
Rathenau Institute, The Hague

Christian van't Hof
Rathenau Institute, the Netherlands

Administrator:

Theodoros Karapiperis
Policy Department A: Economic and Scientific Policy
DG Internal Policies
European Parliament
Rue Wiertz 60 - ATR 00K072
B-1047 Brussels
Tel: +32(0)2 28 43812
Fax: +32(0)2 28 44984
E-mail: Theodoros.Karapiperis@europarl.europa.eu

Manuscript completed in June 2007.

Preface

This is the final deliverable for the STOA project RFID & Identity Management, which was carried out by the Dutch Rathenau Institute as part of the European Technology Assessment Group (ETAG), the STOA framework contractor's network of scientific institutes. The purpose of this deliverable is to provide insight into real life experiences with Radio Frequency Identification (RFID), draw a future scenario, and formulate challenges for this rapidly emerging technology.

The empirical base of this project consists of 24 case studies on a variety of RFID systems. These case studies were performed by a team of researchers at the Rathenau Institute: Christian van 't Hof, Jessica Cornelissen, Sil Wijma, Eefje Vromans and Elisabetta El-Karymi. Methodological issues on these case studies are described in Deliverable 2 of this project (October 2006).

The empirical findings were discussed during three sessions. First at an expert meeting of Dutch experts: Bart Schermer (chairman of the RFID Platform Nederland), Henk Jaap Hoepman (researcher at the Radboud University Nijmegen), Koen Dupont (Consumentenbond). Second at a European Expert Meeting with Chandrika Nath (POST, UK), Christian Wernberg-Tougaard (Unysis, Denmark), Carsten Orwat (Institute for Technology Assessment and Systems Analysis, Germany), Robby Deboelpaep (Flemish Parliament). These expert meetings were organized and chaired by Christian van 't Hof, Rinie van Est and Eefje Vromans. Finally, the findings were discussed during a workshop at the European Parliament, organized by Theodoros Karapiperis of the STOA Secretariat and chaired by a Member of the European Parliament, Jorgo Chatzimerkakis.

This report was written by Christian van 't Hof of the Rathenau Institute, the Netherlands with help from Rinie van Est and Eefje Vromans during its conceptualization and reviewed by Chandrika Nath from POST, UK and Theodoros Karapiperis of the STOA Secretariat.

Executive summary

The STOA project “RFID & Identity Management” aims to provide insight into how Radio Frequency Identification is experienced by European citizens, draw a future scenario, and formulate challenges for this rapidly emerging technology. RFID systems consist of chips that communicate on radio frequency, providing an identity which unlocks information from databases within the system. Specific persons can be identified once the database can link the identity number of the chip to the person carrying it, as is the case with ID cards. Once the identity is confirmed, the system can respond for example by opening a door, providing information, performing a transaction, or any other kind of service. Meanwhile the service, as well as the combination of ID, place and time, is registered.

Until recently, RFID was mainly used for logistical purposes to identify cargo. Now it has entered the public space on a massive scale: public transport cards, the biometric passport, micro-payment systems, office ID tokens, customer loyalty cards, etcetera. What do these applications tell about their users and who profits from the information RFID systems generate? In order to study the societal impact of the identification of people through RFID, we introduce the concept Identity Management. In this context, Identity Management is understood as how a person, interacting with an information system, defines what is known and not known about him/her to others using the system and how this relates to the information known or not known to the persons maintaining the system. It goes beyond the juridical notion of protecting personal data and emphasises an active role for users determining their identity in the digital public space.

In our research, consisting of case studies, expert meetings and a literature review, we found that users generally perceive RFID as not more than an electronic key or wallet. To the maintainers/owners of the system however, it registers movements, spending, productivity, preferences, habits and so forth. This gives them a means of providing feedback according to these identities and control over their users. The use of these identities for maintainers, as well as the degree of free choice for users depends highly on the kind of RFID setting. First of all, retail. Although examples from this setting have been dominating the current privacy debate on RFID, we believe this is not the setting where the power struggle over Identity Management is currently taking place. One of the reasons is that item-level tagging has not taken off yet. Moreover: customers have a choice. If they do not like what their supermarket is doing, they can just go to another. This could also be the case with paying at the gas station, which does not seem to be much different from current pay systems. RFID systems for paying at toll roads has been suggested to enable police to track down people who exceed the speeding limits, but we found no such case in practice. The road as an RFID setting however is yet still in its infancy.

In public transport however, the power balance goes more in the direction of the maintainer: many operators urge users to personalize their card, providing them the opportunity for analyzing travel behaviour, price differentiation and direct marketing. Moreover, users have less of a choice as there are few alternatives. We also found a case in which the travel data served police investigation. In the leisure sector, one would not expect RFID to plays a major role in control, but it does: to track crowds without consent in amusement parks and to control crowds in football stadiums, while leaving little choice as people would just do anything to be part of their club. Tracking people can also have positives for users: being identified as a loyal customer and being rewarded accordingly.

The office environment also provided some interesting cases in which users have no other option than just to use the RFID chips they are offered, while the maintainer of the system could enforce time registration and anti theft measures on its users. In these cases the increased control over its users can be to their advantage as well.

Time registration can also be an instrument for workers to demonstrate how much they work overtime and evacuation management systems could save their lives. Finally, the highest level of force can be discerned at the RFID passport, as the maintainer of the environment is the state and the user a citizen. The question remains to which extent this RFID system will remain just a border control system or whether the data will also serve crime investigation.

Although a more comprehensive survey would need to be undertaken to draw definite conclusions, these first accounts suggest that, relative to the scale of implementation, few Identity Management issues actually occur. In general, both user and maintainer of the RFID settings perceive RFID merely as an electronic key or wallet. The reason for this can be twofold. First of all, in all the cases it is clear who maintains the data and needs to comply with the guidelines on data protection. Second, many systems currently only cover a small area of a specific setting and run parallel to legacy systems. The RFID systems therefore only disclose small fragments of their users' identity, limiting the maintainers' possibilities for control.

In the near future this could be different. Once RFID systems work exclusively with RFID it will become easier to aggregate and analyze the data on the level of the whole user population. Further, once different RFID systems might become connected to each other, or other technologies such as GSM, GPS, CCTV and the Internet, a much richer image of its users will appear. This opens up many opportunities for maintainers of the RFID settings to gain control over their users and governments to use RFID data for police investigation. Meanwhile, for the users it will become much less clear who is actually managing their identity in which setting, upsetting the power balance in the digital public space. This is not just an issue of protecting privacy or personal data, but it is more about securing personal freedom through the right balance between choice, convenience and control. We therefore formulate the following challenges ahead:

1. RFID users need to know what maintainers can and are allowed to do with RFID data.

2. RFID users should play a role in developing new RFID environments.

3. If personal data from different RFID settings are merged it should remain clear who is responsible form handling these data.

4. The Privacy Guidelines and the concepts of personal data and informational self-determination need to be reconsidered in the light of an increasingly interactive environment.

5. Governments should take a clear stance on whether RFID bulk data will be mined for investigation purposes.

Contents

1. Introduction

The STOA project “RFID & Identity Management” aims to provide insight into how Radio Frequency Identification is experienced by European citizens, draw a future scenario, and formulate challenges for this rapidly emerging technology. RFID systems consist of chips that communicate on radio frequency, providing an identity which unlocks information from databases within the system. Until recently, RFID was mainly used for logistical purposes to identify cargo. Now it has entered the public space on a massive scale: public transport cards, the biometric passport, micro-payment systems, office ID tokens, customer loyalty cards, etcetera. Therefore the time is ripe to see what actually happens in practice when RFID becomes a personal ID.

To provide an empirical base for this aim, we performed 24 case studies to describe the use of RFID technology in daily events: taking public transport, driving a car, going to work, shopping, leisure activities and crossing borders. The methodology for this research is described in Deliverable 2 of this project: “RFID & Identity Management in Everyday Life. Case studies from the frontline of developments towards Ambient Intelligence” (Van ‘t Hof & Cornelissen, October 2006). In the chapter, “How RFID data built up identity”, the cases are described according to their settings, while the technical details and sources are described in the appendix.

The future scenario and challenges are based on a number of expert meetings, at which the case studies served as an input. The time line for the possible scenario is between now and 2010, and the experts mainly extrapolated on current developments and technical and organizational possibilities. How RFID would relate to other technologies was also taken into account. However before setting the stage for the scenario with our findings, the first chapter will describe how RFID works and the issues raised when RFID is used to identify people.

2. When RFID becomes a personal ID

RFID systems consist of chips that communicate on radio frequency, providing an identity which unlocks information from databases within the system. Until recently, RFID was mainly used for logistical purposes to identify cargo. Now it has entered the public space on a massive scale: public transport cards, the biometric passport, micro-payment systems, office ID tokens, customer loyalty cards, etcetera. This chapter describes how the technology works, how it can be used to identify people, possible issues at hand when personal data generated by RFID systems are used and how personal data is protected by law.

2.1 How RFID works

An RFID chip contains a small chip and an antenna to communicate on radio frequency. The chip can be active (giving a signal powered by a battery) or passive (powered through induction in its antenna by the signal from the RFID reader). The data on the chip can be fixed or rewritable. When an RFID chip is scanned, it can provide specific information needed at that location, such as the identity of the owner or a deposit. More often, the chip just delivers a unique, fixed code that serves as a key to unlock information on the identity of the chip from a central database. The combination of a unique identity together with the place and time the identity is displayed, can serve to track movements through an RFID system.

Specific persons can be identified once the database can link the identity number of the chip to the person carrying it, as is the case with ID cards. Once the identity is confirmed, the system can respond by opening a door, providing information, performing a transaction, or any other kind of service. Meanwhile the service, as well as the combination of ID, place and time, is registered. This could be valuable information and there is a risk that ‘function creep’ could occur: although a system may be built for a specified function (such as securing access), once it is in place many opportunities open up for which it was not originally intended.

2.2 How citizens are protected by law

Citizens are protected against an unwanted function creep by a number of measures. In general, maintainers of RFID systems should inform their users of the kind of personal data gathered and its purpose, as well as allow them the opportunity to access and even manage their personal data. An overview of the legislative measures in place, their implementation and enforcement would in itself require a research project. For the purposes of this study it suffices to outline the principles which form the basis of the legislation relevant to European citizens and briefly summarize the relevant background. Every European nation has its own laws on the protection of personal data, but they are all national interpretations of the same European directive: the EC Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The principles underlying this directive are to a large extent similar to the Privacy Guidelines adopted in 1980 by the OECD as the so called "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" [www.oecd.org], which are in turn based on the US Fair Information Principles, developed by the US Department of Health Education and Welfare (HEW) in 1973 [www.hhs.gov].

In this study we do not focus on data protection and its legislation or enforcement, but rather on how people think RFID data should be managed in daily life.

We therefore summarise the principles underlying this legislation in order to analyse what their practical implications would be. Building on the work of Rotenberg (2003), Schermer (2007) summarises these principles as follows:

Collection Limitation Principle

This principle states that personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. Furthermore there should be limits to the collection of personal data.

Data Quality Principle

This principle states that any personal data collected should be relevant to the purposes for which they are to be used and when used should be accurate, complete, and kept up-to-date.

Purpose Specification Principle

This principle states that the purpose of the collection of any personal data should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of that purpose, or such others as are not incompatible with that purpose and as are specified on each occasion of change of purpose.

Use Limitation Principle

This principle states that personal data should not be disclosed, made available, or otherwise used for purposes other than those covered by the purpose specification.

Security Safeguards Principle

This principle states that any personal data collected and used should be protected by reasonable security measures to minimise the risk of unauthorised access, destruction, use, modification, or disclosure of personal data.

Openness Principle

This principle states that there should be a general policy of openness about developments, practices, and policies with respect to personal data. It further states that means should be readily available of establishing the existence and nature of personal data, the main purposes of their use, as well as the identity and residence of the data controller.

Individual Participation Principle

This principle acknowledges certain rights of data subjects with regard to their personal data. The first right a data subject has is the right to obtain confirmation from a data controller whether his information is being processed. Furthermore, the data subject has the right to have this information communicated to him within a reasonable time, in a reasonable manner, and in a form that is readily intelligible to him. If such information cannot be communicated, the data subject must be given reasons as to why it cannot be communicated, as well as the right to challenge this decision. Finally the data subject has the right to challenge data relating to him, and if successful have it erased, rectified, completed, or amended.

Accountability Principle

The final principle holds data controllers accountable for complying with measures that give effect to the above stated principles.

In this study we will refer to these principles as the Privacy Guidelines. Most European states have their own version of these guidelines laid down in laws, but the purpose remains the same: to enable a secure flow of personal information managed by others. One exception to this purpose is worth mentioning here. Germany is one of the few countries which puts the control over personal data much more in the hands of the user, rather than the maintainer of the information system through the principle of informational self-determination, or "informationelle Selbstbestimmung". Informational self-determination reflects Westin's description of privacy: “The right of the individual to decide what information about himself should be communicated to others and under what circumstances” (Westin, 1970).

The German Constitutional Court enforced this principle in the so-called Census Verdict, stating that:

> "If somebody cannot overlook with sufficient certainty which information concerning certain areas is known to his social environment (…) he can be significantly hindered from planning and deciding in a self-determined way. (…) If somebody has to reckon with the registration of his participation in a meeting or a citizens' initiative by the authorities and with the danger that risks for him are involved, he will perhaps not exercise his corresponding basic rights. (German Constitutional Law, Article 8, Paragraph 9)." (Krisch 2005: 9)

In this case data protection does not just involve protecting users from unwanted function creep by maintainers of RFID systems, but also from screening practiced by the authorities. From the point of view of this study, informational self-determination is a very interesting concept as it focuses on the user side of Identity Management, which we will define in the final section of this chapter.

2.3 What Europeans think: outcomes of the EC consultation on RFID

The question remains whether users are aware of the personal information gathered on them and whether they are able or even willing to control it as such. A survey by Cap Gemini, for example, 'RFID and Consumers' (2005), showed very few European citizens even know what RFID is, let alone have an opinion on it. Only 20% had ever heard of RFID and the respondents who could state an opinion needed much additional technical explanation. Another effort to obtain the public's view on RFID was undertaken by the European Commission during the summer of 2006. Through an open consultation the Commission got feedback from a total of 2190 'interested citizens'. Needless to say, this group cannot be seen a representative sample of the European population, as they need to know in advance what RFID is, have formed an opinion about it and have an interest in communicating this on-line (For example, only 8% of the respondents were female). Still, these interested citizens can be seen as members of the forefront of public opinion in Europe.

The results of the consultation draw a mixed picture. Some would agree RFID offers great potential for its users (42%), while some not (44%) and a slight majority states the public is not sufficiently informed about and aware of RFID (61%). Although the consultation also covered technical issues, such as standardization of the frequency spectrum, privacy turned out to be the respondents' biggest concern. They consider the solution to these problems to be more awareness raising and privacy enhancing technologies. In particular, the monitoring of employees through their RFID access cards raised considerable concerns (74%). Surprisingly the consultative questionnaire did not question participants about EC Directive 95/46, although it did mention other directives on more technical issues. Finally, a large majority (86%) supported the need for a "governance model that is built on transparent, fair and non-discriminatory international principles, free of commercial interest" for "the Internet of things". The final chapter of the report argues that the aforementioned data protection legislation, EC Directive 95/46/EC is not adequate enough to fulfil the requirements of such a governance model.

2.4 From privacy and data protection to Identity Management

European citizens increasingly use RFID in daily life, leaving personal data in the system, trusting the maintainer of the system to handle this information with care, protected to some extent by the law. As both the threats and benefits of this increase in the processing of personal data are becoming visible, the public image of RFID risks being caught in the middle of two opposing camps.

On one side, there are pressure groups, journalists and members of the public predicting a dark future with a 'Big Brother scenario' unfolding. Their key words are: spy chips, privacy and surveillance. On the other side, there are the business promoters painting colourful pictures of a bright future in which everything is smart, safe and automated. Their keywords: solutions, innovation, efficiency, return on investment and usability.

These words immediately set the stage for evaluating RFID, the first focusing on fear for loss of privacy, the second summing up solutions. In many cases, this urges policy makers to state we should take full advantage of the opportunities RFID offers, but not at the cost of privacy. Still, the technology in itself is neither good nor evil, and whether the future will be dark or bright will depend on how users and owners of RFID systems use these. And are opportunities always in conflict with privacy? In fact, what is privacy? In order to avoid taking one side of the debate, we introduce a more neutral and dynamic concept with regard to the storing and use of personal data: Identity Management.

Identity Management is an activity involving two actors: the owner/maintainer of the RFID environment and the user of this environment. From the maintainer's perspective, Identity Management can involve checking that a specific person (employee, traveller, citizen) logging into the system is who he states to be. Additionally, once the person is identified, all sorts of identity aspects can be attributed to this person: 'this employee is allowed here and currently at work' or 'this customer has paid and is a frequent visitor'. This activity also takes place from the side of the user, but then from their perspective: 'I am allowed here' or 'I am a loyal customer'. The identity being managed by both maintainer and user can be similar, but this is not always the case. Users could want to define their identity just as 'having access' or 'having paid', while the maintainer of the environment might attribute additional identity features to the person, either overtly or covertly. Sometimes a third party also enters the activity, such as direct marketing organizations looking for 'a potential customer for 'additional services' or police searching 'potential criminals' on the basis of travel profiles.

In summary, we define Identity Management 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 the next chapter we will describe how this concept works in practice: what do users do to define who they are within RFID settings, or are their identity solely managed by the maintainer of the setting?

3. How RFID data built up identity

In this chapter we will demonstrate how people currently use RFID in daily life. From their perspective, the RFID systems mainly function to provide access or perform transactions. We will also analyze what the maintainers of the environments are capable of doing and allowed to do with the data generated through these encounters. Having designed the settings and having real-time access to all data generated within it, maintainers/owners gain more insight into their users. Identities start to emerge on users, as the system registers movements, spending, productivity, preferences, habits and so forth. This gives the maintainers a means of providing feedback according to these identities and control over their users. Although perceived as such by its users, RFID chips are generally more than just electronic keys or wallets. What this 'more' can be depends on the setting.

We start with a setting from which the first controversial cases arose: shopping. Tagging groceries is also one of the examples dominating the current privacy debate within the policy discourse, while we believe this is not the setting with the most urgent Identity Management issues. One of the reasons is that item-level tagging has not taken off yet. Moreover: customers have a choice. If they do not like what their supermarket is doing, they can just go to another. To some extent this also counts in the next setting we analysed: paying at the pump, which does not seem to be much different from current pay systems. In the following settings, this freedom of choice is increasingly limited.

First in public transport, a setting where many operators urge users to personalize their RFID card, while many travellers don't have much choice but to use this system. In using their RFID card, travellers provide a broader image of their travel profiles. Next, in the leisure sector, one would not expect RFID to play a role in control, but it does: to track crowds without consent and to control crowds in football stadiums, while leaving little choice as people would just do anything to be part of their club. Then the office environment also provided some interesting cases in which users have no other option than just to use the RFID chips they are offered, but in these cases it can be to their advantage as well. Finally, the highest level of force can be discerned at the RFID passport, as the maintainer of the environment is the state and the user a citizen.

3.1 Shopping: tagged items and customer loyalty cards

In the short history of RFID, the one application that has perhaps stirred most controversy is tagging groceries. It started with the aim of gaining efficiency in the supply chain by replacing barcodes in crates, pallets and boxes with RFID tags, as happens in many logistic chains today. As soon as the price level of a tag dropped sufficiently, the next logical step seemed to be item-level tagging: an RFID chip to identify single products uniquely. With a unique code, the product could identify itself all the way from production, distribution, to sales and even beyond. Notorious future examples were smart refrigerators to tell whether the milk was due or intelligent washing machines to set the temperature according to the tags in clothes. But this did not happen. Item-level tagging in supermarkets displayed a very sensitive link in the chain: customers intent on taking their Identity Management into their own hands. Early examples come from the US, where CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) addressed the Identity Management issues concerned with item-level tagging at Wall Mart supermarkets. In Europe the German FoeBud (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs) triggered a controversy in the Metro Future Store when item-level tagging was combined with RFID customer loyalty cards.

The **Metro Future Store** is a supermarket of the German Metro Group where new technologies are tested in a real setting. RFID was first of all used in supply chain management. Cartons and pallets were tagged and readers installed at the exits and entrances of distributions centres and the warehouse. In 2003 the supermarket started experimenting with tagging groceries individually. RFID readers incorporated in shelves and connected to the central supply chain management system could then scan the tags of individual products. For the supermarket personnel, the main functions of item-level tagging are stock-control, checking for misplacement and quality control. In order to prevent the tags from being read by any third persons once the customer leaves the store, these tags are supposed to be disabled by a de-activator at the store exit.

For the customer, the so-called smart shelves also provide product information triggered by the item tag. Customers can go to an information terminal to retrieve more information on the book, by scanning the RFID chip inside the product. An in-store service to view or listen to trailers used tagged video and audio products. German law, however, demands that this occurs according to age limits set by the industry. The trailers can therefore only be activated with the RFID tag in the customer loyalty cards, checking whether the customer has reached the appropriate age to see or hear the trailer. At that very moment, the identity of the customer and the product were linked.

Once the RFID system was operational, the Metro Future Store invited customers to test it. About a year after the opening of the Future Store, FoeBud protested against RFID in the store. Main issue was the coupling of information about customers' age on the RFID enabled loyalty cards to video and audio products, when using the in-store viewing service. According to Albrecht von Truchseß, a Metro spokesman, this was done to meet German law on age restrictions. Still, according to the protesters, Metro did not inform its customers their loyalty card contained an RFID too. Besides the matter on RFID loyalty cards, several other possible applications were targeted by privacy advocates. One was on the possibility of RFID-enabled shopping carts to track customer movements. Also, the RFID tags should have been de-activated at the exit of the store, but the device malfunctioned on several occasions, leaving the tag open for intrusion outside the store.

In our correspondence with Metro, all of these allegations were refuted. Daniel Kitscha of the Corporate Communication department claimed customers were informed about the presence of RFID in their card orally and by a brochure. Further, the tagged shopping cart was also a fable: there was only one prototype cart with an RFID reader to scan for groceries, which was never actually used. Finally, he claims there was no negative public response towards RFID, not in their surveys and not on their customer hotlines.

Nevertheless, due to this controversy, the Future Store was forced to recall the loyalty cards and restore barcode systems. Some handbooks on RFID (e.g., Garfinkel, S. & Rosenberg, B.,2006 or Van Trier & Rietdijk, 2005) as well as many policy documents still mention Metro as one of the examples in which Identity Management went totally wrong. This image is hard to counter by any good intentions of the supermarket. For now, Metro remains determined to keep RFID technology in the supply chain. Mr Van Truchseß said. "A top priority is the use of this technology for tracking pallets and cases. And although we're still interested in testing the technology at the item level, this isn't a priority at the present."

We saw this precautious behaviour with two other retailers too. They did implement item-level tagging and took careful notice of the controversial aspect of connecting item-level tags to customer identity.

In spring 2006, **Marks & Spencer** implemented RFID item-level tagging using the 'Intelligent Label' for a trial in 53 stores. The RFID system keeps track of in-store inventory and ensures that a full range of sizes of any product is available to the customer.

During an earlier small-scale pilot, the 'Intelligent Label' was attached to the product alongside the pricing label and designed to be cut off and thrown away after purchase. In the extended trial, the tags were not used in the purchase-process, but only read throughout the supply chain and in the store for stock taking. Therefore the RFID inlay was embedded into a single label that also carries a barcode and a text informing customers: "Intelligent Label for stock control use".

During trial design and implementation, Marks & Spencer consulted privacy groups on possible privacy implications. These efforts led to positive reactions among sceptics. CASPIAN for instance acknowledged that Marks & Spencer has taken a socially responsible position. Despite these positive sentiments, CASPIAN denounced the trial in a press release, saying it does set a dangerous precedent by putting RFID tags in clothes. Another privacy watch group, spy.org, claims the message on the labels mentioning "Intelligent Label for stock control use", have recently been removed.

The retailer has opted for minimal customer-directed use of the tag, avoiding privacy issues, and has taken efforts to inform its customers. In the brochure about the RFID tags, Marks and Spencer states that the label does not have a battery, is harmless, can be thrown away after purchase without losing the right to refund or returning and will not be scanned at checkout. Instead, barcodes are scanned. This way, no link is made between the product and the customer, regardless of the method of payment. Our last retailer, **Selexyz Bookstore** also took care to strike the right balance between providing personalized product information and securing privacy. In this case the balance may be even more important, as their products do not consist of perishable goods but information.

Selexyz bookstore in Almere, the Netherlands mainly implemented an RFID system for efficiency reasons: make the supply chain more transparent, improve stock control and reduce labour costs. The system should also enrich customer experience and increase sales. Each of its 38,000 books carries a unique code, which can be read by mobile and stationary readers throughout the store. An employee, for example, places an unopened box with RFID tagged books into an RFID 'tunnel', which is equipped with a reader. This checks the tags against an electronic record of an advanced shipping notice forwarded earlier over the Internet by their supplier Centraal Boekhuis. If there is a discrepancy, the system automatically sends an alert to rectify the order. Checked-in books are placed on store shelves and other displays, with their exact location scanned by employees with handheld RFID scanners. This gives clerks and customers an instant look at a book's exact location as well as its availability.

Customers can use the RFID system to retrieve information on the whereabouts of a book through the information kiosks in the store. Selexyz also offers the possibility to place orders: when the requested book arrives the customer gets a notice by e-mail or text message.

When we bought a book at the store, we were surprised to find out it does not only contain an RFID chip, but also a barcode which is scanned at the moment of purchase. Having these two systems side by side does not appear to be very efficient but it is all meant to prevent controversy as described in the Metro case. The company took several other measures to prevent privacy issues. They proclaim not to link purchase information with specific customer information and when a book is bought, the chip is deactivated by store personnel.

However, it is not clear whether future applications of the RFID environment will be part of marketing strategies. For instance, a member of the management board of BGN mentioned the possibility of linking the tags to screens in the shop to display information or advertisements.

Naturally, it is not prohibited to use smart marketing techniques in your own store, but this method seems to be somewhat more invasive, with screens lighting up when a client picks a certain book from a shelf. Currently, the store has no such displays. In fact, the customer hardly notices the tags and only the leaflet on the RFID tags reminds of their presence.

All in all, there is not much going on with respect to Identity Management when we go shopping. This might be because it was in these settings that the first big controversies emerged, not only in Germany but also in the US, and therefore the sector has become very cautious about linking RFID to customer's identity. Our expert meetings concluded that item-level tagging in groceries will probably take another ten years to fully take off. Even then, supermarkets will remain cautious, as they have been warned in advance.

3.2 Driving a car: pay on the go

The first RFID tag we use for managing our identity on the road is the one in our car key. A small passive tag inside the key tells a reader near the lock it is really us trying to turn on the ignition and not someone with a copy of the metal key. We then drive our car to a gas station, with automated payments with RFID readers at the gas dispensers. We then take some toll roads, bridges and tunnels, where our active RFID transmitter behind the front window pays our toll while we drive. In all these accounts, RFID speeds up transactions and provides us with access, as it defines our identity as a paying customer. Meanwhile, the database of the maintainer of the RFID environments not only registers every transaction, but also where and when it took place. As described in the preceding chapter, this information can be used to profile our movements, which can be very useful for other purposes such as marketing or investigation - with or without our informed consent.

Currently the most widespread RFID application for paying at gas stations is the **ExxonMobile Speedpass**. Although this system is not yet implemented in Europe, more than 6 million Speedpass devices have been issued in the US at 8800 locations of Exxon- and Mobil-branded service stations. An additional 2 million Speedpass devices have been issued in Canada, Singapore and Japan for use at more than 1600 locations in those countries. The pass consists of a small black plastic barrel of about 2 cm which can be carried on a key ring. Readers are placed at the pump and in the stores. The RFID chip in the barrel carries a unique code which is connected to the holders credit card account.

The Speedpass is not just used to perform transactions. It has other purposes too, such as marketing and investigation. This is clearly stated in the 'Privacy Policy' and 'Terms of use', which users are assumed to have read and agreed upon when they subscribe to the pass.

The form states, for example: "Speedpass and its affiliates may disclose any of the information that we collect to affiliates and non-affiliated third parties as described below. We may disclose the information whether you are a current customer or a former customer." Among parties mentioned are security services, mortgage banking, direct marketing organizations and "any bidder for all or part of the Speedpass business". In practice this will mean the identity 'person paying at the pump', through a travel and consuming profile, could evolve into 'potential valuable customer for a motel, mortgage or groceries' or 'a potential link to a criminal network'.

Once a customer uses the Speedpass for the first time, this act is defined as opting in on this policy. The policy also offers an opt out, but if the information is already passed onto another organization, ExxonMobile does not have control or responsibility over it. Additionally, users can maintain their user profile on-line, for example, view their transactions and receive receipts on-line. An Identity Management issue arising here could be persons having access to each other's pass, for example, family, partners or employers, tracking each other.

In general, users of this setting have very little control over their Identity Management, while many other parties can build up an identity of them as they like.

Another Identity Management issue is when the Speedpass is not used by its rightful owner. Tags can be lost, stolen or even copied. Researchers at the Johns Hopkins University and RSA Laboratories, for example, succeeded in reading a Speedpass, cracking the code and reproducing another tag. In order to prevent misuse Speedpass monitors purchase patterns on devices, and looks for unusual behaviour that may signal unauthorized use. So, comparable to how credit companies operate, Speedpass analyses transactions in real-time for awkward profiles. If, for example, an unusual large purchase is made, or purchases occur at awkward locations, the transactions may be blocked and checked at the rightful owner of the pass.

Meanwhile, as these profiling analyses run real-time, one could wonder whether these profiles are only used to prevent fraud, and not to support direct marketing efforts on the basis of movements and buying behaviour. Still, accounts on its current use indicate otherwise. On on-line discussion groups, for example, some people express their fear of 'Big Brother scenarios', but none claim to actually encounter intrusive use of their personal data. Most of the discussion threads mainly evolve around practical matters: at which gas stations it can be used, how the system works and if it really saves time. We encountered similar reactions towards a European system, the French system **Liber-T**. Here users pay at the French toll roads, the Telepeage, with an RFID card. The badge gives drivers the possibility to enter and exit toll-routes through specially designed gates, without stopping and paying with cash or bankcards.

The Libert-T pass contains a passive rewritable RFID chip. Fixed data is identification of the bearer, the product (subscription type) and the tag. Modifiable data is observation data on tag status, last entry or exit point and historical data of last 16 entries or exits. By analyzing time and place of entering and exit, travel profiles emerge, which could be of use to the maintainer of this system or other organizations. What do its users think of this? We started a thread on this issue on a forum visited by Liber-T users. One visitor, MarK, draws a comparison between his bank and his Liber-T subscription. He states: "They know my address and my bank account (otherwise payment would not be possible). My bank knows this and there are a lot of other people and authorities that know this too."

He also mentions other ways in which personal information can be gathered, like using your credit card or your cell phone. Responses from other visitors at the forum confirm his view. Mariette 58, for example, thinks it is merely a "characteristic for this age of time". This argument appears to make up for the fact that "they get to know some things about you". Moreover, for MarK, being tracked actually gives him a feeling of safety in case he got lost on a French highway. Although it may also be used for marketing, we did not find any accounts of people who had actually experienced this.

All in all, these RFID applications mainly function to speed up transactions on the road. During its test phase ExxonMobile also tried active RFIDs in cars to speed up the transaction even more. Customers would then only have to fill up their tank, without even waving their card. But that did not work well. At the pump, there are just too many cars and readers in one reading area to distinguish them. Moreover, for most customers it made the transaction a bit too swift, giving them a sense of losing control over it. Active RFIDs however do work well at toll roads. Here an active RFID transponder sends out a signal stating who we are and facilitating a transaction to pay for the road we use. Users may have a feeling of loosing control over the transaction, but the advantage of not having to stop for the transaction probably outweighs this disadvantage and the system is currently used more frequently. Such is the case with the Italian **SI Pass**. We had previously encountered this case when we took the public transport in Turin, but, being promoted as a "card to open all doors" it also pays for toll roads.

Not by holding it at a reader when we enter a toll road, but as a key for an active RFID transponder right behind our windscreen. This transponder can reach a reader placed somewhere at the entrance gate of a toll road, performing a transaction while we continue driving. By inserting the SI Pass as a key to activate the device, we gain control over the communication, preventing covert transactions while we continue our trip.

Most companies who issue RFID payment cards seek to elaborate on the payment function. During the Olympic Games in Turin, the SI Pass could also be used to pay for parking, car rental and bike rental. The Speedpass is also not just to pay at the pump, we can also use it to pay for fast food and groceries at the ExxonMobile convenience stores. During its implementation phase, several trials were held to extend the reach of the Speedpass system even further. In 2001, ExxonMobile started trials at 450 McDonalds in the Chicago area and in 2003 with Stop & Shop supermarkets to see whether the pay system could be extended to fast food and groceries. According to Joe Giordano, vice president of systems and product development at Speedpass their customers expressed the need to use it at other "around-the-town, convenience oriented-type purchases". Still, these applications never passed the trial phase towards the broader public. It seems likely RFID systems do have their limits when it comes to payments, as is confirmed by our experiences in shopping. As in supermarkets, users have a choice not to use RFID as they can just go to another gas station or use other means of payment.

3.3 Public transport: urge for personalization, marketing and police investigation

In the public transport system, there is still some choice to either use or not to use RFID, but it is slightly more limited than in the preceding setting. Many public transport organizations in Europe are currently replacing paper-based tickets in plastic public transport cards with RFID chips. These passive and partly rewritable chips are being read on entering a bus, metro, train or ferry. Most cards work as a debit card: money needs to be put on it before travelling, either by putting cash into a machine or a bank transaction.

Some cards are more like credit cards: the costs of travelling are purchased by the company after the trip took place. Debit cards can therefore, in principle, be anonymous as the traveller has already paid, while for credit cards full personal details are needed in order to secure payments.

As long as the RFID system merely functions as a payment system, Identity Management is basically a matter of distinguishing between people who have paid or not, in some cases differentiating between one-off tickets, some forms of discount or seasonal tickets. For the user, it is just like any other payment system. For the maintainer however, many opportunities open up to monitor travelling behaviour. With paper tickets, identities connected to them were cut off at the exit. With RFID, the link remains through the unique code which is scanned on every entry or exit. Sometimes this identity can be anonymous, for example, "traveller X entering Bus 1 at 10.05, taking Bus 2 at 11.40." This provides information for building profiles, such as: "people going from A to B, also travel frequently between C and D". This can be valuable information for the marketing or the logistics department. In the following cases, cards are also linked to a specific name, address and bank account – opening up many opportunities for direct marketing or crime investigation.

Remarkable enough, we found relatively few cases in which this use of RFID triggered any debate. One such example is the **VRR/VRS Card** in North-Rhine-Westphalia, Germany. In 2003, the German Verkehrsverbund Rhein-Ruhr (VRR) and Verkehrsverbund Rhein-Sieg (VRS), was Europe's biggest case of implementing smart cards in trains and buses. The cooperation involved 54 different transport operators covering the whole region of North-Rhine-Westphalia, with a total population of 10.6 million inhabitants and handling 1.1 billion passengers per year.

The main advantage of the e-Tickets is that travellers no longer have to buy a ticket. A card reader which is placed in the bus or train registers where the cardholder gets on and off. At the end of the month the costumer gets the bill.

Privacy watch group FoeBud (see Section 3.1) warned on its website that the travel data could be used to monitor movements of people and make extensive use of personal data. Still, we found very few accounts of people or organizations who claimed that VRR/VRS actually uses the cards for purposes other than making transactions. VRS/VRS also explicitly claims that only the relevant data necessary for the validity of the card are stored on the chip: name, validity date and zone validity. No travel details or more personal data are stored. Customers can even choose if they want to pay with a personalized credit card or an anonymous debit card.

In the case of **SI Pass** in Italy, the maintainer of the RFID environment goes one step further in using personal data from travellers. This RFID card was introduced during the Olympics of 2006 to pay, amongst other things, for public transport. Mr Aliverti, Sales Director at Gruppo Torinese Transport, stated: "This new system will not only help us to combat fraud but also enable us to collect data so that we can offer customized fares and value-added services to travellers". When we acquired the application form from the SI Pass website, we could read the following statement:

> "Personal data is collected solely for employment related purposes or for use in connection with other such matters. Personal data shall be disclosed or made accessible to third parties exclusively for the aforementioned purposes. TURISMO TORINO hereby guarantees that anyone may request access to their personal data at any moment in order to up-date, change or supplement such data, and may oppose such data being used for the purposes given above."

This formulation provides the user with a certain level of Identity Management by gaining control over the use of their personal information, but, unlike the VRR/VRS Card, they have to do something for it. Still, in our research we did not encounter any negative responses to this use of data. Either the Italians agree their identity is managed as such, or they are just not aware of it. Meanwhile, London has got its **Oyster Card**, which demonstrated another Identity Management by a third party: police identifying criminals through travel profiles.

This RFID card was introduced in August 2004 and is currently used by 5 million people. The card serves to pay on buses, the subway and some trains. On purchasing the card, one has to fill in full personal details: name, address, phone number and e-mail address. This is apparently to fulfil the transaction in order to obtain the card. Yet it could also be used to track specific persons through the public transport system, as was claimed by The Guardian in January 2006. According to this British newspaper the police are very interested in using the journey data that is stored from travellers who use the Oyster card: a total of 61 requests were fulfilled in January 2006 alone. In a response, a spokesperson from Transport for London stated:

> "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. […] A very few authorized 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."

Indeed, data protection laws prevent personal data being handed over to anyone without the consent of the person involved, with the exemption of police investigations. Still, being seen as a potential criminal will not be the kind of identity some users of this environment would wish to have forced upon them. As demonstrated before, this can easily trigger fear for a 'Big Brother scenario'.

According to a weblog on the Oyster Card, yet another involvement of third parties may trigger Identity Management issues: conspicuous spouses using their partners' card to track their movements. The travel data is reported to be accessible through machines at stations and via a website, using only the registration number of the card. Yet whether this actually occurs on a large scale remains to be seen. All in all, these RFID systems do provide far more possibilities than just payment. Still, while they are employed on a large scale throughout Europe, few controversies have arisen. One case in the Netherlands, however, did result in a large national debate on Identity Management: the Dutch **OV-chipkaart**. This application is expected to be Europe's first nationwide, multimodal public transport card.

With this card travellers will be able to pay for buses, trains, subways, trams and ferries throughout the entire Netherlands. However, during its first implementation phase in 2005 and 2006, Identity Management issues triggered a national debate.

Owner and maintainer of this RFID environment is Trans Link Systems (TLS), a consortium of the five largest public transport companies in the Netherlands, representing 80% of the Dutch market. Travellers are represented by a whole host of organizations, such as two travellers' interests groups (Locov and Rover), the Dutch Data Protection Authority (College Bescherming Persoonsgegevens), a consumer organization (Consumentenbond) and a privacy watch group (Bits of Freedom). Even the Dutch Parliament got involved and discussed the issues at more than 20 meetings. The Dutch Minister for Transport assumed a position as a mediator between the maintainer of this RFID setting and organizations protecting the interests of its users. Due to the scale of both the system as well as the controversy, we analyzed this case quite thoroughly, using government documents, user evaluations from Trans Link Systems, publications from privacy organizations and pressure groups, newspaper articles and on-line newsgroups. We also got our own OV-chipkaart, to see how the system works and talk to other travellers.

The OV-chipkaart contains a passive rewritable RFID chip, which contains a unique number and a rewritable section to store information on travel time and uploaded value. Users can opt for an anonymous card or a personalized card. In case of a discount or season ticket a personalized card is obligatory. Buses and trams have readers placed at the doors, where people check in and out. Now and then a security officer with a hand-held reader goes through the bus or tram to check on fare dodging. At the train and subway stations travellers check in at the platform, holding their card near a reader in order to open a gate. At the start of the project, the total cost was estimated to be EUR 1.5 billion of which a small part would also be paid by local and national governments. A first large pilot was held in 2005 in the city of Rotterdam and the region South West. About 30,000 test travellers started using the card in the metro, bus and one rail track from the city to the beach. A second pilot is currently being held in Amsterdam.

In order to get an OV-chipkaart ourselves we needed to fill in an application form requesting many personal details: name, address, bank account, signature and a copy of our passport. This is quite surprising, as the card is a debit system and not a credit system. Money can be put on the card through machines placed at the stations and we did not see why identification was necessary. According to Trans Link Systems an anonymous card should also be available in time, but these were not offered yet. Another OV-chipkaart was sent automatically to us by the Dutch Railways, replacing a discount card we already possessed and for which we had already provided personal data.

The accompanying letter proclaimed that we were now “prepared for a new way of travelling”. It also stated that, once we waved our card the first time at the reader, this act would be interpreted as an opt in for the user agreement. For details on this agreement we were referred to a website. Although this action can be interpreted as service in order to make the transition smoother, it is also a subtle way of getting a personalized card more accepted than the anonymous card.

On the subway, the OV-chipkaart worked quite well. When holding our card near the TLS sign, the reader bleeped, displayed the current value of the card, stated we had checked in and wished us a pleasant journey. However, we did not have to use the card to open the gates. These were left open for people still using the paper-based tickets.

On the buses however many problems occurred. Sometimes we could not check in. The readers just gave a mysterious code: 707. Most of the bus drivers could not handle the malfunction, made some jokes about them and offered us a free ride. On other occasions, the readers did not sufficiently check us out, resulting in a payment for as far the bus would go. One of our researchers made 40 trips and reported more than half of the transactions failed. A bus driver, helping her out on many of these events, called her one night at home to inquire if everything was sorted out with the card. This account demonstrates the link between the card and the personal information in the database has not been sufficiently secured yet. Finally, at one occasion we were checked for fare dodging by a controller with a hand held reader. We then found out the data on the card also contains our date of birth – yet another bit of identity being managed by the maintainer without our consent.

According to an evaluation of the Rotterdam pilot many other people had difficulties with checking in and out of the buses. About 25% of the respondents claimed there are too many problems with malfunctioning of the system. Yet what this evaluation did not account for, was how the users felt about what was being done with the data they generated. It took the Dutch Data Protection Authority to bring the issue out in the open. Many national newspapers followed suit and a controversy was born. It revolved around two issues related to tracking people throughout the system: price differentiation and direct marketing. Moreover, central in these issues is the degree of free choice users have within the system to manage their identity.

From the start of the project, the Dutch Railways (NS) have been open about the fact they favour personalized cards and will use the data generated by travellers for marketing purposes, without specifying what kind of marketing. In February 2006, this led the Dutch Data Protection Authority (CBP) to warn the NS and other public transport corporations that their storage and use of travel information was not always legitimate. The CBP stated that, according to the Dutch law on protecting personal data, the aggregation of data has to be limited to the necessary data – in this case data for administering payments and not for marketing – and data can only be used once the person involved has agreed explicitly. In response the Dutch Railways said they interpret this law differently and claim they can store and use the data as they deem necessary and travellers still have a choice to travel anonymously. Still, personalized cards turned out to be temporarily cheaper than anonymous cards. Also, no *explicit* user consent is sought to the data policy of the NS – as we encountered with our discount card, simply using the system is seen as acceptance of the data policy. Finally, for discount cards and season ticket personal data is obligatory, as it is needed to automated billing.

A second issue concerns price differentiation. According to calculations of Locov, a consumer organization of public transport users, the RFID system will be used to enable unfair price differentiation. Costs of travelling in rush hours, for example, will rise by 10% while travelling outside these hours will cost 20% less. They consider this to be unreasonable, because most travellers have no choice but to travel during rush hours.

Another price differentiation they consider unacceptable is the difference in price depending on whether the user specifies his destination before travelling. Travellers entering the public transport can specify beforehand were they are going, or just check in and out. The price of the latter option is 10 to 100 percent higher, depending on the trip. Locov expects most travellers will specify their journey beforehand instead of just checking in and out, thus limiting the usability of the card.

Reactions on the Internet show that many people currently have doubts about the OV-chipkaart system. On the forum Tweakers.net, for example, some test travellers praise the system because it is easy to use as you just have to wave your card before a reader. However many others are afraid of the idea that more and more information about themselves and their whereabouts is registered. Some fear the police soon will get access to all travel data, or data will be used for all sorts of commercial purposes such as advertisements. Others worry about the security of the travel data, especially when this data will be accessible over the Internet. Some explicitly criticize the lack of choice: when using the public transport regularly – and therefore using a discount card or a subscription – they cannot travel anonymously. Finally some people are worried that the OV-chipkaart system is too complex for many people, especially the elderly. Due to these concerns, people are already searching for ways to undermine the system; for example, by exchanging cards with each other and thereby confusing the Identity Management schemes of the maintainer of this environment.

The Netherlands once had the ambition to be the first European country with a nationwide, multimodal RFID public transport system in 2007. One card should give travellers access to buses, trams, metros, trains and ferries throughout the whole country. However opinions on Identity Management still differ widely, hampering a system which once promised efficiency and usability. Currently, the debate in parliament has stopped due to elections, but according to the Minister for Transport, the Dutch Railways can move forward with implementing the system. Nevertheless, the national launch has now been postponed until 2009.

3.4 Leisure: privileged persons and tracked masses

The leisure sector turned out to be the most surprising in our research. Unlike the retail sector, we encountered many interesting stories on Identity Management, some being widely discussed in the media, while others only unfolded within the secure boundaries of the leisure setting. Just like the previous settings, RFID can be used to secure access and payments, yet it can also be used for more. In some cases, users can build up an identity of loyal customer, while in others they are tracked as masses of people without their informed consent, leaving little choice other than not using the system.

One case that has received some media attention is the **LEGOLAND KidSpotter** in Billund, Denmark. At the entrance of the park, parents can rent a wristband containing an active RFID for their children for EUR 3 a day. Throughout the 150,000 square meters park about 40 to 50 RFID readers have been placed. If the parents lose sight of their child, they can send an SMS message to the KidSpotter system. They will receive a return message stating the name of the park area and the map coordinate of their child's position in the park to within an accuracy of 3 meters.

This security function is the main reason for parents renting the wristband, countering the problem that about 1600 children get lost in the park annually. Identity Management in this case involves a combination of personal identity, place and phone number. Some newspapers hypothesized parents could also just drop off their children at the park and go shopping elsewhere, trusting their children would be confined within the area, but we are not sure this actually happens.

From the park's point of view, another Identity Management opportunity arises: tracking the flow of visitors through the park. The readers divide the park up into a number of areas and the database shows the number of people in each area and how many move from one area to another. This is valuable information, for instance for the marketing or catering departments. We contacted several spokespeople at LEGOLAND, but none of them was willing to give us more details on Identity Management issues in the park. One even claimed the system had been abandoned, but according to its provider, KidSpotter, it had not been. We therefore went to a theme park in the Netherlands which also tracks visitors with active RFID, but this time without them knowing.

The **Apenheul** is a zoo specialized in all kinds of apes and monkeys. An outstanding feature of the park is the opportunity for some kinds of monkeys to move freely through the crowd of visitors. Curious as they are, the monkeys often try to open visitors' bags in hope of a free lunch. The park therefore introduced the 'Monkey bag', a green bag with an extra clip lock which monkeys cannot open. The bag is obligatory, which is enforced by the receptionists providing the bag at the entrance of the park and a warning sign. Aside from this security reason for implementing the bag, the department of marketing added a marketing feature to the bag: scanning visitors' movements through the park through an active RFID sewn into the bag.

Currently about 200 of the 3000 bags are tagged. In order to provide a representative sample of visitors, the tagged bags are handed out at random, with 1 in 15 visitors tracked. A dataset of 90.000 readings provided the data for an analysis of visitor flows. If, for example, an area receives too few visitors, it presumably needs to be made more attractive. If the area receives the most visitors, it is probably a hit. Also, if visitors demonstrate a pattern of 'getting lost', for example, moving back and forth a lot between two areas, the directions need to be changed. Finally, the overview of visitor flows can detect congestion spots that need to be relieved.

According to several park hosts, visitors were informed about the presence of the tag during a pilot phase, but this policy has changed as people might then refuse the bags. Marketing manager Smit remarked afterwards that there is no reason to inform the visitors about the presence of the tag as it does not gather personal data, only anonymous movements. The Apenheul therefore complies with data protection laws. Jochem, the park host who recollects the bags at the exit, sometimes receives questions from visitors who discover the tag (it is tangible, about 4 to 10 cm on the inside of the bag). Visitors react surprised, according to Jochem, but never with much discontent.

This case touches upon the issue on what are personal data and the control customers should have over data retrieved from their movements. The Monkey Bag RFID has a marketing function: how do visitors move through the park and how can the flow of people be optimized? Visitors are being traced without informed consent. The tagged bag is provided without informing its user on the tractability. Moreover, the use of the monkey bag is obligatory. Visitors are given a bag at the entrance with a security argument "Monkeys move freely through the park and will try to steal your goods." Although legitimate in itself, this rule limits the free choice of the visitors not to use the bag.

Still, the visitors remain anonymous, are not traced real-time and do not suffer any consequences as a result of the data they provide. In that sense, the data retrieved cannot be seen as an identity that should be managed from a user perspective. Bert Smit, the marketing manager who leads the implementation, says it is exactly for this reason that his visitors tracking system complies with the law on protection of personal data.

Being profiled on movements can be experienced by some as invasive, while for others, it can also give a feeling of being privileged. Imagine 50,000 people in a building who will do just anything to manage their identity as being part of that group.

Add to this a maintainer of that building who has to identify those who are or are not paying, consuming, being loyal and behaving well - all this in a matter of just two hours. This is the case at the **Madejski Stadium** in Great Britain, which calls itself a "smart stadium" using among other ICT applications RFID tickets. The ticket system not only provides access to the stadium, but also serves as a customer loyalty, payment, crowd control, security and direct marketing application.

The RFID system was initially implemented at the Madejski Stadium in 2004 for security reasons: to limit access to valid ticket holders only and to control the number of people in the stadium. Tags are passive and used in plastic RFID cards (member cards and season tickets) and in one-off paper tickets. RFID readers in all the turnstiles administer access to valid ticket holders. Service personnel throughout the stadium carry pocket computers (PDAs) which are linked to the central database through a wireless network. This database can be accessed through entering the card number (not through RF!), providing the full identity of the card holder: ID number of the card or ticket, name of the carrier, time of entrance, status of ticket (e.g., access to which game and through which entrance), status of carrier (e.g., blocked card, watch-listed or black-listed person) and area and turnstile of entrance. Besides the RFID tickets, Closed-Circuit television (CCTV) is used to feed the information system. For example, taking pictures of supporters or to supervise the ground. Together with the ticketing system, the stadium knows exactly who is sitting at a certain seat. When a supporter is not following the rules or is having a dispute with personnel, the CCTV system can serve as proof and adequate action can be undertaken.

At our visit to Madejski stadium IT manager Mr G. Hanson, informed us that he function of the club card will be extended as a payment system, a so-called e-purse system. The e-purse is a debit card to pay, for example, for parking, public transport to the stadium and consumptions in the stadium. The system not only facilitates the transactions executed at the ground, but it also gives the stadium management insight in the expenditures of each supporter. This way they can see who are the club's 'big-spenders' and link this to their Customer Relation Management scheme. This means the stadium management is actively approaching its most loyal visitors, giving them special offers on their birthday or priority on popular matches. They can also be approached if, for example, they did not renew their season ticket or did not buy a new T-shirt that year.

A smart stadium indeed, but what do the fans think of this? During our visit, one member cardholder commented on the fact his whole history is retained and analyzed: "It is good that they can see who are the better supporters." Another mentioned: "It then helps to keep good fans in the club and get rid of troublemakers". A third regular mentioned: "Yes this is good so you get a benefit for attending more matches." Still, the fans do have one worry: the use of information by third parties. This should not be allowed according to them.

One person says they do not have any experience with non-football related marketing, but are not certain if this will remain like this: "But they probably also use personal information for marketing purposes. What can you do about it? You cannot prove it and you cannot change it". Another supporter states he would want to have a say in the applications for which personal information or the information obtained through the RFID system is used and that he would not want any third party being involved or benefiting from this. According to Mr Hanson, the information gained in the RFID environment is only used for in-house purposes. The stadium can and will not trade the information to third parties. For one thing, the Data Protection Statement of the registration procedure prohibits this, while other issues about privacy are covered by British Law.

This system, provided by Fortress Systems, is currently in use in many British and Norwegian football stadiums and we found accounts of comparable systems in other countries. Although these systems can be seen as being very invasive, taking full control over a person's Identity Management within a stadium setting, we did not encounter any public controversy. One controversy we did encounter in football was on a ticketing system which was even less intrusive about tracking people, but was just of a different league: the World Cup 2006 in Germany.

Football fans who attended a match at the World Cup in Germany got their ticket through the **FIFA World Cup ticketing Centre**. These tickets contained passive RFID tags in order to combat counterfeiting and to ensure only those with legitimate tickets could get in. On applying for a ticket one had to provide personal information: name, address, nationality, sex, date of birth, passport number, e-mail address (optional), telephone number (optional) and, possibly, also the club you are supporting. This information was stored in a database and linked to the ID-number on the chip. The chips were only scanned at the entrance of the stadium, and there were no scanners inside the stadium or anywhere else. The data, however, were shared with third parties such as security agencies, stadium operators and shipping providers if necessary, as was stated on the FIFA website. This led some privacy groups to accuse Germans football authorities of 'Big Brother tactics'. FoeBud, for example, stated that the RFID tags were being justified under false pretexts, like security reasons, and that it is unfair to insert this kind of technology in an item that much wanted by fans. On their website they stated:

> "What could be nicer: A top-event with millions of enthusiastic people who would do just about anything for their most beloved hobby. Add to this a September 11 heralding no end of "threat by terrorism", and you have all the justification you need for just about any measure to cut down on freedom rights as long as there is a sticker on it saying "security". And should the World Cup go past without any assaults you have every justification to afterwards call the whole "security-concept" a success, RFID in the tickets and all, and silence all the critics with a hearty salute: "Hey, all of you conspiracy theorists, hundreds of thousands of soccer fans didn't have any problems with RFID!"

Another group entering the debate was the German Data Protection Centre. They state on their website that supervision and security are two different things. Therefore, introducing technologies under the pretext of enhanced security cannot be done just like that. According to FIFA however personal data are processed in compliance with the Data Protection Legislation.

Moreover, compared to the other cases in football, this RFID system is not as much intrusive as it only tracks the user at one point: the access of the stadium. Still, it was the privacy watch groups who initiated the debate about this case. Our final case in the leisure sector did involve a much broader public debate, urging not just privacy groups, but also a whole host of journalists and even parliamentarians to participate. Not because people were tracked without knowing or in a disproportionate manner, but because of the way in which the RFID chips are carried: inside human flesh.

Barcelona (Spain) and Rotterdam (the Netherlands) both host a leisure branch called the **Baja Beachclub**. While the Barcelona club actually resides on the beach, the Rotterdam club creates a beach atmosphere in a concrete environment with all sorts of water attributes such as water scooters, palm trees and Jacuzzi. Personnel are dressed in swimwear. Next to the bar there is a VIP deck, where fancy drinks and snacks are served. This is the area for loyal customers who carry an RFID implant in their upper arm which serves as an access code and digital wallet to pay for drinks. The cost of the chip and the resulting membership is EUR 1000, while the club places a credit on the chip of EUR 1500 for drinks.

According to Conrad Chase, director of the Baja Beach Club Barcelona, the chip was introduced for two reasons. First, for the image of the nightclub, they wanted to offer their guests an original item. Second, to benefit from the latest most advanced technology, something that could offer convenience for both the nightclub as well as the carriers. His Dutch colleague Jo van Galen adds to this that the carriers regard the chip as a special gadget that supports the VIP treatment in a positive way. It is not just they do not have to show identification or have to handle money, but it is more the feeling of being an appreciated guest of the club.

The VeriChip was initially developed for medical purposes, to identify patients. It consists of a glass tube the size of a grain of rice containing a passive RFID with a single fixed code. It is implanted in the upper arm with a needle. Before implanting the chip the VIP signs a statement of free will. This statement also contains an acknowledgement that the chip and the information will remain property of the nightclub and the carrier can decide to have the chip removed any time and without former notice to the nightclub. When they go to the club, VIPs have their chip read at three moments: on entering the club, on entering the VIP deck and when paying for drinks. Club personnel read the chip with a portable reader which displays only the ID-number of the chip. This number is transmitted to the central computer and details of the customer are displayed on screens which can be accessed throughout the club. These details involve: name and photo of the carrier, balance on the chip and transaction history. The transaction history consists of transaction amount, time of transaction and bartender running the transaction. No information goes outside the club.

The club uses the system as an informal loyalty system, but the technology is not a key-instrument in this; it could also be done without this based on personal experiences with guests. Regulars and 'big-spenders' get offers like first options to limited tickets, invitations to special nights and Mr Van Galen even mentioned offering a airplane ticket to a Spanish guest. Guests regard this loyalty scheme as positive, according to our respondent. The Rotterdam club currently has 70 people who carry the chip. Manager Jo van Galen explains that the number will not be increased, because it has to remain an exclusive thing.

Interestingly, most of the chip carriers are men, about 80%. Van Galen explains: "A VIP can also invite two other persons to the VIP deck. Women want to be invited to the VIP area, whereas men want to invite women."

From the perspective of Identity Management, this case can be seen as quite normal: user and maintainer of the system mutually agree upon what kind of information is used to what purpose and no other parties are involved. As the user receives extra VIP treatment and extra credit for drinks, it can be seen as an extended version of a customer loyalty scheme. Still, due to the method of implanting tags, this case triggered huge debates. Some journalists compared the tagging of VIP to the tagging of cattle. Privacy groups claimed it set a precedent to use implants for other purposes too. Some Christians regard the implant as unethical, referring to biblical verses on the arrival of the beast, which should be preceded by people being marked with a number. In the Netherlands, the issue went all the way up to Parliament, where a spokesperson of the Christian Union party opened the debate on whether it should be allowed to tag people in this way.

Barcelona director Chase foresees a future in which everyone will have an RFID implant: "The objective of this technology is to bring an ID system to a global level that will destroy the need to carry ID documents and credit cards. The VeriChip that we implant in the Baja will not only be for the Baja, but is also useful for whatever other enterprise that makes use of this technology." One of the VIP guests of the Baja Beach Club Rotterdam, Steve van Soest agrees: "The main benefit is that you can go out without having to carry a wallet, which can get easily lost in a night club. […] It would be great if this catches on and you could put all your personal details and medical records on it.

If I was involved in an accident, doctors could simply scan me and find out my blood group and any allergies." The director of the Rotterdam club, Jo van Galen, has a more reserved view on the application. He recognizes the multiple opportunities the technology has, but is cautious about expanding the applications of the chip. His main concern is running a business, while Dutch society and Dutch media tend to portray the VeriChip in a negative manner. Consequently Mr Van Galen is very much aware that opinions on the technology can change easily from positive to negative and that this can harm the nightclub's image.

Still, Van Galen foresees some future applications too, such as chipping personnel. Currently, personnel of the nightclub carry tokens with chips in them. This way they can enter through a personnel entrance. However, the token could be transferred to another person. The implant could have a big advantage there, since it cannot be transferred nor lost by the carrier. But it should not be used, for example, for time-registration. Mr Van Galen also thinks about using a credit system instead of the current debit system. This will involve linking the ID of the chip directly to a bank account or credit card. An advantage could be that a guest would never have to hand over any cash or bankcard and may enhance the feeling of exclusiveness. A disadvantage could be that it does not 'protect' a guest from spending more than intended, since there is no maximum amount to spend. Furthermore, it involves issues of privacy and safety. Finally Van Galen is in favour of the application expanding to other nightclubs. He envisions a 'chippers-community' in which VIP Chip carriers from different nightclubs can meet (in person or virtual) and in which they can use their status in associated clubs. For now, the chipping community will remain inside the Baja Beachclub until the negative storm of publicity surrounding the chip has settled down.

3.5 Going to work: access and presence

The working environment is perhaps a setting where we can see some of the oldest applications of RFID for Identity Management. In the last decade many offices have switched from the normal iron keys or magnetic cards to RFID. Surprisingly very few studies exist of RFID use in this area. One exception is a study from the RAND Corporation on five large offices in the US. Their accounts demonstrated that none of them used RFID merely as a key. Although the systems were put into place by the security departments and managed as such, other departments soon took an interest in the information gathered, such as human resources, the legal department and line management. [Balkovich et al, 2005: p.12] Many functions were added, such as time registration, as we will see in our European cases too. Identity Management is then not just distinguishing between who has access and who does not, but is also about controlling the office population: having the right people at the right place on the right time.

At the **NWO office** in The Hague, the Netherlands, people are still learning that the small plastic token they hold is not just a key, although it appears to be at first sight. On entering their office, they go through several doors which are secured with an electronic lock: from the underground car park, to the elevators and on each floor. Readers are placed next to the door handle. The RFID tag can be read when it is held less then a centimetre from the reader. The unique code is sent to the database, which checks whether the token can provide access. If it does, the door opens, if it does not, the door remains closed and the system operator receives a signal on his screen. At every reading the following information is stored in a central database for an unlimited time: door, department, time of entry and name of employee.

This key function is extended by the possibility of differentiating levels of access. Token holders can be given access just on the route to their place of work from 7.30 up until 19.00 and some of the general facilities such as the canteen. Access can be extended at the central database: allowing personnel to visit offices of other organizations in the building as well, or get access beyond the time limits.

We discovered a lively trade evolved around this extension, especially between different organizations residing in the building. In our interviews, the system administrator appeared quite strict about the rules: only permanent staff can get the key, with fixed level of access. However, the system operator, who has access to the database appeared to be more flexible, demonstrating Identity Management is not quite fixed, but negotiable.

Many people succeeded in obtaining additional tokens for temporary staff, although this is not allowed. Also, one head of facilities convinced the system operator to bring her own access level up to a higher grade and that of others down, providing her with access to all other offices, while she got all other personnel from other offices rejected - even the service people who needed to access the office for maintenance. Another employee also turned out to have extended access: this was revealed when staff were having a celebratory drink down the hall one day and they discovered they could not enter their offices again because it was past 19.00. To everyone's surprise this employee's token opened all doors while others were locked out, even the director of the organization.

In our time in the office, we asked several people about their opinions of the system. Almost all of them were surprised to find out their check-in time was registered and had assumed the system to be nothing more than an access system. The system operator also told us an interesting story of one employee who discovered that the token is more than just a key. His colleagues and supervisor saw him leaving quite early every day, while he claimed he also started very early when others were not there. The supervisor then went to the system operator and requested a table of check-in times of this employee. The data showed the staff member did not always start as early as he claimed to. The system administrator however refutes this story, reclaiming the primary function of the system: access, not time registration. Still, a database administering the whereabouts of all staff, may prove to be too valuable to be merely used as an access system.

This case study can be seen as a very basic example of RFID and Identity Management in offices. We now go to the offices which do overtly use RFID for tracking personnel real-time. In order to do that, some practical, but essential adjustments must be made on the system. Most passive RFID access devices are mainly used to enter, but not to exit buildings. Serving its function as a key, the person only has to identify at entrance, while a push button at the other side provides an easy exit. Also, once one personnel member has opened the door, several colleagues can come along leaving no trace in the database. A football stadium kind of turnstile could be a solution, but may obstruct the movement of personnel too much and be less suitable to the office culture. One solution could be stepping up from passive to active RFIDs, tracking movements real-time, anywhere on the premises, as we can see in the cases below.

Mol-Logistics is an international company specializing in logistics and has considerable experience of using RFID for cargo. The technology has now been extended to monitor personnel movements too. Their location in Tilburg is divided into zones by a number of strategically placed RFID readers, both at the truck area as well as the offices. Each truck driver and office staff member carries an active RFID tag which broadcasts a unique signal every 1.5 seconds. The database thus provides a real-time image of who is present in which zone, managing the identity of all people inside the premises based on time, place and access levels. First of all, the active RFID tag serves as a key to open the fence, providing access to drivers and as a hands free door opener at the offices. Secondly, it also serves to deny access, for example, for visiting drivers who receive active tags too. As long as they remain in the docking area nothing happens. Once the visitor moves into a restricted area, for example, the warehouse, an alarm is triggered. Thirdly, at the offices, the tag functions as a punch card, registering time-in and time-out as personnel enter and leave the office. Finally in case of an emergency, security personnel can immediate spot whether people are still in the danger zone.

It is reasonable to assume that the logistics sector might readily adopt RFID as they already have broad experience with it. But what will happen if this system is used in an office environment? **Alcatel**, the international telecommunications company, tried this. Although some employees initially perceived the system as a 'Big Brother tactic' it turned out to be in favour of the staff when the Workers' council addressed the issue of overwork.

At the start of 2005, the Alcatel office in Rijswijk, the Netherlands shifted from magnetic card access to active (battery powered) RFID access. All employees received a thick card (100, 50, 5 mm), with a picture of themselves on it, to be carried visibly at all times.

An active RFID chip inside the card broadcasts a signal every 1.5 seconds. Readers are placed at all doors and throughout the halls. The system as a whole registers the whereabouts of all the tags in the building in real-time. Guests at the office also receive an active tag, the identity of which is linked to the person receiving the guest. Valuable devices such as laptops and beamers are also tagged with active RFID. This serves several functions: automatic hands-free access, evacuation management, time registration and theft prevention. This is what the system is supposed to do. Yet according to several people we interviewed at the office, some remarkable things happened.

First, the automated access. On arrival, employees go through three access points: the parking lot (if they come by car), entrance to the building and the staircase or elevator. With active RFIDs, the users should not have to hold their cards near a reader, but just wave it in its direction or not at all. Still, the communication between tag and reader does not always work properly. The reader at the entrance of the parking lot appears to have its moods, presumably depending on the weather. Some readers on one floor appeared to register people moving on another. This was just a matter of adjustment. A remaining problem is that the exit reader does not always register exit, presumably because several people move through at the same time. Also, as many other offices, this building has several exits clustered together. This caused a single approaching employee to open the elevator, hall door and fire escape at the same time – the latter setting off an alarm.

Second, the evacuation management. Every now and then, the Alcatel office holds an evacuation drill. Facility Manager Hans van der Kooij then sets off the alarm and the staff are expected to leave the building. The system then provides a table of all active RFID tags left in the building, presumably of employees in hazard. At their first drill with the new system, Van der Kooij came out last, disappointed, holding four tags with no employees attached. In the case of a real fire, this may have caused a fireman to risk his life, searching through the smoke for injured workers, only to find a tag left on the desk.

Third, time registration. The database registers the time of entry and exit of all employees. The net time spent in the office is presented in a time registration sheet to the employee, who then justifies hours spent on projects. This system may appear like a punch card system but actually it is not. The simple reason for this is that less than 25% of staff perform their work in the office only. The rest of them are continuously on the move for their clients. Also some people live quite some distant from the office and are allowed to add some travel time to their working time. The time being registered by the system is therefore merely an aid for the employees to fill in their time sheets. One of our respondents, Jan Vet, had just came back from a customer in Luxembourg and had to add 14 hours to the sheet. It would otherwise say that Jan had not been at work at all these days. Also, some flaws occur, especially on checking out of the office. Then the system registers the employee entered, but never left the building, leading employees to maintain all kinds of paper based registries to correct the system. Although employees apparently have a degree of freedom in managing their identity of being at work, they are being tracked in and out of the office which may give a sense of being checked when they fill in their time sheets.

During the implementation of the system, the Workers' Council got involved as they received questions from staff members. These questions mainly revolved around what would happen with the information registered by the system.

For example: "where is the information stored", "who has access to it", "how long are the data retained" or "is it connected to our desktop phones"? A small number of people argued that the system was a 'Big Brother tactic', scanning all their movements through the building. It turned out that one specific sales representative triggered these concerns. He was found to have major difficulties with time registration, which is in fact an issue in its own and not linked to the RFID system. Nevertheless, this demonstrates people are likely to use the 'Big Brother story' in relation to RFID. In response Jan Vet and his colleagues checked the implementation with a number of legal advisers and used a checklist of the Dutch Data Protection Authority. A read of this checklist clearly shows that it is derived from the Privacy Guidelines (see Introduction).

Jan Vet, member of the Workers' Council, stated: "I consider myself to be quite an anarchistic person, but if you describe this system as 'Big Brother', I think that is a gross exaggeration. You are being followed through your GSM and while you surf the Internet. RFID is not much worse than that." Moreover, the system is not used beyond its purpose, for example, to evaluate personnel productivity based on their movements or whereabouts. One thing he does worry about is what governments will do now RFID is implemented on such a large scale. "Governments should be liable for not misusing these systems. Their hunt for so-called terrorists should not evolve into permanent scrutiny, which I think is disproportional compared to, say, casualties of car crashes."

Now the system is fully operational and accepted, the Workers' Council even turned it to their advantage: they use the time registration to prove they are overburdened with work. Like any telecommunications business, Alcatel cut down on personnel during the recent telecommunications crash. Now business is improving, the workload is increasing while few new staff are hired. Overwork was claimed to be incidental, but, with the time registration in hand, the Workers' Council demonstrated is was structural, for some, even beyond the boundaries set by labour laws.

All in all, implementing an active RFID system in order to track personnel may initially appear to be quite invasive, while in practice this has not proved to be the case. Aside from some practical issues, the system was accepted by the staff quite easily. Jan Vet stated one of the reasons may be that, as they work for large telecommunications companies, they are used to high-tech, high-security environments. Although the system could be used to evaluate the functioning of staff members on the basis of their movements, it is not. It remains, above all, a security system. One of the reasons for this may be that the Workers' Council was involved in the implementation from the start.

As they bring security in the workplace up to a higher level, RFID systems are currently used in prisons too. Here we can analyze Identity Management on the work floor in what is perhaps its most extreme form. In this case identities are not just based on access or presence, but as a monitoring system on the way people move about – prisoners as well as guards. **Penitentiary Lelystad** in the Netherlands is one such 'smart prison', where RFID not only scans for unauthorized behaviour, but also functions as a reward system.

This prison has been especially built for testing new technologies and detention concepts. A maximum of 150 prisoners who volunteered for the new detention concept have a (remaining) penalty not exceeding four months and share a room with five other prisoners. They all carry a non-removable bracelet containing an active RFID chip. Identity and location of the prisoner is tracked in real-time. The prisoners can design their individual day programme and the RFID system tracks whether they stick to it, providing information for a crediting and penalty function.

An alarm is activated when a prisoner is not following the programme, while they receive extra credits if they do. Although this reward system can be perceived as labour, it is questionable whether this case can be seen as a working environment for the prisoners. For the warders it is and they carry an active RFID tag too, locked on their key-chain.

The warden's chip provides the control room real-time information about their whereabouts. It also has a 'panic button'. When there is a problem on the floor, the control room has in instant overview of the warder's whereabouts and appropriate orders can be given. At first, the prison warders did not express concerns, nor did they have questions about the technology. After a while however, some issues arose, for instance about what happens if somebody visits the toilets. It seems as though realization of the possible consequences of the technology grew in time and that examples can help in creating this understanding. In addressing these issues, the concept designer and the prison wardens reached an agreement not to use any information that could possibly be collected with the RFID environment. According to the designer, this has never been the intention and the agreement remains in force to take away or avoid any concerns.

One Dutch newspaper described the prison as being called 'Big Brother bajes' (bajes is Dutch slang for prison). A visitor of a discussion board commented on an article about the concept: "I also had a major problem with the fact that failure to pay traffic fines or petty theft could land you in a prison like this. That means I, and many others in the class, could have our right to privacy legally stripped from us in a very dehumanizing way if we lived in the Netherlands. I think this kind of surveillance, for petty crimes, is completely backwards of the Dutch, who are otherwise liberal". For now, this person may be incorrect, as both wardens and prisoners have a choice to work or serve time in a conventional prison. Yet once this pilot proves to be successful and all prisons start using the system, they will not.

All in all, the working environment proves to be an interesting site to investigate Identity Management issues. RFID systems primarily function to ensure that the right people are at the right place. Especially in working environments already focused on security, more advanced systems enter, leading to new functions for better or worse for both user and maintainer of the environments.

3.6 Crossing Borders: identifying the whole European population through RFID

If we were to take a plane from Amsterdam to Paris, two RFID chips could be managing our identity: one to track our luggage and one to prove we are who we claim to be. The first one is easy from our point of view: Instead of a barcode strip, the hostess connects an RFID to our bag. From the perspective of the owner of this setting, the new system is a massive operation which will make luggage handling faster and easier. The second application, our RFID passport, is perhaps the most complex Identity Management operations in the history of RFID. The chip does not only store a unique number, but also a picture of us. In the future, fingerprints will be added. To ensure that only the legitimate owner of the RFID environment can read the chip, many complex security measures need to be taken.

In 2004, the International Air Transport Association (IATA) launched a programme to test and build a business case for the use of RFID for luggage management. In November 2005 the organization introduced a global standard for RFID baggage tags. **Air France-KLM luggage handling** serves as a test site on flights between Paris-Charles de Gaulle and Amsterdam Schiphol Airport. Later in 2006 more drop-off points in Amsterdam Schiphol Airport will be using RFID labels. The goal of the pilot is to improve the baggage handling process. By implementing RFID labels more reading points are possible, due to automated reads and a higher read rate than barcodes. Thus, bags can be sorted and loaded faster than with barcode systems and the number of mishandled bags and associated costs are reduced.

For now, the pilot looks promising from the point of view of Identity Management. Bags can be identified easier, while the code can also be changed, for example, when a flight direction is changed. From the perspective of the traveller, one may suggest this new system does not involve any Identity Management issues. Still, we did find some accounts on on-line forums of people who worried their bags may be read by unauthorized persons or others may distort the database by deploying chips in their bags with false IDs. For now, this case is still unfolding and there are no issues yet. Accounts of unauthorized readings or even falsifications of the **RFID passport** however are alarming, as we will see in the next case.

Last year Europe passed the deadline of 28 August 2006, on which all European countries should have implemented the biometric passport. The following countries made it: Belgium (November 2004), Sweden (October 2005), Germany (November 2005), Great Britain (April 2006), Austria (June 2006), Denmark (August 2006) and the Netherlands (August 2006). Following demands from the US Visa Waiver Program, the ICAO (International Civil Aviation Organization) decided in May 2003 to use facial recognition in travel documents. The European Union followed in September 2003 with the decision to use a photograph and two fingerprints. The technical specifications were determined on 28 of February 2005. At first only digital photographs will be saved on the chip inside the passports. Later additional biometric data can be added, such as fingerprints, DNA-profiles and iris scans.

The main reason for going from a paper-based to an RFID passport is to combat look-alike fraud. With the former passport, anyone who would resemble the picture in it or succeeded in replacing the picture with their own could take the identity of the rightful owner. With the RFID passport, the picture is not just visible in the document, but also stored on the chip in a universal format. Border control officers can then check whether the visible and electronic picture matches. Cameras can also analyze the facial structure of the person holding the passport and compare this with the electronic picture. Another, more practical reason for using RFID is to speed up border control: the passport can be read automatically, cutting down on time for manual checks.

Many technical measures have been taken to secure the communication between reader and RFID, such as Basic Access Control (BAC). The chip can then only be read if the passport is opened and placed on the reader, which reads the text printed on Machine Readable Zone (MRZ). The text contains the name, country and passport number of its holder and also serves as a key to start the communication with the RFID chip inside. Advanced as it may appear, researchers from the Radboud University Nijmegen [Hoepman et al 2006] succeeded in eavesdropping on the BAC procedure (‘skimming’) from a distance of several meters by guessing the 128 bits on the MRZ. Normally, guessing a code of that size would be merely impossible, that is, if it were a random code. The MRZ however is not random, but contains certain information which can be expressed in a formula, drastically bringing down the range of possibilities.

For example, the issuing date and expiring date are limited and logically connected. Some countries issue the passport numbers sequentially, again establishing a link with issuing date. The researchers cracked the code and could read from a distance who was holding the passport.

The European Union therefore stepped up to Extended Access Control in which not only the passport but also the reader needs to identify itself with a certificate. The Radboud researchers state this is a major step forwards but still doubt whether it will work in practice. Reading machines will probably be stolen, breaking the security chain. This will be countered by issuing temporary certificates, but the current chips do not have a source to measure time. Also, managing a large international issuing system for certificates will lead to major overheads.

Another leak in the system also appeared when it turned out different countries use different RFID chips. It would, for example, be possible to distinguish from a distance between Europeans and Americans, without going through the Basic Access Control procedure. One hypothesis, occurring in the media quite often, is a smart bomb placed in a public space, being set off at the moment a certain number of passports from a certain country are near. Although this may be possible in theory, it has not occurred yet. Yet people are already taking precautions by shielding off their passports with metal covers, preventing unwanted communication with readers.

These issues can be seen as the technical side of Identity Management. From the users' perspective a much more personal Identity Management issue arises: governments using the passport for much more than just border control. Although this is mainly triggered by the biometric database and not by RFID, contactless communication facilitates the exchange of biometric information and is therefore also seen as responsible. One such function added to border control is that the biometric database will itself be an analysis tool. For example: searching for potentially hazardous people on the basis of their appearance. A picture can, for example, tell much about someone's religion or race. Another function creep involves connecting the central database to other databases, getting a full picture of a person's whereabouts and being sure the person actually is who they appear to be. It is for this reason organizations such as the Dutch Data Protection Authority are opposed to a central database for the biometric passport. Also, many reactions in newspapers claim the biometric passport is just another step towards a 'Big Brother regime'. Put more subtly, the Radboud researchers state:

> "The possibility of biometric identification of the entire (passport-holding) population involves a change of power balance between states and their citizens. Consent or cooperation is then no longer needed for identification. Tracing and tracking of individuals becomes possible on a scale that we have not seen before." [Hoepman et al 2006: 11]

They expect some political groups will be likely to combat the RFID passport. These groups could, for example, persuade people to put their passport in the microwave, destroying the chip while saving its physical appearance.

Even stronger, such a political action group could build disruptive equipment to destroy the RFID chips from a distance without the holder noticing. Yet for now, citizens are complying with the new passport. Identity Management issues from the side of users currently focus on practical problems with biometrics, as it took many people much effort to get their picture right. They had to look straight into the camera and were not allowed to smile, which gave them a feeling of being squeezed into a uniform format. Also, early tests show facial recognition does not always work well, especially with children and the elderly.

Once the majority of the European population has an RFID passport, new, perhaps unanticipated applications may be suggested. Being the ultimate Identity Management application, banks, insurers and other organizations would also want to use it to manage the identity of their customers. How Europeans then try to take Identity Management back into their own hands remains to be seen.

4. The next four years and beyond

The preceding examples demonstrate how users of RFID systems leave digital footprints in a variety of settings. In some cases, these footprints are used to build up a digital identity of the users and provide appropriate feedback through the system: price differentiation, direct marketing, measure employee productivity, etcetera. In some sectors such as employment and leisure, we found little direct evidence of user opposition to RFID. Opposition, where it occurs, is often led by campaign groups. Although a more comprehensive survey would need to be undertaken to draw definite conclusions, these first accounts suggest that, relative to the scale of implementation, few Identity Management issues occur. In general, both user and maintainer of the RFID settings perceive RFID merely as an electronic key or wallet. The reason for this can be twofold. First of all, in all the cases it is clear who maintains the data and needs to comply with the guidelines on data protection. Second, many systems currently only cover a small area of a specific setting and run parallel to legacy systems. The RFID systems therefore only disclose small fragments of their users' identity, limiting the maintainers' possibilities for control.

In the near future this could be different. Once RFID systems work exclusively with RFID it will become easier to aggregate and analyze the data on the level of the whole user population. Further, once different RFID systems will become connected to each other, or other technologies such as GSM, GPS or Internet, a much richer image of its users will appear. The scenario unfolding then is currently known as 'the Internet of things'. In this chapter we elaborate on these technological developments to explore how these could affect the relation between users and maintainers of RFID settings and the role of government in the coming four years.

4.1 Towards a new balance of power with the Internet of things

According to the RFID users we interviewed in our field research, very few actually see any problem in the digital footprints in the RFID settings they use. It has to be clear who maintains the environment and the use of RFID will have to give them something in return: convenience, choice, safety, discount, etcetera. Aside from that, they trust the chip they hold is not more than an electronic key or wallet. This trust in the limited function of the system is somewhat justified. Unlike, for example, GSM, GPS or Internet data, RFID data currently only provide a very fragmented image of its users. The systems only encompass a small area: one subway line, one club, a single office entry or part of a road. Within these limited settings, many systems still run parallel to the system they are supposed to replace: paper tickets, barcodes, cash, iron keys, magnetic cards, etc. This could limit the convenience for the users, but it also provides them with more choice and limits the possibilities for control by the maintainer. In other words, a poor digital identity is not worth managing.

This could change in the coming years. According to the experts with who we discussed our findings, a number of developments are likely to take place that will lead to an 'Internet of things' in which RFID will play a key role. First, the exclusive use of RFID within current systems is likely to rise. The RFID passport and public transport cards, for example, are currently used by a fragment of the population on a limited number of settings. Once every citizen holds an RFID version of these identity cards, the databases running within these systems will provide a real-time overview of all movements within the system.

Secondly, elaborating on the opportunities for both users and maintainers, it is likely more RFID systems will be connected with each other. This can enhance the convenience for the users: more possibilities with less cards and tokens to manage, receiving more personalized service. For the maintainers it can mean extending their service area and gaining control over the setting. A combination of travel and payment, in particular, is expected to provide these opportunities.

The Japanese Suica Card is a good example of a public transport card which can also be used for other small transactions at the stations. The American example of paying at the pump as well as in stores and snack bars is another example, although it is not clear whether this application was a success.

Third, a tendency to couple RFID systems to other technologies in the digital public space (GSM, CCTV, Internet) can be distinguished. In the British Madjeski stadium, for example, the RFID database is connected to the CCTV system to manage the identity of potential hooligans. Many banks, telecommunications companies and RFID suppliers are currently seeking collaboration in connecting RFID to the GSM network, using Near Field Communication. In NFC, a mobile phone can function as an RFID chip, enabling the user to perform small transactions while just waving their phone at a reader. The Asian Felica system works that way. The NFC phone can also be an RFID reader at the same time, to read tags in the environment, for example, a poster, and use the code from the chip to unlock information to be retrieved through an Internet connection. Caens in France and some places in Finland use this as a tourist application.

Finally, the coupling of different networking systems will get a new dimension once these run on IPv6, Internet Protocol version 6. The current version, IPv4 is used to provide computers and servers within the network with a unique identity, but is limited in the number of possible unique identities. IPv6 contains so many numbers, that virtually any person, object and RFID chip on the planet can be given their own unique address, opening up many opportunities for identification, tracking and control. The combination of an all-encompassing interconnected network in which all actors are uniquely identifiable will lead to an 'Internet of things', a digital one-on-one copy of the physical public space.

This scenario could unfold in the next four years. Whether is actually will, remains to be seen. However it is clear that RFID is still in its infancy and if we look at the possibilities ahead, the balance of power within RFID settings is likely to change. If payment and access systems become exclusively digital, maintainers will have access to a much broader picture of their users. Meanwhile, once systems become much more interconnected, it is far less clear to the user who actually owns and maintains the environment and who is tracking their digital footprints for what purpose. The development of RFID into an 'Internet of things' will provide maintainers many opportunities to manage the identity of its users. Will users acquire an equal gain in these benefits?

4.2 Applying the Privacy Guidelines to RFID

Users of RFID systems are protected by privacy guidelines and have, in some cases, a right to informational self-determination, described in the chapter on personal ID. According to the experts, these guidelines are just, but it remains to be seen whether they work in practice. The case studies demonstrated several shortcomings in applying the guidelines.

First of all, awareness. It remains doubtful whether all users of RFID are aware of these guidelines. Moreover, as RFID is being implemented by many different kinds of organizations at an accelerating pace, it remains to be seen whether all maintainers are as well. The previously mentioned RFID employer identity at the Alcatel office was managed in agreement with the workers' council, using the guidelines. Yet Alcatel is a large telecommunications company for who data protection is part of daily routine. At the NWO Office on the other hand, employers were handed out 'electronic keys', not knowing the code was connected to their name and the database could be used to track their movements. It is also unlikely all staff and people who have access to the database would be aware that the directive was applicable in this case.

Secondly, a maintainer of an RFID environment could, in principle, provide full insight into the purpose and process of data gathering, while making this virtually impossible in practice. Notorious examples are the user license agreements, which are very elaborate, unreadable and impossible to find. The Dutch Railways, for example, sent holders of seasonal tickets an RFID replacement of their card, accompanied with a letter stating that the act of use will be interpreted as an agreement with the terms stated on a website with a very long address. In case of the Italian SI Pass, the agreement literally states the data will be used for marketing. The agreement on the American version of the Exxon Mobile Speedpass informs about the marketing function too and even states the data can be sold to "any bidder" and the agreement can be changed by the maintainer at any time without informing the users.

Third, data can be analyzed anonymously, as in the case of De Apenheul. Visitors were tracked through their Monkey bag, without their informed consent. The identity of a tracked visitor was in no way connected to the name or any other personal information of its bearer. Therefore the directive did not apply. Although visitors do not have to experience any concrete disadvantage through their digital identity, not every visitor will appreciate the practice. This could be the case when the maintainer of such an anonymous RFID environment does feed back the identity as price differentiation, service level, denying access or any other consequences.

Finally, it appears natural to RFID that the value of additional functions is mostly proven in practice. Once the setting is in use and the databases start running, new opportunities emerge, are tested and implemented gradually leading to a function creep. Will the maintainer of an RFID setting inform its users on every new function of the system and every new bit of identity added? Do users want to be informed on every step of the way? Or will this prove to be too laborious in practice for both parties and will convenience prevail without critique?

These limitations in applying the guidelines can already be discerned in the current cases, although they did not lead to major controversy yet. How about the next four years? What will happen if the scenario sketched above unfolds? If the sheer number of RFID chips and systems in use continues to rise at this pace, it will become practically impossible to inform users about every event of data reading and to apply the guidelines to it. If access and payment systems totally abandon their legacy systems and switch to RFID, there will be less choice for citizens not to use RFID. If more and more systems are coupled, it will be increasingly difficult for users to single out who is actually managing their identity and hold this party responsible for complying with the regulation. The kinds of identities the systems are supposed to manage will also be elaborated on by an increasing number of maintainers, making it practically impossible to seek agreement every step of the way.

In the longer run, the whole concept of 'personal data' may prove to be lacking. Then the issue is not just about information related to a physical person, but may also encompass how users of RFID systems gain advantages or disadvantages through their interaction with RFID systems. Differentiation in level of access, price or service level, for example, can also be implemented by analyzing anonymous data. Then the maintainer of the environment does not have to comply with the Privacy Guidelines, while gaining control over his users.

4.3 RFID and police investigation

In the short history of RFID in public places we already came across accounts of RFID being used for police investigations. In the football stadium, it was suggested access codes in combination with CCTV will be handed over to the police. The database of the London Oyster Card was requested 61 times by the police. Due the limitations mentioned above RFID data currently give a very fragmented image of the behaviour of its users and officers would be likely to rely more on GSM, bank accounts and Internet traffic data.

Yet as systems may be more exclusively RFID and connected, the digital footprints in the database may indeed be valuable to police investigation. How RFID will be used for this purpose will become apparent in the future.

In case of the Oyster Card, the transport company claimed they were complying with the Privacy Guidelines, and they are as the state is exempted from the directive. Interestingly enough, the spokesperson also stated "There is no bulk disclosure of personal data to the law enforcement agency." This touches on a very sensitive issue. International travel data, GSM traffic and bank transactions fall under the data retention directive, which means the maintainers of these digital public places need to store the data centrally in case the police would like to use it for investigation. Although this directive covers traffic and location data generated by telephony, SMS and internet, but not the content of the information communicated, the data can be used to track the whereabouts of citizens and who they communicate with [Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006]. According to a Rathenau study [Vedder et al, 2007] a shift in methods of enquiry can be discerned which is relevant for RFID too: centralized data are not just used in the case of tracking down a specific suspect, but also to mine and analyze, using risk profiles in order to *prevent* crime.

The first method is likely to meet few protests from users, while the second is at the very heart of the current debate on privacy versus security: enquiry for proving guilty or every citizen under surveillance. Police currently have more means to force maintainers to retain and exchange their data, extending the force of law to businesses involved. Will RFID data be mined for the same purpose? This debate has already taken off with respect to the RFID passport, as described in the preceding chapter. European law now leaves the decision for centralizing data up to the Member States. Germany for example, one of the few countries strictly applying the principle of informational self-determination, as well as Italy have already explicitly rejected centralization. Many other states have yet to decide.

The debate on RFID in general for investigation purposes is yet to take off. Some citizens will feel safer knowing the state is watching over every RFID user, while some will deem it to be unacceptable. Some could accidentally build up a wrong identity in the system and meet consequences accordingly, while others trust only the real criminals will be caught.

Will users gain trust in RFID as they feel more secure, or will they increasingly experience RFID as a control system? Also, what will the consequences be for businesses implementing RFID in public places? Do they fear users will reject the system? And who will pay for the labour and server power involved in retaining the data?

5. Challenges ahead: balancing convenience, control and choice

We live in an era in which our public space is digitalizing at a rapid pace, heading for an 'Internet of things'. RFID is seen as a key technology in this development. This research demonstrated the small chips being read from a distance can provide many choices for users and maintainers, making daily life more convenient and controllable. RFID users in general perceive RFID chips as not more than an electronic wallet or key and trust their personal data are managed accordingly. Once RFID is used in more settings, exclusively and connected to each other and other technologies, digital footprints will provide a much broader picture of the users, opening up new opportunities for control by businesses and government. This is not just an issue of protecting privacy or personal data, but it is more about securing personal freedom and striking the right balance between choice, convenience and control. We therefore formulate the following challenges ahead.

1. RFID users need to know what maintainers can and are allowed to do with RFID data

Users need to be aware RFID can be more than just an electronic wallet or key and they leave digital footprints in RFID environments. Transparency should not lead to an information overload: user license agreements should be short, clear and available. They should not just be in concordance with the Privacy Guidelines, but also be tested on usability. Only then can users consciously manage their identity. Full informational self-determination may prove to be impractical, due to the number of systems in use. Still, users need some form of gaining knowledge to regain power. Being a very multicultural, multilingual continent, a typical European challenge could be the development of communication standards, for example, pictograms explaining the kind of smart environment a user is entering.

2. RFID users should play a role in developing new RFID environments

During the design of RFID environments, important decisions are made concerning the choices users will have and the degree of usability and control. Identity Management should not be organized just one way, but users need to have a say in how the RFID setting defines them. For some applications, for example, personal data are not required for the functioning on the system, while in other cases, adding personal services can be valuable for both maintainer and user alike. Their involvement does not have to stifle innovation; it can also stimulate for as we have seen, innovation mostly takes place in practice.

3. Responsibly extending RFID settings

The two aforementioned points are increasingly important once the function of RFID settings is elaborated on through connecting them to other smart environment technologies such as GSM, GPS, Internet, or, perhaps in time, these become part of a whole 'Internet of things'. Although this could enhance convenience, for example, bringing down the number of tags one carries while extending service delivery, it should remain clear for the users who is actually managing their identity in the different settings. If the coupling of systems would lead to an unacceptable degree of control from the side of the maintainer, this should be prevented.

4. Reconsidering the Privacy Guidelines and the concepts of personal data and informational self-determination

The Privacy Guidelines and the principle of informational self-determination can currently be seen as just, but will be increasingly difficult to enforce in practice. More research is needed to monitor new applications on how the guidelines are applied and are experienced by users.

Then two questions can be answered. First, should personal data remain those data connected to a specified, physical person (e.g., name and address) or should it be extended to all sorts of interactions with RFID systems which have consequences for the users, even though the user remains anonymous? Second, to what extend can and will users be able to manage their identity themselves or do they need to trust increasingly on others managing their identity?

5. Governments should take a clear stance on whether RFID bulk data will be mined for investigation purposes

Are police officers only permitted to inquire in RFID databases in the case of a specified suspect, or will they gain continuous access in order to screen the whole user population for suspected behaviour? If so, users and maintainers should be made aware of the possible consequences and strict monitoring will be needed to prevent innocent people being under suspicion just because their identity was not well managed.

6. Sources

6.1 Literature

Balkovich, E., Bikson, T. & Bitko, G. (2004) *9 to 5: Do You Know If Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace.* Los Angeles: RAND Corporation.

Capgemini (2005) *RFID and Consumers: What European Consumers Think About Radio Frequency Identification and the Implications for Business.*

Garfinkel, S. & Rosenberg, B. (ed.) (2006) *RFID: Applications, Security and Privacy.* Addison-Wesley.

Harrop, P. & Das, R. (2006) RFID in Healthcare 2006 – 2016: report summary. IDTechEx

Leisner, I. (ed.) (2006) *RFID from Production to consumption: risk and opportunities from RFID-technology in the value chain.* Copenhagen: Teknologirådat.

Locquenghien von, K. (2006) 'On the Potential Social Impact of RFID-Containing Everyday Objects.' In: *Science, Technology & Innovation Studies,* Vol. 2, March 2006, pp. 57-78.

Nsanze, F. (2005) *ICT Implants in the Human Body.* European Group on Ethics in Science and New Technologies.

POST (2005) "Pervasive Computing" POST note May 2005, no. 263 of the Parliamentary Office of Science and Technology

Retail Systems Alert Group (2004) *RFID: How Far, How Fast: A View From the Rest of the World.*

Rodotà, S. & Capurro, R. (2005) *Ethical Aspect of ICT Implants in the Human Body.* European Group on Ethics in Science and New Technologies.

Rotenberg, M. (2003) *The Privacy Law Sourcebook 2003* Electronic Privacy Information Center, Washington

Schermer, B.W. & Durinck, M. (2005) *Privacyrechtelijke aspecten van RFID.* ECP.nl

Schermer, B.W. (2006) *RFID & Privacy voor managers.* Platform Detailhandel Nederland, ECP.nl, RFID Platform Nederland.

Schermer, B.W. (2007) *Software agents, surveillance, and the right to privacy: a legislative framework for agent enabled surveillance.* Leiden University Press

Srivastava et al (2005) *The Internet of Thnings.* ITU Report, Geneva

Srivastava et al (2006) *Digital Life.* ITU Report, Geneva

Thomas, A. (2004) 'Radio Frequency Identification (RFID).' In: *Postnote,* no. 225.

Trier van, M. & Rietdijk, J.W. (2005) *Innoveren met RFID: op de golven van verbetering.* The Hague: Sdu Uitgevers.

Vedder et al. (2007) *Van privacy paradijs naar controle staat?* Rathenau Institute, the Netherlands.

6.2 Meetings

6 June 2006, *STOA Workshop RFID & Identity Management* European Parliament (Brussels)

26 June 2006, *Think Tank RFID & Privacy* (The Hague, the Netherlands)

18 September 2006, *Think Tank RFID & Privacy* (The Hague, the Netherlands)

7 November 2006, *Expert meeting RFID & Identity Management*, the Dutch experts (The Hague, the Netherlands)

13 November 2006, *Expert meeting RFID & Identity Management*, the international experts from ETAG (Amsterdam, the Netherlands)

24 January 2007, Workshop *RFID & Identity Management in the Everyday Life* European Parliament (Brussels)

6.3 Case studies sources

Sources used for the case studies are reported for each case in the Appendix.

Appendix: Case Studies

Case #1: METRO Group Future Store

Case ID	# 4, level 2
Title	METRO Group Future Store
Researcher	Jessica Cornelissen and Christian van 't Hof
Timing	April 2003 – present
Geography	Germany (Rheinberg)
Setting	Shopping
Environment	Grocery store (serving as a test site)
Technology	ICODE (high-frequency) and UCODE (ultra high-frequency), which are read-only passive chips. Tags are positioned on cartons, pallets and a few selected products. RFID readers at incoming and outgoing gates of the warehouse and in Smart Shelves. The maximum reading distance for product labels is approximately one meter operating at high frequency, whereas labels on cartons and pallets can be read up to six meters using ultra high frequency [1, 17]. "Mobile Assistant" handhelds for employees and the "Personal Shopping Assistants (PSA)" for customers communicate via a Wireless Local Area Network (WLAN) with the merchandise management system. [20] The De-Activator does not put the item-level tags in a dormant state, but it permanently disables the tag. In addition case-level tags are disabled at the information counter upon request by customers.
Maturity	Pilot
Function	Tracking and tracing of products
Owner	METRO Group Future Store Initiative [10]. This initiative is a joint platform of the Metro Group [11], Intel [12], IBM [13], T-Systems [14] and more than 60 other cooperating partners from the IT and consumer goods industries and the service sector
Maintainer	
Users	Suppliers, distribution centres, store employees, customers.
Other actors	- Intermec > supply of readers [18] - Philips Semiconductors (currently NXP) > supply of RFID chips [19] - Partners of the Metro Group Future Store Initiative involved in the RFID applications [15] - FoeBud e.V. > privacy group [8]
ID issue	The Future Store implemented RFID enabled loyalty cards. Pressure groups claimed the customers were not informed on this, triggering a public controversy. This led to Metro withdrawing some of its applications and re-issue barcoded loyalty cards. Since this event, privacy groups have kept a close watch on the store. Metro claims there was no overall negative public response. Nevertheless, in much of the literature on RFID, this case is referred to as one of the bigger controversies in RFID and Identity Management.
Sources	1. ' Metro Opens 'Store of the Future''. In: RFID Journal, 28 April 2003 (http://www.rfidjournal.com/article/articleview/399/1/1/, visited 29 June 2006)

2. ‘ RFID for Your Shopping Cart’. In: RFID Journal, 1 July 2003 (http://www.rfidjournal.com/article/articleview/489/1/1/, visited 29 June 2006)

3. Best, J., ‘ Supermarket cans RFID trials in Germany’. 1 March 2004, (http://www.silicon.com/networks/lans/0,39024663,39118760,00.htm, visited 29 June 2006)

4. ‘More on the Metro RFID consumer loyalty cards’. 2 March 2004 (http://www.rfidbuzz.com/news/2004/more_on_the_metro_rfid_consumer_loyalty_cards.html, visited 29 June 2006)

5. ‘Metro zieht RFID-Karte zurück’. 27 February 2004 (http://www.heise.de/newsticker/meldung/45062, visited 29 June 2006)

6. Houtman, J., ‘Online boodschappenlijst toegevoegd aan Future Store’. 3 May 2004 (http://www.emerce.nl/nieuws.jsp?id=279616, visited 29 June 2006)

7. Blau, J., ‘Metro Store bows to pressure from anti-RFID activists’ 1 March 2004 (http://www.infoworld.com/article/04/03/01/HNmetrostore_1.html, visited 29 June 2006)

8. http://www.foebud.org (visited, 29 June 2006)

9. Trier, M. van & J.W. Rietdijk (2005). Innoveren met RFID, op de golven van verbetering. Den Haag: SDU Uitgevers BV.

10. http://www.future-store.org (visited 22 August 2006)

11. http://metrogroup.de (visited 22 August 2006)

12. http://www.intel.com (visited 22 August 2006)

13. http://www.ibm.com (visited 22 August 2006)

14. http://www.tsystems.com (visited 22 August 2006)

15. http://www.future-store.org/servlet/PB/menu/1007073_l2_yno/index.html (visited 22 August 2006)

16. http://www.spychips.com/metro/overview.html (visited 22 August 2006)

17. ‘A successful start for the future of retailing: welcome to the Future Store’ (http://www.future-store.org/servlet/PB/show/1004095/off-Presse-Pressemat-FSI-Booklet-engl_05-01-10.pdf, visited 22 August 2006)

18. http://www.intermec.com (visited 30 August 2006)

19. http://www.semiconductors.philips.com (visited 30 August 2006)

20. E-mail correspondence with Daniel Kitscha from Metro Groups Corporate Communication. 29 September 2006.

21. http://www.futurestore.org/servlet/PB/menu/1007869_l2_yno/index.html, and

22. http://www.futurestore.org/servlet/PB/show/1011188/off-UeberdIni-Publik-Welcome-06-08-24.pdf

Case #2: Marks & Spencer Intelligent Label Project

Case ID	# 6, level 1
Title	Marks & Spencer Intelligent Label Project
Researcher	Jessica Cornelissen
Timing	Spring 2006 – present
Geography	United Kingdom
Setting	Shopping
Environment	Clothing department of retail chain
Technology	Item-level tagging with passive tags, using 868 MHz frequency. Tags are embedded in the 'Intelligent Label' on garments. Reading range is approximately half a meter. Tagging of trays and dollies in the distribution chain, using 13.56 MHz frequency. Readers can be either mobile (Mobile Store Reader (MSR)) or fixed (in the distribution center) [1, 9, 12, 13]. The central database contains stock information of each specific item. This information is used for restocking and re-ordering [13].
Maturity	Pilot
Function	Tracking and Tracing of items
Owner	Marks & Spencer
Maintainer	BT Group and Intellident ltd.
Users	Distributors, personnel in retail store
Other actors	- Consumers Against Supermarket Privacy Invasion and Numbering (C.A.S.P.I.A.N.) > privacy group [2] - Spy.org > privacy group [3] - BT Group > maintenance of database [4] - Intellident ltd > development of MSR [5] - Paxar corporation > production of labels [6] - EM Microelectronic > production microchips - Dewhirst > supply of goods [7]
ID issue	Using the RFID system only for the purpose(s) it has been implemented for, and being cautious in expanding to further applications, could avoid controversy over privacy and identification. Informing consumers can be very important in preventing negative publicity and increasing understanding, even among sceptics.
Sources	1. 'U.K. Trial Addresses Privacy Issue'. In: RFID Journal, 23 October 2003 (http://www.rfidjournal.com/article/articleview/623/1/1, visited 26 June 2006) 2. http://www.nocards.org (visited 31 July 2006)

	3. http://www.spy.org.uk (visited 1 August 2006) 4. http://www.btplc.com (visited 31 July 2006) 5. http://www.intellident.co.uk (visited 1 August 2006) 6. http://www.paxar.com/ (visited 31 July 2006) 7. http://64.233.183.104/search?q=cache:DeJ9T5WMfYQJ:www.dsionline.com/collateral/pdf/software/ss_Dewhirst.pdf+dewhirst+marks+spencer&hl=nl&gl=nl&ct=clnk&cd=4 (visited 31 July 2006) 8. 'Marks & Spencer to Extend Trial to 53 Stores'. In: RFID Journal, 18 February 2005 (http://www.rfidjournal.com/article/articleview/1412/1/1/, visited 28 June 2006) 9. 'Background to Marks & Spencer's business trial of RFID in its clothing supply chain'. (http://www2.marksandspencer.com/thecompany/mediacentre/pressreleases/2004/com2004-01-30-00.shtml, visited 26 June 2006) 10. Sullivan, L., 'Marks & Spencer Prepares To Expand Item-Level RFID Tagging', In: InformationWeek, 18 February 2005, (http://www.informationweek.com/story/showArticle.jhtml?articleID=60402017, visited 28 June 2006) 11. McCue, A., 'Marks & Spencer starts tracking tag trials: High Wycombe store to use RFID tags for men's clothes', 16 October 2003 (http://management.silicon.com/smedirector/0,39024679,10006439,00.htm, visited 28 June 2006) 12. 'EPC in Fashion at Marks & Spencer'. In: RFID Journal, 11 April 2003 (http://www.rfidjournal.com/article/view/377, visited 28 June 2006) 13. 'Marks and Spencer takes stock'. (www.btplc.com/innovation, visited 7 August 2006) 14. http://www.mandslibrary.com/(S(4kamypmlxhtres45gb0pyazc))/ThumbNails.aspx?SectionID=101&Place=Innovation&TopLev=Company&ID=450&ParentID=101&landingimage= (visited 1 August 2006)

Case #3: Air France-KLM Baggage handling

Case ID	# 15, level 1
Title	Air France-KLM Baggage handling
Researcher	Jessica Cornelissen
Timing	July 2006 – March 2007
Geography	The Netherlands (Amsterdam) and France (Paris)
Setting	Border crossing
Environment	Luggage handling on flights
Technology	Passive UHF tags 'Monaco' by Impinj, compliant with ISO 18000 6C standard. Chips are read-write/rewrite and equipped with 64 bits of memory beyond the standard 96-bit electronic product code. The baggage labels and the RFID solution are developed by IER.
Maturity	Pilot
Function	Tagging and tracing of products
Owner	Air France-KLM [1]
Maintainer	Amsterdam Schiphol Airport [2]
Users	Travellers and parties involved in luggage handling at both airports
Other actors	- International Air Transport Association (IATA) > coordinating body on RFID applications in airline industry [3] - Impinj > production of microchips [9] - IER > development of RFID solution [10] - IATA member airlines []
ID issue	It seems as though public opinion on a new technology is susceptible to irrelevant or false claims about privacy. The party running the pilot might not foresee any privacy concerns, but these concerns could arise. Also the fact that someone's property is tagged, could make it more prone to concern from the public.
Sources	1. http://www.klm.com, visited 30 August 2006 2. http://www.schipholairport.com, visited 30 August 2006 3. http://www.iata.org, visited 30 August 2006 4. 'Air France and KLM test radio frequency identification tags for baggage handling and tracking management.' 3 July 2006 (http://www.klm.com/travel/corporate_en/press_room/press_releases/index.htm?id=39399, visited 14 July 2006).1. 'KLM en Air France rusten bagage uit met rfid-chip', 3 July 2006 (http://www.webwereld.nl/articles/41839/klm-en-air-france-rusten-bagage-uit-met-rfid-chip.html, visited 4 July 2006). 5. 'IATA Introduces Global Standard for Baggage Tags', 20 November 2005 (http://www.rfidinternational.com/news.php?action=full_news&NewsID=103, visited 5 July 2006) 6. Collins, J., 'Air France-KLM Embarks on RFID Luggage-Tag Trial.' In: RFID Journal, 18 August 2006 (http://www.rfidjournal.com/article/articleview/2600/1/1/, visited 4 September 2006) 7. Comment by 'Thyxx' on 3 July 2006 (http://www.webwereld.nl/comments/41839/klm-en-air-

france-rusten-bagage-uit-met-rfid-chip.html, visited 4 September 2006)

8. Comment by 'Xtian' on 3 July 2006 (http://www.webwereld.nl/comments/41839/klm-en-air-france-rusten-bagage-uit-met-rfid-chip.html, visited 4 September 2006)
9. http://www.impinj.com/page.cfm?ID=Chips (visited 4 September 2006)
10. http://www.ier.fr/htmleng/acceng/accueileng_estore.html (visited 4 September 2006)
11. http://www.iata.org/membership/airline_members.htm (visited 6 September 2006)

Case #4: Baja VIP Chip

Case ID	# 18, level 3
Title	Baja VIP Chip
Researcher	Jessica Cornelissen

Timing	2004 – present [1, 2]
Geography	Spain (Barcelona) and The Netherlands (Rotterdam)
Setting	Fun
Environment	Night Club

Technology	Implantable read-only passive RFID tags with 16 digit ID-number by VeriChip Corporation. The chip can be implanted subcutaneously with a syringe. The database contains a carrier's information and is linked to an electronic payment system. [3, 4,11]
Maturity	Operational
Function	Identification, access and payment
Owner	Baja Beach Club
Maintainer	Baja Beach Club
Users	- VIP guests of the night club - Personnel and management of the night club
Other actors	– VeriChip Corporation > provider of – The No VeriChip Inside Movement > privacy and digital civil rights group [7] – The Resistance Manifesto > religious group [8] – Bits of Freedom > digital civil rights group [9] – U.S. Food and Drug Administration > public health institution [17]
ID issue	Most controversy on this RFID application is about implanting a chip in the human body. Main issue is the violating of one's personal integrity. Also, some belief it is 'the mark of the beast'. On the other hand, implanting the VIP Chip is done out of free will and having such an implant is not a necessity. Information on 'clubbing' and drinking behavior will be accessible to the nightclub. It is up to the potential carrier to decide whether he or she finds this acceptable.
Sources	1. 'Applications Continue to Grow for Applied Digital Solutions' VeriPay Baja Beach Club in Barcelona, Spain Employs RFID Technology for Cashless Payment System' 05 April 2004 (http://www.findarticles.com/p/articles/mi_m0EIN/is_2004_April_5/ai_114927021, visited 20 June 2006). 2. 'Een onderhuids dranktegoed' In: Algemeen Dagblad, 01 October 2004. 3. http://www.verichipcorp.com (visited 20 June 2006) 4. 'Implantable RFID Tags' (http://www.verichipcorp.com/content/company/verichip#implantable, visited 20 June 2006) 5. 'Bedrijf wil onderhuidse identificatiechip beproeven.' In: Automatisering Gids Webeditie, 28

February 2002

6. Slingerland, C.S. 'Presentatie Baja Vip Chip', 24 May 2006. Rotterdam, Emerce.
7. http://noverichipinside.com (visited 21 June 2006)
8. http://www.theresistancemanifesto.com (visited 21 June 2006)
9. http://www.bof.nl (visited 21 June 2006)
10. Hemment, D., 'Interview with Conrad Chase.' 19 June 2004. (http://www.drewhemment.com/2006/interview_with_conrad_chase.html, visited 21 June 2006)
11. http://en.wikipedia.org/wiki/Verichip (visited 20 June 2006)
12. 'Conrad Chase, Director of Baja Beach Club's Interview with the EFE News Agency about the VIP VeriChip' (http://www.bajabeach.es, visited 20 June 2006)
13. Hemment, D., 'Last Night An Arphid Saved My Life'. (http://www.drewhemment.com/2006/last_night_an_arphid_saved_my_life.html, visited 20 June 2006)
14. Martin, L., This chip makes sure you always buy your round.' In: The Observer, 16 January 2005
15. Personal communication with Mr. Van Galen, Managing Director of the Baja Beach Club Rotterdam, 4 August 2006
16. 'I've got you under my skin.' In: The Guardian, 10 June 2004.
17. http://www.fda.gov (visited 29 August 2006)

Case #5: FIFA World Cup Germany Tickets

Case ID	# 19, level 1
Title	FIFA World Cup Germany Tickets
Researcher	Jessica Cornelissen

Timing	December 2005 – July 2006
Geography	Germany
Setting	Leisure
Environment	Football stadium
Technology	Passive chips incorporated in the access-ticket for the event, chips are supplied by Phillips (MiFARE Ultralight, ISO 14443, Ultra-high frequency). The software is from CTS Eventim
Costs	0,10 per ticket (total of 3,2 million tickets sold) [1]
Maturity	Operational
Owner	FIFA World Cup Ticketing Centre
Maintainer	German Football Association (DFB), system provider CTS Eventim
Users	- Visitors to world cup 2006 matches - Stadiums participating in the 2006 World Cup
Other actors	- FoeBuD [2] > Privacy group - Datenschutz Zentrum > Data Protection Centre [3] - Bündnis Aktiver Fußball-Fans (BAFF) > Alliance of active football fans [4]
ID issue	Implementing RFID technology in a place where users have no choice to use it or not, brings about controversy. Also, privacy groups could cause a lot of negative publicity because policies on data sharing and protection remained unclear for a long period as equally the actual occasions a ticket would be read,. In addition, the widespread and thorough implementation of the technology makes it quite likely that it will be maintained at the stadiums and used on regular matches after the World Cup event. Skeptics think the World Cup serves as a test to see how the technology works out in practice and as a means of justification in retrospect.

Sources	1. Libbenga, J., 'World Cup Tickets will contain RFID chips.' 04 April 2005. (http://www.theregister.co.uk/2005/04/04/world_cup_rfid/, visited 26 July 2006) 2. http://www.foebud.org (visited 26 July 2006) 3. http://www.datenschutzzentrum.de (visited 26 July 2006) 4. http://aktive-fans.de (visited 26 July 2006) 5. Ermert, M., 'World Cup 2006 'abused for mega-surveillance project'.' 08 February 2005. (http://www.theregister.co.uk/2005/02/08/world_cup_2006_big_brother_charges/, visited 26 July) 6. http://fifaworldcup.yahoo.com/06/en/tickets/overview.html (visited 09 July 2006) 7. Best, J., '3,2 million World Cup tickets RFID chipped.' (http://networks.silicon.com/lans/0,39024663,39159715,00.htm, visited 07 July 2006) 8. 'Philips ticket technology opens the doors of the FIFA World Cup', 14 June 2006. (http://www.semiconductors.philips.com/news/content/file_1245.html, visited 28 August 2006)

Case #6: the European Biometric Passport

Case ID	23, level 3
Title	Passport
Researcher	Sil Wijma
Timing	2006
Geography	Europe
Environment	Border control, identification
Technology	Passport with RFID tag, 13,56 MHz, different readers.
Maturity	Pilot
Function	Identification
Owner	Different European countries
Maintainer	International Civil Aviation Organization (ICAO)
Users	Citizens
Other actors	Different governments, different manufacturers (Philips, Oberthur Card Systems, Setec, etc.), European Union and different consumer organizations such as Bits of Freedom (BOF).
ID issue	Researchers showed that the encryption used on the passport could easily be cracked [13, 25]. Also eavesdropping is easier than earlier thought. The signals used to communicate between a passport chip and a reader can be read from more then 9 meters [28] while in laboratories 50 meters is possible [6]. Biometrical data can contain different sorts of information. A photograph, for example, can tell a lot about a persons religion. All sorts of biometrical data like fingerprints, photographs and retina scans can contain medical information [1]. Apart from that there might be other problems because the large-scale use of biometry is untested [26]. Further there are problems with the use of the biometric data gathered. Digital photographs can be placed on chips but identification of persons by this photo is not flawless, especially with children and the elderly [37].
Sources	01. Dessimoz, D. & J. Richiardi (2006) Multimodal biometrics for identity documents (http://www.europeanbiometrics.info/images/resources/90_264_file.pdf, visited 28 July 2006). 02. Mom, P. (2006). 'Groeiend verzet tegen paspoortbiometrie'. In: Automatisering Gids, nr. 5, 2006, Den Haag. 03. 'Kamer eist stop opslag biometrie'. In: Nieuwsbrief Bits of Freedom, nr. 4.5, 6 March 2006 (http://www.bof.nl/nieuwsbrief/nieuwsbrief_2006_5.html, visited 29 June 2006). 04. 'Kamer eist stop op opslag gelaatsscans en vingerafdrukken'. In: De Volkskrant, 25 February 2006 (http://www.volkskrant.nl/den_haag/article231026.ece (visited 5 July 2006). 05. 'De wereld van Orwell lijkt bijna onvermijdelijk' In: De Volkskrant, 25 February 2006 (http://www.volkskrant.nl/binnenland/article231020.ece (visited 5 July 2006). 06. '2006: het jaar van het biometrisch paspoort', 6 January 2006

(http://www.netkwesties.nl/editie138/artikel1.html, visited 5 July 2006).

07. ''RFID tag' - the rude words ID card ministers won't say: Lengthy descriptions of duck, but no d-word', 30 January 2006 (http://www.theregister.co.uk/2006/01/30/burnham_rfid_evasions/, visited 6 July 2006).

08. EBP (2006) Biometrics in Europe: Trend report. Brussels: European Biometrics Portal (http://www.europeanbiometrics.info/images/resources/112_165_file.pdf, visited 28 July 2006).

09. 'Chips op Belgische identiteitskaarten verwisseld', 30 August 2006 (http://www.clubmetro.nl/index.php?actie=nieuws&c=1&id=64223, visited 31 August 2006).

10. 'Rfid-paspoort vol met beveiligingslekken', 3 August 2006 (http://www.webwereld.nl/articles/42291/rfid-paspoort-vol-met-beveiligingslekken.html, visited 4 August 2006).

11. Kc, G.S. & P.A. Karger (2005) Preventing attacks on MRTDs, http://eprint.iacr.org/2005/404.pdf (visited 25-07-06).

12. 'SE: Biometric passports introduced in Sweden and Norway', 07 October 2005 (http://europa.eu.int/idabc/en/document/4792/194, visited 25 July 2006).

13. 'Nederlands paspoort al gekraakt voordat het uit is', 30 January 2006 (http://www.security.nl/article/12842/1/Nederlands_paspoort_al_gekraakt_voordat_het_uit_is.html, visited 05-07-06).

14. 'Paspoort met RFID-chip gepresenteerd: Aan de buitenkant nauwelijks anders',

25 April 2006 (http://www.zdnet.nl/news.cfm?id=55905 (14-07-06).

15. 'Italy: Decree to implement electronic passports containing biometric data: biometric data collected 'will not be stored in databases", 8 February 2006 (http://www.statewatch.org/news/2006/feb/08italy-biometric-passports.htm, visited 17 July 2006).

16. 'ID cards an interference', 27 January 2006 (http://www.mirror.co.uk/news/voiceofthemirror/tm_objectid=16633371%26method=full%26siteid=94762-name_page.html, visited 10 June 2006).

17. 'Europa wil uitstel invoering biometrisch paspoort: Gros lidstaten haalt Amerikaanse deadline niet', 5 April 2005 (http://www.zdnet.nl/news.cfm?id=44553, visited 10 July 2006).

18. 'Käuflich: Personalausweis-Daten auf Bestellung', 2 February 2006 (http://www.chip.de/news/c1_news_18539262.html, visited 6 July 2006).

19. 'Gesellschaft für Informatik lehnt Verkauf von Personalausweisdaten durch Regierung ab: Bürger werden informationell und gesundheitlich durchleuchtet', 11 April 2006 (http://de.internet.com/index.php?id=2042438&section=Security, 6 July 2006).

20. 'DE: Germany to phase-in biometric passports from November 2005', 7 October 2005 (http://europa.eu.int/idabc/en/document/4792/194, visited 25 July 2006).

21. 'Germany plans passports with biometric data in November', 2 June 2005 (http://mathaba.net/x.htm?http://mathaba.net/0_index.shtml?x=234451, visited 6 July 2006).

22. 'German group opposes sale of biometric passport data: Government planned to fund changeover with sale of personal info', 11 April 2006 (http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=110413, visited 6 July 2006).

23. 'Europese Commissie legt regels vast voor vingerafdrukken op paspoort', 29 June 2006 (http://ipsnews.be/news.php?idnews=7340, visited 10 June 2007).

24. 'Stille Post im digitalen Dorf', 4 February 2006 (http://www.heise.de/tp/r4/artikel/21/21937/1.html, visited 6 July 2006).

25. 'E-passports without the big picture', Hoepman & Jacobs, 20 February 2006 (http://www.egovmonitor.com/node/4716, 17 July 2006).

26. Hoepman et al. Crossing Borders: Security and Privacy Issues of the European e-Passport. Nijmegen: Radboud University, unpublished.

27. IPTS (2005). Biometrics at the Frontiers: Assessing the Impact on Society, February 2005,

European Commission; Joint Research Centre (http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/iptsBiometics_FullReport_eur21585en.pdf, visited 11 July 2006).

28. Juels, A., D. Molnar & D. Wagner (2005). Security and privacy issues in E-passports. Securecomm 2005 (http://eprint.iacr.org/2005/095.pdf, 25 July 2006).

29. Kamerstuk 2003-2004, 25764, nr. 005.

30. Kamerstuk 2003-2004, 25764, nr. 022.

31. Kamerstuk 2003-2004, 25764, nr. 022, Bijlage 1.

32. Kamerstuk 2003-2004, 25764, nr. 022, Bijlage 2.

33. Kamerstuk 2003-2004, 25764, nr. 022, Bijlage 3.

34. Kamerstuk 2004-2005, 25764, nr. 024.

35. Kamerstuk 2004-2005, 25764, nr. 026.

36. Kamerstuk 2004-2005, 25764, nr. 027.

37. Kamerstuk 2004-2005, 25764, nr. 027, Bijlage 1, Evaluatierapport.

38. Kamerstuk 2004-2005, 23490, nr. 350.

39. Kamerstuk 2005-2006, 25764, nr. 028.

40. Kamerstuk 2005-2006, 25764, nr. 029.

41. Jacobs, B. & R.W Schreur (2005). Security review of the biometric passport. VVSS 24 November 2005 (http://www.cs.ru.nl/~bart/TALKS/jacobs-vvss05.pdf, visited 28 July 2006).

42. KST 2293

43. http://www.bprbzk.nl/ (visited 31 July 2006).

44. http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Themen/Informationsgesellschaft/DatenundFakten/Biometrie.html (visited 31 July 2006).

45. 'Ministers plan to sell your ID card details to raise cash', The Independent,

26 June 2005 (http://www.mkno2id.org/article1.htm, visited 31 July 2006).

46. 'ID card database 'not for sale'', 26 June 2005 (http://news.bbc.co.uk/1/hi/uk_politics/4624735.stm, 31 July 2006).

47. KST 25764, 018, KST59219.

48. 'Hackers Clone E-Passports', 3 August 2006 (http://www.wired.com/news/technology/0,71521-0.html?tw=wn_technology_security_4, visited 31 August 2006).

49. http://www.rfid-paspoort.nl (visited 6 September 2006).

50. http://forum.scholieren.com/showthread.php?s=da6ff22eaf2e0c6986400111eb6e20eb&threadid=1461229 (visited 6 September 2006).

51. http://www.kraak-forum.nl/viewtopic.php?t=3127&sid=903b5e8c41f7e1dd7b3f5a6c07f413ef (visited 6 September 2006).

52. 'Lachen mag best, geen gekke bekken', AD, 2 September 2006 (http://www.ad.nl/binnenland/article593393.ece, visited 6 September 2006).

53. 'Babymondje moet dicht op pasfoto', AD, 2 September 2006 (http://www.ad.nl/binnenland/article593394.ece, visited 6 September 2006).

54. 'Scans nieuw paspoort mislukken', AD, 1 September 2006 (http://www.ad.nl/binnenland/article589867.ece, visited 6 September 2006).

55. 'Chaos pas is compleet', AD, 1 September 2006 (http://www.ad.nl/binnenland/article589933.ece, visited 6 September 2006).

56. 'RFID-paspoort laat bom afgaan' (http://tweakers.net/nieuws/43817/, visited 6 September 2006).

57. 'Most member states miss deadline for new e-Passports', 31 August 2006

	(http://euobserver.com/?aid=22304, visited 7 September 2006). 58. http://retecool.com/forum/threads.php?id=17273_0_19_0_C (visited 6 September 2006). 59. 'Nieuwe paspoort maakt de wereld niet veiliger', 25 August 2006 (http://www.parool.nl/nieuws/2006/AUG/25/bin1.html, visited 31 August 2006) 60. http://indymedia.nl/nl/2006/08/38054.shtml (visited 7 September 2006).

Case #7: AMC hospital

Case ID	# 29, level 1
Title	AMC
Researcher	Christian van 't Hof and Jesica Cornelissen
Timing	2006
Geography	Amsterdam, the Netherlands
Environment	Hospital
Technology	Passive RFID tags, PDAs
Maturity	Pilot
Function	Matching patients to blood bags
Owner	AMC
Maintainer	AMC
Users	Patients
Other actors	Doctors and nurses
ID issue	Besides matching and error prevention of blood transfusion materials, individuals working in the operation rooms (OR) are identified and localized, as well as OR-materials.
Sources	1. 'Zorgsector start proef met RFID.' (http://www.rfidnederland.nl/Default2.aspx?tabid=264, visited 13 September 2006) 2. Garfinkel, S. & Rosenberg, B. (ed.) (2006) RFID: Applications, Security and Privacy. Addison-Wesley.

Case # 8: Selexyz Scheltema SmartStore

Case ID	# 35, level 2
Title	Selexyz Scheltema SmartStore
Researcher	Jessica Cornelissen
Timing	April 2006 – present
Geography	The Netherlands (Almere)
Setting	Shopping
Environment	Bookstore (warehouse-to-consumer supply chain)
Technology	Rafsec 'Shortdipole2' UHF passive RFID tags by UPM Ralflatac, readers by CaptureTech and software applications by Progress. This provides a total back-office system called Atlas. The software system consists of Progress OpenEdge platform, Apama Event Stream Processing, Sonic Enterprise Service Bus), Progress EasyAsk [1, 12, 16].
Maturity	Operational
Function	Tracking and Tracing of products
Owner	Selexyz Bookstore (formerly Boekhandels Groep Nederland (BGN))
Maintainer	Progress Software Corporation
Users	Suppliers, customers and clerks of the bookstore
Other actors	- UPM Raflatac > supplier of tags [6] - Progress Software Corporation > design of software [7] - CaptureTech > supplier of readers [8] - 3Com > wireless components [9] - Centraal Boekhuis > supplier of books [10]
ID issue	Item-level tagging is quite well accepted for distribution and logistics application. However, the use of it in stores brings about controversy over privacy. In order to avoid negative sentiment, it is important to be very clear on the nature of data on the chips and the purposes of the system.
Sources	1. 'Progress Software pioneers retail automation with first item-level RFID and SOA deployment'. 19 April 2006 (http://www.computerworld.com.au/index.php/id;1836075961, visited 1 August 2006) 2. Malykhina, E., 'BGN is one of the first merchants to tag individual books, in a new line of stores branded "Selexyz." ' In: InformationWeek, 19 June 2006. (http://www.informationweek.com/story/showArticle.jhtml?articleID=189401951, visited 26 June 2006) 3. 'Besteld boek in Almere belt zelf met klant'. 26 April 2006 (http://www.volkskrant.nl/economie/article294564.ece/Besteld_boek_in_Almere_belt_zelf_met_klant, visited 20 June 2006) 4. Demery, P., 'With RFID tags on each book, Netherlands` BDG chain gives new meaning to speed-reading'. (http://www.internetretailer.com/internet/marketing-conference/74189-rfid-smartstore.html, visited 1 August 2006) 5. Peteghem, L. van, 'Boekhandel Almere koploper met RFID'. In: Automatisering Gids, nr. 27, 2006

6. http://www.rafsec.com/homeb.html, visited 30 August 2006
7. http://www.progress.com (visited 1 August 2006)
8. http://www.capturetech.nl/ (visited 1 August 2006)
9. http://www.3com.com (visited 1 August 2006)
10. http://www5.cbonline.nl/vni/html/ (visited 1 August 2006)
11. Vink, J. and Smit, M., 'Een RFID chip op elk product in een boekenwinkel'. 24 May 2006. Rotterdam, Emerce (http://www2.emerce.nl/downloads/selexyz.pdf, visited 1 August 2006)
12. 'First RFID Item-Level Tagged Store Opens'. 26 April 2006 (http://www.rfidupdate.com/articles/index.php?id=1103, visited 1 August 2006)
13. 'Uitgebreide rfid-proef in Almeerse boekhandel succesvol' (http://tweakers.net/nieuws/42763/Uitgebreide-rfid-proef-in-Almeerse-boekshop-succesvol.html, visited 19 July 2006)
14. 'Slimme boekwinkel draait op RFID'. In: Automatisering Gids, no. 17, 27 April 2006
15. Songini, M. L., 'Dutch bookseller creates item-level RFID system'. In: Computerworld, 8 May 2006
16. Personal observations in Selexyz Scheltema Bookstore on 29 august 2006
17. 'Nieuw. In onze winkel heeft elk boek zijn eigen chip.' (leaflet provided in the Selexyz Scheltema bookstore)
18. Interview with Mr. Jan Vink, ICT manager of BGN, on 13 September 2006

Case #9: KidSpotter Child tracking application

Case ID	36, level 3
Title	KidSpotter Child-tracking application
Researcher	Jessica Cornelissen

Timing	Launched on 27 March 2004 in LEGOLAND Billund, Denmark
Geography	Denmark
Environment	Leisure
Technology	The Child-tracking application involves four elements, which combines technologies from Theme Park Intelligence KidSpotter [9] and Aeroscout [10]: - T2 tags incorporated in a wristband or a badge clip. The technology combines active RFID detection with a Wireless LAN environment. The tags make it possible to locate any asset normally not Wi-Fi enabled and is 802.11b compatible. The tag has a battery life of 3 years and weighs 35 grams. - location receivers are placed throughout the park; roughly 40 to 50 location receivers are to be installed throughout an 150.000 square meters park. These remotely configurable receivers are housed in rugged NEMA-rated weatherproof enclosures. They can be connected to the park's network by fiber optic cable links and wireless bridges. - location server software, installed on a server with Intel Xeon processors. The core software, written in C#, manages the collection and processing of location data. - mobile communication platform handles the communication between the KidSpotter applications, the location server and the SMS gateway that sends up-to-date location information to visitors' mobile phones. [9, 2, 12, 14]
Costs	The rental fee is EUR 3 per day; (in comparison: the entrance fee is mid-EUR 20s) Installation of a location receiver costs USD 3000 to USD 4000 each. The tags cost approx. USD 85 each and the park is starting with 500 of them [11]
Maturity	Fully implemented
Function	1. A tracking and alerting system for parents 2. An information system for park management (real-time location service)
Owner	LEGOLAND Billund
Maintainer	LEGOLAND Billund
Users	Visitors of the theme-park
Other actors	
ID issue	Obtaining information about movement of visitors in the park by coupling it to a popular service (without them knowing it?).
Sources	9. http://www.kidspotter.com (visited 26 June 2006) 10. http://www.aeroscout.com (visited 26 June 2006)

11. Collins, J., 'One of Europe's largest amusement parks deploys a Wi-Fi-based RFID system that helps parents retrieve children who have wandered off.' In: RFID Journal, 28 April 2004.
12. 'Child Tracking Application at Legoland: customer case study.' AeroScout
13. 'Legoland volgt kinderen met RFID-armband' In: Automatisering Gids Webeditie, 25 June 2004.
14. 'AeroScout Visibility System Overview: data sheet.' AeroScout
15. Nash, E., 'Legoland builds safety system for kids: Windsor theme park could follow the lead of its Danish counterpart.' (http://www.iwr.co.uk/computing/news/2070665/legoland-builds-safety-system-kids, visited 26 June 2006)

Case #10: OV-chip Kaart

Case ID	56, level 3
Title	OV-chip Kaart
Researcher	Christian van 't Hof and Sil Wijma
Timing	2005 – 2007
Geography	The Netherlands
Environment	Public Transport
Technology	ID card with passive tag, rewritable Readers installed at the entrance and exit of the different means of public transport. Central database controls payments and profiles travellers. East West builds and maintains the system [22, 34].
Costs	Starting costs: according to one source more than one billion euro [8]. The total costs are probably around EUR 1.5 billion [33]. The government only pays a small part of this: the pilots were supposed to cost EUR 7.8 and the total implementation EUR 90 million [23]. Later more money was needed up to a total of EUR 129 million [38].
Maturity	Different pilots. A pilot runs in the city of Rotterdam, while the card will be implemented in the whole Dutch public transport system in 2007.
Function	Payments
Owner	Trans Link Systems (TLS), a consortium of the five larges public transport companies in the Netherlands, representing 80% of the Dutch market.
Maintainer	East West
Users	Dutch users of the public transport, trains, busses, subway, etc.
Other actors	- Different organizations: CBP (College Bescherming Persoonsgegevens), Landelijk Overleg Consumentenbelangen Openbaar Vervoer (Locov), Landelijke Campagneteam invoering OV-chipkaart (Lcov), EastWest - Different consumer organizations: Consumentenbond, Rover, Bits of Freedom - Different public transport operators: NS (Dutch Railways), TLS, GVB, RET, Connexxion, HTM, Mobis
ID issue	The OV-chip card is used both for payment and profiling travellers' behaviour. Users have two choices in managing their identity: being profiled while travelling with a personal card or anonymous travelling with an anonymous card and fewer possibilities. The case revolves around the question as to whether travellers have a fair and clear opt in or opt out choice.
Sources	01. "NS schendt privacy" In: Volkskrant. 20 February 2006. 02. 'CBP legt OV-chipkaart aan banden'. In: Bits of Freedom nieuwsbrief, Nr. 4.5, 6 March 2006 (http://www.bof.nl/nieuwsbrief/nieuwsbrief_2006_5.html, visited 29 June 2006). 03. 'Pechtold ziet geen problemen met RFID'. In: Automatiseringgids, 11 May 2006 04. CBP 'Visie CBP chipkaart', 16 November 2005 (http://www.cbpweb.nl/downloads_overig/z2004-0850_ov_chipkrt_visie_CBP.pdf?refer=true&theme=purple, visited 20 June 2006). 05. CBP 'brief over chipkaart' (http://www.cbpweb.nl/downloads_uit/z2004-0850.pdf?refer=true&theme=purple, visited 20 June 2006). 06. 'Waarom vertrouwen jullie de klant niet?'. In: Volkskrant, 20 February 2006 (http://www.volkskrant.nl/binnenland/article224714.ece/Waarom_vertrouwen_jullie_de_klant_niet,

visited 20 June 2006).

07. Ejure.nl, 'Commentaar eJure op de OV chipkaart' (http://www.ejure.nl/mode=display/downloads/dossier_id=49/id=371/Commentaar_eJure_op_de_OV_chipkaart.pdf, visited 26 June 2006).

08. 'OV-chipkaart ook in Amsterdam te gebruiken', 31 July 2006 (http://www.clubmetro.nl/index.php?actie=nieuws&c=2&id=61561, visited 2 August 2006).

09. http://www.ov-chipkaart.nl (visited 22 June 2006).

10. http://www.verkeerenwaterstaat.nl/Images/G0-besluit%20OV-Chipkaart_tcm195-160470.pdf?dossierURI=tcm:195-15678-4 (visited 26 June 2006).

11. 'Ook tram-, bus- en metrovervoer wil gegevens opslaan'. In: Telegraaf, 21 February 2006 (http://www.telegraaf.nl/binnenland/33944341/Ook_tram___bus__en_metrovervoer_wil_gegevens_opslaan.html (visited 26 June 2006).

12. 'Spitsreiziger 10 procent duurder uit'. In: De Volkskrant, 11 April 2006 (http://www.volkskrant.nl/binnenland/article278824.ece/Spitsreiziger_10%C2%A0procent_duurder_uit, visited 11 July 2006).

13. LOCOV (2005) Advies kaartproposities OV-chipkaart, 26 April 2005, http://www.minvenw.nl/cend/overlegorganen/locov/uitgebrachte_adviezen/2005/Index33.aspx#0 (visited 23 June 2006).

14. 'OV-chipkaart mag vervoer niet duurder maken', 12 April 2006 (http://www.consumentenbond.nl/nieuws/nieuws/Archief/2006/4093170?ticket=nietlid, visited 11 July 2006).

15. 'Consumentenorganisaties willen uitstel besluit OV-chipkaart', 11 May 2006 (http://www.consumentenbond.nl/nieuws/nieuws/Archief/2006/4339524?ticket=nietlid visited, 11 July 2006).

16. 'Doorgaan met OV-Chipkaart', 28 June 2006 (http://www.rover.nl/nieuws/berichten/berichten.php?id=ber060629, visited 11 July 2006).

17. 'Extra jaar voor invoering OV-chipkaart hard nodig', 13 June 2006 (http://www.rover.nl/nieuws/berichten/berichten.php?id=ber060613, visited 11 July 2006).

18. 'Als de poortjes maar hufterproof zijn'. In: NRC Handelsblad, 30 May 2006 (http://www.nrc.nl/binnenland/article335132.ece, visited 22 June 2006).

19. The chip card for public transport in The Netherlands. 2004, EastWest (http://www.eastwestconsortium.nl/downloads/presentation.pdf, 28 July 2006).

20. Kamerstuk 2003-2004, 23645, nr. 061

21. Kamerstuk 2003-2004, 23645, nr. 074

22. Kamerstuk 2003-2004, 23645, nr. 074, Bijlage 2511

23. Kamerstuk 2004-2005, 23645, nr. 078

24. Kamerstuk 2004-2005, 23645, nr. 078, Bijlage 3135

25. Kamerstuk 2004-2005, 23645, nr. 084

26. Kamerstuk 2004-2005, 23645, nr. 085

27. Kamerstuk 2004-2005, 23645, nr. 088

28. Kamerstuk 2004-2005, 23645, nr. 093

29. Kamerstuk 2004-2005, 23645, nr. 095

30. Kamerstuk 2004-2005, 23645, nr. 101

31. Kamerstuk 2005-2006, 23645, nr. 111

32. Kamerstuk 2005-2006, 23645, nr. 114

33. Kamerstuk 2005-2006, 23645, nr. 119

34. Kamerstuk 2005-2006, 23645, nr. 123

35. Kamerstuk 2005-2006, 23645, nr. 135

36. Kamerstuk 2005-2006, 23645, nr. 136

37. Kamerstuk 2005-2006, 23645, nr. 139

38. Kamerstuk 2005-2006, 23645, nr. 141

39. 'Stand van zaken invoering OV kaart' (http://www.verkeerenwaterstaat.nl/Images/br%2E873%20stand%20van%20zaken%20invoering%20OV-Chipkaart%20-%20%20%20%20www%2Everkeerenwaterstaat%2Enl%20cend%20bsg%20brieven%20data_tcm195-134235.pdf?dossierURI=tcm:195-15678-4, visited 26 June 2006).

40. 'Strippenkaart wordt OV-chipkaart'. In: Trouw, 28 June 2006 (http://www.trouw.nl/laatstenieuws/ln_binnenland/article362227.ece/Strippenkaart_wordt_OV-chipkaart?backlink=true (29-06-06).

41. RET verzamelt reizigersinfo met chipkaart'. In: AD, 18 June 2006 (http://www.ad.nl/rotterdam/article413455.ece, 22 June 2006).

42. 'Reactie van CBP op E-jure over OV' (http://www.ejure.nl/downloads/dossier_id=49/id=371/show.html, visited 26 June 2006).

43. 'Axalto selected for world's first national project covering all transport modes', 27 July 2004 (http://www.rfidnews.org/news/2004/07/27/axalto-selected-for-worlds-first-national-project-covering-all-transport-modes/, visited 28 July 2006).

44. 'Nederland open voor OV-chipkaart', 11 November 2003 (http://www.tns-nipo.com/, visited 11 July 2006).

45. KST 23645, 141, bijlage 1

46. KST 23645, 141, Bijlage 2

47. KST 23645, 141, Bijlage 3

48. KST 23645, 141, Bijlage 4

49. KST 23645, 141, Bijlage 5

50. KST 23645, 141, Bijlage 6

51. 'OV-chipkaart van start zonder duidelijkheid over privacy'. In: Bits of Freedom nieuwsbrief, Nr. 4.13, 21 June 2006 (http://www.bof.nl/nieuwsbrief/nieuwsbrief_2006_13.html, visited 31 July 2006).

52. http://nl.wikipedia.org/wiki/OV-chipkaart (visited 1 September 2006).

53. http://forum.trosradar.nl/viewtopic.php?t=24738&postdays=0&postorder=asc&start=30&sid=53f4c33df9a33cdf31dcc10abc280711 (visited 8 September 2006).

54. http://tweakers.net/nieuws/43150/Bits-of-Freedom-twijfelt-aan-privacywaarborgen-OV-chipkaart.html (visited 8 September 2006).

56. 'Ov-chipkaart vernietigt sociaal kapitaal', 26 June 2006 (http://www.refdag.nl/artikel/1265566/Ov-chipkaart+vernietigt+sociaal+kapitaal.html, visited 8 September 2006)

57. Several site visits by Christian van 't Hof and Chris de Jongh

Case #11: Transport for London (Oyster card)

Case ID	61, level 1
Title	Transport for London (Oyster card)
Researcher	Christian van 't Hof and Sil Wijma
Timing	2002–2006
Geography	London, UK
Environment	Public transport
Technology	Philips Semiconductors' MIFARE Standard 1 Kbyte ICs in G&D and SchlumbergerSema cards [3]
Maturity	Fully operational
Function	Payment
Owner	Transport for London, TranSys
Maintainer	Who maintains the database and readers?
Users	Who uses the RFID tags to move through the environment
Other actors	TranSys (consortium of Cubic, EDS, Fujitsu and WS Atkins), Transport for London (TfL) and London Underground Limited (LUL)
ID issue	When purchasing the Oyster Card, full personal details are required [11] The police are very interested in using the journey data that is stored from travellers who use the Oyster card. The number of requests from the police has risen from seven in 2004 to 61 requests made in January 2006 alone [4]. A spokesman of TfL said: "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. "A very few authorized 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. [4]. People are using the information that is stored from the journeys made with a Oyster card to track their partners' movements. The data is accessible through machines at stations and via a website whereby only the registration number is required. This source states that this data is kept for ten weeks [9].
Sources	1. http://www.tfl.gov.uk/tfl/fares-tickets/oyster/general.asp (visited 27 July 2006). 2. http://en.wikipedia.org/wiki/Oyster_card (visited 27 July 2006). 3. 'Easing travel in London's congested public transport network' (http://mifare.net/showcases/london.asp, visited 27 July 2006). 4. 'Oyster data use rises in crime clampdown', 13 March 2006 (http://www.guardian.co.uk/uk_news/story/0,1729999,00.html?gusrc=rss, visited 27 July

	2005). 5. 'Transport Secretary and Mayor of London announce new Oyster deal' Press Release, 10 May 2006 (http://www.london.gov.uk/view_press_release.jsp?releaseid=8032, visited 27 July 2006). 6. 'Is this end for notes and coins? Patrick Collinson and Tony Levene on the 'tap and go' card', 15 April 2006 (http://money.guardian.co.uk/consumernews/story/0,1754069,00.html, visited 27 July 2006). 7. ''£50,000 lost' in Oyster failure' (http://news.bbc.co.uk/1/hi/england/london/4335291.stm, visited 27 July 2006). 8. 'Inquiry into Tube's Oyster card', 23 January 2004 (http://news.bbc.co.uk/1/hi/england/london/3422051.stm, visited 27 July 2006). 9. 'And the next witness is.... an Oyster Card', 22 February 2006 (http://london-underground.blogspot.com/2006_02_01_london-underground_archive.html#114059551043902945, visited 31 July 2006). 10. http://www.tfl.gov.uk/tfl/fares-tickets/oyster/general.asp 11. User application form: https://sales.Oyster Card.com/oyster/lul/basket.do

Case #12: Detention Concept Lelystad

Case ID	# 66, level 2
Title	Detention Concept Lelystad
Researcher	Jessica Cornelissen

Timing	January - December 2006
Geography	The Netherlands, Lelystad
Setting	Work
Environment	Prison
Technology	Active RFID tag incorporated in non-removable bracelets for prisoners [1] and in key-chains for wards. Two types of location measurements are tested: triangular locating and zone locating. triangular locating was developed in a cooperation of KPN, Geodan, Aeroscout and Tsilink Hardware. The zone locating was developed by Transquest and Wavetrend [17]. DJI controls the following applications and/or data [16, 19]: - Selection of activities that inmates can choose - Linkage of an inmate to his/hers wristband - Giving out information about inmates to thirds parties - Managing inmate dossier (checking out of inmates) - Planning of activities - Software for handheld computers (PDA's) - Login into a personal prisoner information system using the wristband
Maturity	Pilot
Function	- Information on inmate's stay (security and monitoring) - Planning of daily schedule - Keeping record of inmate's credits - Information on personnel [17]
Owner	DJI (Penitentiary Lelystad)
Maintainer	DJI's 'Shared Service Centre' [6, 16]
Users	Wards and prisoners enrolled in the trial
Other actors	- Van de Geijn Partners ketenarchitecten > design of total detention concept [2] - Ministry of Justice [3] - DIGIT Touch Systems > supply of touch screens [4] - Geodan (KPN, Aeroscout, Tsilink Hardware) > software and hardware design [5] - Transquest and Wavetrend > software and hardware design [7, 8] - Supporting parties like the food supplier

ID issue	The use of constant surveillance brings some controversy and 'Big Brother-scenarios' can easily be related to this case. Applying it to punish or reward a person goes even further. However, it remains debatable how much privacy rights imprisoned people (should) have. Besides the prisoners being constantly monitored, the wardens are also under permanent surveillance. This brings about a different employer-employee relationship in which the employees' privacy could be impinged. It could be seen as a trade-off between being monitored and being more secure at work. It appears as though realization of the possible consequences of the technology came in time. Addressing concerns and allowing for a dialogue between employer and employees can facilitate in the acceptance of a new technology.
Sources	1. http://www.wavetrend.net/content.asp?IDS=126 (visited 25 July 2006) 2. http://www.vdgp.nl (visited 27 June 2006) 3. http://www.minjus.nl/ (visited 26 July 2006) 4. http://www.digit.nl (visited 26 July 2006) 5. http://www.geodan.nl (visited 27 June 2006) 6. http://www.dji.nl (visited 26 July 2006) 7. http://www.transquest.nl (visited 22 August 2006) 8. http://www.wavetrend.net (visited 22 August 2006) 9. 'Een nieuwe manier van strafuitvoering' (http://www.dji.nl/main.asp?pid=251, visited 26 July 2006) 10. Stordiau-van Egmond, A.M.E., 'Uitnodiging perspresentatie detentieconcept Lelystad' http://www.perssupport.anp.nl/Home/Persberichten/Actueel?itemId=74217, visited 26 July 2006) 11. 'Prison of the future: Detention Concept Lelystad' (http://www.geodan.nl/en/markets/public-order-and-safety/detention-concept-lelystad/, visited 25 July 2006) 12. 'Modernste gevangenis van Europa voorzien van nieuwste technologie: DIGIT Touch Systems / Creative Action voorzien modernste gevangenis van Europa in Lelystad van nieuwste technologie' (http://www.perssupport.nl/Home/Persberichten/Actueel?itemId=74659&show=true, visited 26 July 2006) 13. Maurits, R. 'Nederlandse gevangenen bewaakt via RFID-chip: ook uitgebreide multimediavoorzieningen in cellen.' 24 January 2006. (http://www.zdnet.be/news.cfm?id=53006&mxp=109, visited 6 July 2006) 14. 'Gevangen in ketens: modernste gevangenis: opvallend resultaat van gedurfde visie.' (http://www.vdgp.nl/bbcms/assets/pdf%20bestanden/Gevangen%20in%20ketens.pdf, visited 25 July 2006) 15. ''Big Brother Bajes' nu al omstreden'. In: Algemeen Dagblad, 30 May 2006. 16. Bouwman, R., 'Digitale detentie gooit gevangenis 'open''. In: Livre Magazine, February 2006. 17. Personal communications with a representative of Van de Geijn Ketenpartners, 26 July 2006 18. Comment by 'reginav' on 12 March 2006 (https://secure.lsit.ucsb.edu/phpbb/viewtopic.php?t=297&sid=db0cb28e98afac6130a8f66cbb5b9d9c, visited 31 July 2006) 19. Personal communications with a representative of Van de Geijn Ketenpartners, 1 September 2006 and 4 September 2006

Case #13: SI.PASS

Case ID	84, level 1
Title	SI.PASS
Researcher	Elisabetta El-Karimy
Timing	2006
Geography	Torino, Italy
Environment	Public transport / traffic
Technology	Developed by Norwegian company Q-Free on behalf of the Italian transport operator SITAF, the SI-PASS is a two-piece tag consisting of an on-board unit, called a Transponder Mobipass, and a Smart Card. SI-PASS integrates two payment systems using ASK's TanGO-based CT4002 contactless smart cards and active RFID tags for long-range payments. [6] The Smart Card itself is a readable card consisting of a microchip with a double interface (contact and contactless) that uses tag and beacon technology. Operated by microwave dedicated short-range communications (DSCR) at 5.8GHz, the system is compatible with European standards. Operation of SI-PASS is based on two very simple mechanisms. When the card is used with the Transponder it allows motorway barriers to be opened from a distance without the need to stop at motorway tolls. On its own, the card can be read by a scanner, enabling the user to automatically pay for public city transport (buses, trams and underground) in addition to a large number of car parks. For the Turin Winter Olympics, the card was also used to pay for ski-passes and had the capacity to gain access to other events. [7]
Costs	Customers pay EUR 100-170 plus EUR 20 deposit for Transponder
Maturity	Just implemented
Function	Access / payment
Owner	SITAF
Maintainer	SITAF
Users	Visitors to Winter Olympic Games and users of Frejus highway tunnel and the A32 highway
Other actors	ASK, Gruppo Torinese Trasporti (GTT), Societa Italiana Traforo Autostrade del Frejus (SITAF), Centro Ricerche Fiat (CRF, Q-Free ASA (Norwegian company for electronic toll collection systems), city car parks and public transport (Trenitalia and 27 private operators), Torino Turismo (museums, concerts, car and bike rental, etc.)
ID issue	"This new system will not only help us to combat fraud but also enable us to collect data so that we can offer customized fares and value added services to travellers, says Mr. Aliverti, Sales Director, GTT."[1]. “The Smart Card is very much like the Oyster card that is already employed across London. The difference here is that it can automatically debit users as they travel around a city. Unlike the Congestion charging zone in London, users will not have to make individual payments for each journey they make and can use the card across a number of mobility services.” [7] It is not clear what information will be collected besides data on the movement of vehicles. “We are one of the first companies in the world to offer contactless smart cards for both toll payment and public transport, says Mr. Ugo Jalasse, director, SITAF. The versatility of ASK’s TanGO platform allows us

	to combine GTT transport services with our own, making public transport at this year's Winter Olympic Games a smooth and uncomplicated experience." [1] GTT manages the public transport networks in Torino and its suburbs. Whilst season ticket-holders tend to use new GTT dual interface card, there are 4 different contactless paper tickets (C.ticket®) to meet the needs of other users: a pass for school children, a multimodal pass, a pass for tourists and tickets to museums and galleries. [1] According to the GTT-site the tickets are equipped with magnetic bands [2]. The usefulness of such combination card for payment of toll and public transport beyond the Olympics is not addressed. When purchasing the Torino Card, the customer consents to the processing of personal data: "Personal data is collected solely for employment-related purposes or for use in connection with other such matters. Personal data shall be disclosed or made accessible to third parties exclusively for the aforementioned purposes. TURISMO TORINO hereby guarantees that anyone may request access to their personal data at any moment in order to up-date, change or supplement such data, and may oppose such data being used for the purposes given above."[8] It is not clear what 'employment-related purposes' implies. This disclaimer does not prevent the data of the Torino Card to being passed on to SI-PASS systems. No privacy information is provided on the SI-PASS website. For future use, the possibility has been considered of employing SI-PASS to effect toll payments with the help of satellite technology, such as is already in use for heavy goods in Germany (TOLL COLLECT). The telematic platform has been devised to expand the functionality of the system, in particular to give out information on traffic flow and to integrate with working systems on road security (such as INFONEBBIA). [10] But also other linkages of the SI-PASS transponder with other chipcards can be envisioned, such as could as credit cards and cash cards. [3]
Sources	All visited 14 September 2006 1. ASK.com, producer of card 'Torino 2006 on the Right Track With ASK Contactless Smart Card Technology' http://www.ask.fr/uk/news/news_article.php4?id=3 2. County of Torino where technology was implemented http://www.comune.torino.it/gtt/en/olympicgames/tickets.shtml (visited 05 July 2006). 3. Homepage of SI-PASS device http://www.sipass.it/on-line/Sipass/Home/SIPASS.html 4. On Olympic Games organization http://www.kataweb.it/spec/articolo_speciale.jsp?ids=1251016&id=1251040 5. On transportation and Olympic Games organization http://www.radio.rai.it/cciss/view.cfm?Q_EV_ID=162476&Q_TIP_ID=328 6. RFID news Italy homepage http://www.rfidnews.it/news.asp?id=230 7. Q-Free website, Europe's leading supplier of electronic toll collection (ETC) systems http://www.intertraffic.com/marketplace/mypage/pressreleases_detail.asp?mypageid=1102&newsid=581 8. Turismo Torino on Torino Card http://www.turismotorino.org/uploads/4/1925_Torino_Card_2006.pdf 9. http://www.traspi.net/notizia.asp?IDNotizia=7467 10. Centro Ricerche Fiat http://www.crf.it/C/C7_1.htm

Case #14: Madesjki Smart Stadium

Case ID	# 88, level 3
Title	Smart Stadium Solution at the Madejski Stadium
Researcher	Jessica Cornelissen

Timing	2004
Geography	United Kingdom (Reading)
Setting	Leisure
Environment	Stadium

Technology	Smart Stadium Solution developed by Fortress GB [16].
	
	It offers the following modules [42]:
	- SmartTicketing
	  - Virtual ticket
	  - New outlets – scratch card
	  - New outlets - kiosks
	  - Membership scheme
	  - Buy-back scheme
	  - Concession upgrades
	
	- SmartAccess
	  - Multiple Ticket Types
	  - Independent Rule Engine
	  - Visual “traffic light” indicators
	  - Offline capabilities
	  - Dynamic reallocations
	  - Evacuation reset
	
	- SmartController
	  - Detailed access report
	  - Ticket verification
	  - Real-time Access reporting
	  - White / Watch list
	  - Real-time card blocking
	  - Steward time & attendance
	
	- SmartCRM (Customer Relationship Management)
	  - Fan Loyalty scheme
	  - Integration with ticketing

	- FlowPayments
	  - E-Purse
	  - Merchandise Kiosks
	  - Gift Vouchers
	
	The Madejski stadium uses both plastic RFID cards (member cards and season tickets) and one-off paper tickets (with a barcode or RFID chip). Chips are passive and encrypted. There are RFID readers installed in all the turnstiles [16, 41, 42].
	
	The system software offers the Time Attendance Monitor (TAM) option. TAM gives information on [41]:
	- ID-number of the card or ticket
	- Name of the carrier
	- Time of entrance
	- Status of ticket (e.g., access to which game and through which entrance)
	- Status of carrier (e.g., blocked card, watch-listed or black-listed person)
	- Area and turnstile of entrance
	
	Some statistical analysis can be done with the TAM, both real-time and afterwards, like [41]:
	- number of people entering the total stadium
	- number of entries through each turnstile
	- division of season passes, member cards and one-time tickets
	
	In the ground, there are service personnel equipped with pocket computers (PDA's). These PDA's are linked to the central database through a wireless network, meaning that information is uploaded and downloaded real-time. On a PDA, one can access one's card-history by entering the ticket-number. The tickets cannot be read by the PDA using RF [41].
	
	Fortress GB has also developed the so-called Smart Campus Solution and Smart School Solution. These are similar to the Smart Stadium Solution and use the same type of smartcard [16].

Maturity	Implemented
Function	ID / AC / (PA) / IC / IS
Owner	Madejski Stadium
Maintainer	Madejski Stadium, IT department
Users	Supporters, corporate guests and staff of the stadium or clubs playing in the stadium (home clubs of the Madejski Stadium are Reading Football Club and London Irish Rugby Football Club)

Other actors	- Fortress GB's Technology Partners [42]
	
	- Stadiums using the Smart Stadium Solution:
	  - Color Line Stadium in Norway [20]
	  - Headingley Carnegie Stadium in United Kingdom [21]
	  - Åråsen stadion in Norway [22]
	  - Anfield Stadium in United Kingdom [23]

	- Kiryat Eliezer in Israel [24] - Carrow Road in United Kingdom [25] - Stor Stadium in Norway [26] - JJB Stadium in United Kingdom [27] - Viking Stadium in Norway [28] - Emirates Stadium in United Kingdom [29] - Kristiansand Stadium in Norway [30] - City of Manchester Stadium [31] - Giuseppe Meazza Stadium in Italy [32] - Upton Park Stadium in United Kingdom [33] - Venues using the Smart Campus Solution - Bristol City Academy in United Kingdom [34] - University of Hertfordshire in United Kingdom [35] - London South Bank University [36] - Gwernyfed High School in United Kingdom [37] - Little Ilford School in United Kingdom [38] - Thames Valley University in United Kingdom [39] - Fan clubs [17, 34]
ID issue	It seems that the loyalty of the supporter surpasses the will to remain completely anonymous, all for the sake of the game. Supporters are fine with their club using the information and are happy to benefit from it through a loyalty scheme. On the other hand, they do not agree on the use of the system by any third party.
Sources	16. http://www.fortressgb.com (visited 31 July 2006) 17. http://www.backtheboys.com (visited 31 July 2006) 18. 'IBM Case Study: Manchester City Football Club scores a home win with IBM and Software4Sport, part of Computer Software Group.' 18 March 2004 (http://www-306.ibm.com/software/success/cssdb.nsf/CS/DNSD-5X5LK3?OpenDocument&Site=, visited 27 July 2006) 19. Booty, F., 'Reading FC and London Irish Rugby FC keep ahead of the game.' 25 October 2004. (http://www.iseriesnetwork.com/nodeuk/ukarchive/index.cfm?fuseaction=viewarticle&CO_ContentID=19530, visited 27 July 2006) 20. http://www.colorlinestadion.no (visited 23 August 2006) 21. http://www.leedsrugby.com (visited 23 August 2006) 22. http://www.lsk.no (visited 23 August 2006) 23. http://www.newanfield.co.uk (visited 23 August 2006) 24. http://maccabi-haifafc.walla.co.il (visited 23 August 2006) 25. http://www.canaries.premiumtv.co.uk (visited 23 August 2006) 26. http://www.sandefjordfotball.no (visited 23 August 2006) 27. http://www.jjbstadium.co.uk (visited 23 August 2006) 28. http://www.viking-fk.no (visited 23 August 2006)

29. http://www.arsenal.com (visited 23 August 2006)
30. http://www.ikstart.no (visited 23 August 2006)
31. http://www.mcfc.co.uk (visited 23 August 2006)
32. http://www.sansiro.net (visited 23 August 2006)
33. http://www.whufc.com (visited 23 August 2006)
34. http://www.cityacademybristol.co.uk (visited 23 August 2006)
35. http://perseus.herts.ac.uk (visited 23 August 2006)
36. http://www.lsbu.ac.uk (visited 23 August 2006)
37. http://www.gwernyfed-hs.powys.sch.uk/ (visited 23 August 2006)
38. http://www.littleilford.newham.sch.uk (visited 23 August 2006)
39. http://www.tvu.ac.uk (visited 23 August 2006)
40. http://www.lisc.org.uk (visited 23 August 2006)
41. Interview with Mr. G. Hanson, IT manager at the Madejski Stadium, on 2 August 2006
42. 'Smart Stadium Presentation: brought to you by FortressGB'. Personal communication with Mr. J. Rosenthal, Legal Counsel at FortressGB, on 2 August 2006
43. Interview with a season pass holder and a steward, on 2 August 2006
44. 'Member Card Application' In: Supporters' Guide: premiership 2006/07
45. http://www.stadiacard.com/products/index.php?id=4 (visited 23 August 2006)
46. Interview with a member card holder, on 1 and 11 September 2006
47. Interview with a member card holder, on 9 August and 13 September 2006

Case #15: TopGuard Patrol

Case ID	# 91, level 1
Title	TopGuard Patrol
Researcher	Jessica Cornelissen
Timing	Unknown
Geography	Worldwide
Setting	Work
Environment	Outsourced services (guarding, maintenance, recording service activities, cleaning, attendance [24])
Technology	GCS ProxiPen Data Collection Unit (RFID reader operating at 125 KHz and reading range 3 – 18 mm) GCS TopGuard Patrol reporting software Passive RFID tags on checkpoint and incidents ('Unique' and 'Nova' World Tag) and on personnel (Guard Identification Tag, either a 'ISO Card Unique' magnetic stripe card, 'Tear Shape Unique' key fob or 'Unique' wrist band) by Sokymat [23, 24, 25]
Maturity	Operational
Function	To provide an unfalsifiable record of services which must be performed at predetermined times and places [25].
Owner	Guard Control Systems [25]
Maintainer	Companies executing patrolling services
Users	- Companies and personnel executing patrolling missions - Companies out-sourcing patrolling services
Other actors	- Sokymat, provider of tags [26] - Distributors of the system, worldwide
ID issue	This application makes it possible for employers to follow employees throughout their shift. This brings has consequences for the relationship between employers and employees.
Sources	23. 'Finally! Proof to back up Service Performance.' (http://www.practicalfm.co.uk/shownews.asp?search_type=id&id=72199, visited 25 August 2006) 24. 'ProxiPen: the New Compact Reader for RFID Tags' (http://iccdata.com/proxipen.htm, visited 25 August 2006) 25. http://www.gcscontrol.com (visited 28 August 2006) 26. http://www.sokymat.com (visited 28 August 2006)

Case #16: NWO Office

Case ID	# 096, level 3
Title	NWO Office
Researcher	Jessica Cornelissen and Christian van 't hof

Timing	2005 – present
Geography	The Netherlands (The Hague)
Setting	Work
Environment	Office building
Technology	Passive, 125 KHz RFID tags (HID ProxKey) and HID MiniProx readers [50]
Maturity	Operational
Function	Access
Owner	Information and system management of the NWO office building
Maintainer	Installerende Partners
Users	Employees at the NWO office building
Other actors	- HID [52] - Installalrende Partners [51]
ID issue	The system offers several possibilities to track employees more thoroughly than is being done at present. However, management is not using these possibilities. There has been no concern among employees working in the office building. This could be because they are very poorly informed about the system or because the application is accepted as it is right now.
Sources	48. Personal observations 49. Interview with Mr. Cees Besseling, Information and system management, system administrator of the NWO office building, on 18 July 2006. 50. 'Proxkey II' (http://www.hidcorp.com/pdfs/products/proxkey2.pdf, visited 11 September 2006) 51. http://www.ipgroep.nl (visited 11 September 2006) 52. http://www.hidcorp.com (visited 11 September 2006)

Case #17: Liber-T

Case ID	# 108, level 1
Title	Liber-T
Researcher	Jessica Cornelissen

Timing	Unknown
Geography	France
Setting	Car
Environment	Toll roads
Technology	Read/write/rewrite tags installed in the vehicle. Reader installed in the entry or exit gates.
Maturity	Operational
Function	Automatic charging of toll fee.
Owner	The Federation of French motorway and toll facility companies (ASFA) and the French toll-companies (ALIS, AREA, ATMB, Autoroutes Paris-Rhin-Rhone, CCI du Havre, COFIROUTE, ASF / ESCOTA, SANEF, SAPN, SFTRF, SMTPC) [53]
Maintainer	French toll-companies
Users	Subscribers to the Liber-T system (In 2005 there were almost 1.5 million subscribers and there have been 179 transactions per tag per year [54].
Other actors	
ID issue	This system will provide information about the journeys a subscriber makes. The information could be used for marketing purposes, though there is no indication that this happens at this moment. It seems that users see the RFID system in relation to other technologies; there are other ways in which information can be gathered so why cause a commotion over this particular technology? The 'age of time' and 'running the business means knowing things about you' seems to settle doubts.
Sources	53.http://www.autoroutes.fr/asfa/qui.php?lng=2 (visited 7 July 2006) 54.'Key figures 2005: French tolled motorway facilities network.' (http://www.autoroutes.fr/upload/institutionnelle/cles2005-EN.pdf) 55.'Liber-T: the French toll system' (http://www.autoroutes.fr/upload/institutionnelle/telepeagedoc) 56.http://www.sanef.fr/fr/ecommerce/particulier/decouvre.jsp (visited 7 July 2006) 57.French Toll Road Operators (2002) Knowing our costumers (http://www.sanef.fr/fr/ecommerce/particulier/decouvre.jsp, visited 14 July 2006). 58.'Liber-T, The French toll system' (http://www.autoroutes.fr/upload/institutionnelle/telepeagedoc.pdf, visited 7 July 2006) 59.Comment by 'MarK' on 4 September 2006 (http://www.frankrijkforum.nl/index.php?link=home/lees.php&id=84195&reactieid=8430 0, visited 5 September 2006) 60.Comment by 'Mariette 58' on 4 September 2006 (http://www.frankrijkforum.nl/index.php?link=home/lees.php&id=84195&reactieid=8430

	0, visited 5 September 2006) 61. Comment by 'pwi' on 4 September 2006 (http://www.frankrijkforum.nl/index.php?link=home/lees.php&id=84195&reactieid=8430 0, visited 5 September 2006)

Case #18: VRR/VRS

Case ID	#123, Level 1
Title	VRR/VRS
Researcher	Christian van 't Hof, Sil Wijma and Eefje Vromans
Timing	2003
Geography	Germany, region of North-Rhine-Westphalia
Environment	public transport
Technology	ASK MV5100 dual-interface contactless smartcards Contactless mode for transit applications (RFID), contacted mode for e-purse application (chip)
Costs	RFID Implementation costs: EUR 33million [6]
Maturity	Fully operational
Function	Payment
Owner	Verkehrsverbund Rhein-Ruhr (VRR) and Verkehrsverbund Rhein-Sieg (VRS)
Maintainer	Card.etc AG (general contractor) and KompetenzCenter EFM (Automatic fare collection) [?]
Users	Travellers
Other actors	• Transport operators: VRR and VRS represent 54 different transport operators • Card supplier: ASK S.A. • VDV (the association of public transport in Germany) [1] • FoeBud e.V. (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V)
ID issue	By using RFID in public transport it becomes possible to track person's movements [2].
Sources	[1]. RFIDnews.org (2003) 'ASK Delivers 1.7 Million Contactless Cards for Largest Transit Smart Card Project in Europe', 21 May 2003 (http://www.rfidnews.org/news/2003/05/21/ask-delivers-17-million-contactless-cards-for-largest-transit-smart-card-project-in-europe/, visited 25 July 2006). [2] http://www.foebud.org/rfid/en/where-find#fahrkarten (visited 06 September 2006) [3] http://www.vrsinfo.de/25598.php (visited 10 September 2006) [4] http://www.breitband-nrw.de/download/050407/20050407-Megger.pdf (visited 10 September 2006) [5] http://www.foebud.org/rfid/en/faq-english [6]http://www.brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat_63/PDF/RFID261005.pdf (visited 10 September 2006)

Case #19: Alcatel

Case ID	#126, level 3
Title	Alcatel
Researcher	Christian van 't Hof
Timing	2006
Geography	Global company, office in Rijswijk the Netherlands
Environment	Office
Technology	Active tags from Wavetrend carried by personnel and placed in lap ops and beamers. Readers are placed at doors and in ceilings and connected with DSmarttech system, based on Windows 2003 server and an SQL database. [1]
Costs	Cost of the RFID system: EUR …, Implementation costs: EUR …
Maturity	fully operational
Function	Hands-free access, evacuation management, theft prevention and time registration
Owner	Alcatel provides communications solutions to telecommunication carriers, Internet service providers and enterprises for delivery of voice, data and video applications to their customers or employees. With sales of EUR 13.1 billion and 58,000 employees in 2005, Alcatel operates in more than 130 countries. [4]This story is about the Dutch office in Rijswijk, which has 230 staff members.
Maintainer	Transquest
Users	Alcatel staff
Other actors	Workers' Council at Alcatel
ID issue	The system was applied foremost as a security system (evacuation and theft prevention) but soon evolved as a tracking and time registration device. During the implementation phase complaints and worries were expressed by a small number of employees, some claiming it to be a 'Big Brother system'. These matters were addressed by the Workers' Council and the discomfort soon faded away. Afterwards, the time registration system was even used to advantage of the staff to show how much overwork they were performing. [2]
Sources	[1] "Handsfree toegangscontrole draagt zorg voor tijdsregistratie en evacuatiemanagement" www.transquest.com [2] Interview with Jan Vet, Technical Project Manager Operations and member of the Workers' Council. {3] conversations with Alcatel personnel passing down the hall [4] www.alcatel.nl [5] Alcatel Workers' Council questionnaire on the new access system, 31 January 2005

Case #20: Mol Logistics

Case ID	#128, level 3
Title	Mol Logistics
Researcher	Christian van 't Hof
Timing	2006
Geography	Tilburg, Netherlands
Environment	Office
Technology	Active RFID
Maturity	Pilot / just implemented / fully operational
Function	Access / security / identification
Owner	Mol
Maintainer	TransQuest Tag & Tracing Solutions B.V.
Users	Mol employees, visiting drivers, temporary labour forces
Other actors	
ID issue	How do the users and maintainers of the RFID environment define what kind of personal information is known, to what purpose is it used? Is there a controversy?
Sources	Transquest: MOL Logistics Handsfree toegangscontrole draagt zorg voor tijdregistratie en veiligheid (2006)

Case #21: AlpTransit Gotthard AG

Case ID	# 129, level 2
Title	AlpTransit Gotthard AG
Researcher	Christian van 't Hof and Eefje Vromans
Timing	2006
Geography	Italy
Environment	Work
Technology	Active RFID tags
Maturity	fully operational
Function	Security
Owner	Alptransit Gotthard
Maintainer	Acter ag
Users	Workers and material in the tunnel; visitors
Other actors	Techselsta (Lugano, CH), TransQuest Tag & Tracing Solutions B.V
ID issue	The only purpose of the RFID badges is to track down people in case of an incident. It is not known if workers or visitors have ever refused to use the RFID for privacy reasons [3].
Sources	[1] http://www.alptransit.ch/pages/e/ [2] http://www.transquest.nl/nederlands/gebruikers.php [3] Alptransit (+41(0)918212121), contacted on 07september 2006 [4] http://www.acter.ch/products.php?hauptrubrik=500&product=acterrfid (visited on 07 september 2006) [5] Telephone contact with the Alp Transit Visitors Center

Case #22: Apenheul

Case ID	# 130, level 3
Title	Tracking visitors flows through the tagged Monkey Bag
Researcher	Christian van 't Hof
Timing	2006
Geography	The Netherlands
Environment	Leisure
Technology	The system consists of active RFID tags sowed into the visitors bags and 11 reader/buffers defining 10 areas through the park. The readers are stand-alone, their data is downloaded weekly. Numbers of visitors per area, time spent and speed of movement through the park are provided in Excel and Access spreadsheets. Visitors profiles and an overview of the total flow of visitors emerge after analysis.
Costs	Each RFID tag costs EUR 25 the whole system about EUR 20,000
Maturity	Just implemented
Function	Profiling flow of visitors through the park
Owner	Apenheul, a Dutch zoo specialized in monkeys and apes
Maintainer	Wavetrend
Users	Visitors of the park
Other actors	Monkeys and apes
ID issue	This RFID application touches upon the issue on what is personal data and the control costumers should have over data retrieved from their movements. The Monkey Bag RFID has a marketing function: how do visitors move through the park and how can the flow of people be optimized? The visitors remain anonymous, are not traced real-time and are in no way affected by the data they provide. In that sense, the data retrieved cannot be seen as an identity that should be managed from a user perspective. Still, visitors are being traced without informed consent. The tagged bags are provided without informing the user about the tractability. Moreover, the use of the monkey bag is obligatory. Visitors are given a bag at the entrance with a security argument "Monkeys move freely through the park and will try to steal your goods." Although legitimate in itself, this rule limits free choice of the visitors not to use the bag. A side issue on Identity Management is that the bag is sometimes used by park hosts, to carry food across the park. In order to keep the profiles clean, data on personnel movements need to be erased.
Sources	We discovered this case through the website of the provider Wavetrend. We then contacted the Apenheul and visited the park on 3 August 2006 for observations and eight short interviews with park hosts. Finally we held a telephone interview with the marketing manager Bert Smit on 22 August 2006. De Apenheul

	Park Berg en Bos J.C. Wilslaan 21-31 7313 HK Apeldoorn Phone: +31 55 3575757 E-mail office@apenheul.nl

Case #23: Exxon Mobile Speedpass

Case ID	#131, level 1
Title	ExxonMobile Speedpass
Researcher	Christian van 't Hof
Timing	1997-2006
Geography	US, Canada, Singapore, Japan
Environment	traffic and retail
Technology	The Speedpass consists of a 134kHz RFID chip (Texas Instruments) in a small black plastic barrel of about 2 cm which can be carried on a keyring. Readers are placed at the gas dispenser and at the cashier. Communication between reader and tag is secured through a challenge response protocol, which works as follows. When the readers send out its signal, a random number is given. The chip performs a mathematical operation on the number, using its own secret code and sends back the result together with its serial number. The readers send this information through satellite communication to the central database in Houston, which has lists of all authorized Speedpass owners, performs the same calculation as the tag and compares the result. If the numbers match, the purchase is made through the customer's credit card number. This proves takes about 3 seconds. [4]
Costs	Cost of the RFID system: USD 60,000 for each location. [4] Customers can order and use the tag free of charge.
Maturity	Fully operational
Function	Payment
Owner	The Speedpass system was developed by ExxonMobil.
Maintainer	ExxonMobile. The radio frequency technology is provided by Texas Instruments and integrated into the fuel dispensers by the Wayne Division of Dresser Industries.[3]
Users	Customers at the gas station
Other actors	Trials at McDonalds and Stop & Shop.
ID Issue	The Speedpass is not just used to pay, but also has a marketing purpose. This is clearly stated in the "Privacy Policy" and "Terms of use", which users are assumed to have read and agreed upon when they subscribe to the pass. For example: "Speedpass and its affiliates may disclose any of the information that we collect to affiliates and non-affiliated third parties as described below. We may disclose the information whether you are a current customer or former customer." Among parties mentioned are security services, mortgage banking, direct marketing organizations and "any bidder for all or part of the Speedpass business". In practice this will mean the identity "person paying at the pump", through travel- and consuming profile, could evolve into "potential valuable customer for a motel, mortgage or groceries" or "a potential link to a criminal network". Once a customer uses the Speedpass for the first time, this act is defined as opting in on this policy. The policy also offers an opt out, but if the information is already passed onto another organization, ExxonMobile does not have control or responsibility over it. Additionally, users can maintain their user profile on-line, for example, view their transactions and receive receipts on-line. An IDM issue arising here is one family member tracing another, for example, a suspicious spouse. Another IDM issue is when the Speedpass is not used by it's rightful owner. Tags are lost or

	stolen. Moreover, they can be copied. Researchers at the Johns Hopkins University and RSA Laboratories, for example, succeeded in reading a Speedpass, cracking the code and reproduce another tag. In order to prevent misuse "Speedpass monitors purchase patterns on Devices, and looks for unusual behavior that may signal unauthorized use." [2] So, comparable to how credit companies operate, Speedpass analyses transactions in real-time for awkward profiles. If, for example, an unusual large purchase is made, or purchases occur at awkward locations, the transactions may be blocked and checked at the rightful owner of the pass. However, while these profiling analyses run real-time, one could wonder whether these profiles are only used to prevent fraud. Still, although the Speedpass system could, in principle, facilitate all sorts of direct marketing efforts, tracking of people or frauds, accounts on it's current use indicate otherwise. On on-line discussion groups, for example, many people express their fear for 'Big Brother scenarios', but none claim to actually encountered privacy invading actions. Most of the discussion threads mainly evolve around practical matters: on how the system works, if it really saves time or at which gas stations it can be used.
Sources	[1] Speedpass Privacy Policy: https://www.speedpass.com/forms/frmDynPrin.aspx?pId=2 (28 august 2006) [2] Speedpass Terms of use: https://www.speedpass.com/forms/frmDynPrin.aspx?pId=23 (28 august 2006) [3] Speedspass Factsheet: http://www2.exxonmobil.com/corporate/files/corporate/speedpass_fact_ sheet.pdf#search=%22speedpass_fact_sheet%22 (28 august 2006) [4] Garfinkel, S. "RFID Payments at ExxonMobil" In: Garfinkel, S. & Rosenberg, B. (ed.) RFID. Applications, Security, and Privacy. [5] For example: alt.tv.pol-incorrect, misc.activism.progressive or alt.culture.ny-upstate [6] For example: misc.transport.road [7] Biba, E. (2005) "Does your Car Key pose a Security Risk?" in PC World 14 February

Case #24: Medixine

Case ID	# 133, level 1
Title	Medixine RFID Communication Board
Researcher	Jessica Cornelissen

Timing	End of 2005
Geography	Finland (Imatra)
Setting	Healthcare
Environment	Homecare
Technology	RFID communication board: the board can be fitted with up to 6 NFC-RFID tags. NFC enabled mobile phones: mobile phone equipped with RFID reader Medication Management Server Application
Maturity	Pilot
Function	Informative for users (medication compliance)
Owner	Medixine [62]
Maintainer	Medixine
Users	- Patients enrolled in the trial - Medical staff enrolled in the trial - Caretakers and family of patients enrolled in the trial
Other actors	- Nokia > provider of cell phones [63] - Alzheimer Society of Finland > financial support [64] - Pfizer > production of Alzheimer drugs [65] - Elisa > provider of wireless network [66]
ID issue	In this case, strict supervision by a medical team is necessary because patients are not capable of taking care of themselves. The technology brings this supervision into people's own houses. On the other hand, without the system the patients might not even be living in their own houses anymore.

Sources	62.http://www.medixine.com (visited 5 September 2006) 63.http://www.nokia.com (visited 5 September 2006) 64.http://www.alzheimer.fi (visited 5 September 2006) 65.http://www.pfizer.com (visited 5 September 2006) 66.http://www.elisa.com (visited 5 September 2006) 67. Collins, J., 'Medixine Tests System for Alzheimer's.' In: RFID Journal, 27 September 2005 (http://www.rfidjournal.com/article/articleview/1892/1/1/, visited 5 September 2006) 68. 'RFID Technology for Blood tracking: a new application finds Ospedale Maggiore.' In: RFID Gazette, 20 June 2006 69. 'Saarbruecken Clinic adds stocks of stored blood to its RFID pilot project.' Siemens Business Services Press Release, Munich, 20 February 2006 70. 'Zorgsector start proef met RFID.' (http://www.rfidnederland.nl/Default2.aspx?tabid=264, visited 13 September 2006)