Privacy implications of RFID: an assessment of threats and opportunites

Marc van Lieshout and Linda Kool

TNO Information and Communication Technologies,
Brassersplein 2, PO Box 5050, 2600 GB
Delft, the Netherlands
{marc.vanlieshout, linda.kool}@tno.nl

Abstract. European citizens consider Radio Frequency Identification (RFID) to be the most intrusive technology of the past two decades. Safeguarding privacy requires specific action that needs attention of all parties involved. European citizens consider legal instruments to offer insufficient guarantees for safeguarding privacy. 'Privacy by design' offers interesting opportunities to build in privacy guarantees in the technology, not as an end-of-pipe solution but as an integral design parameter. Notwithstanding the commercial focus on RFID in logistic processes and – eventually – in the retail sector, the first grand scale uses of RFID will be in public domain applications. These application domains are perfect 'niches' to stimulate a 'privacy by design' approach, both to academic researchers and application engineers.

1. Introduction

The Big Brother Award in the Netherlands has this year (2007) been awarded to the Dutch railway organisation (NS). The award was given to the NS for its intentions regarding the introduction of the RFID-based public transport card in the Netherlands. These intentions were suspect, not transparent and at the cost of the privacy of passengers travelling with the card. Since the card will be the single transport ticket throughout the entire Dutch public transport system, use of the data for a variety of purposes which are not known to the data subjects (the passengers) may impact on the privacy of the passengers. At the same event the Dutch public was awarded with a Big Brother Award as well, for being totally absent in the debate on privacy these days. While the magazine Time had identified 'You' as the person of the year in 2006, the Dutch organisation Bits of Freedom in co-operation with the Amsterdam cultural centre De Balie identified 'You' as the person who is co-responsible for privacy violations. While Time's You was heralded because of his or her contributions to today's ICT revolution in which innovation is democratised and in which all kind of new services are developed by users themselves, Bits of Freedom considered the contribution of these same users to defending their own privacy as overtly insufficient and factually absent.[1]

Please use the following format when citing this chapter.

van Lieshout, M. and Kool, L., 2008, in IFIP International Federation for Information Processing, Volume 262; The Future of Identity in the Information Society; Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, Leonardo Martucci; (Boston: Springer), pp. 129–141.

The Dutch railway organisation is one of the many organisations that are implementing Radio Frequency Identification as means to re-organise their services. RFID is an enabling technology that may be used in many different situations for many different purposes. RFID is one of the cornerstones of the so-called Internet of Things [2] It is a technology that enables objects to identify themselves wirelessly by means of radio frequency. The objects are usually tagged with an RFID chip, encased with a small antenna, and – depending on the kind of application – sometimes with a battery as power source. Together with developments as the new Internet Protocol (IPv6) RFID enables a total coverage of the physical world and a complete linking of all conceivable objects to each other by means of unique labels. Having access to the labels enables parties to construct links between seemingly separated objects and events and link these to persons as well. With the advent of a unified coding scheme such as the Electronic Product Code (the successor of the bar code) each object will be uniquely determined and – if linked to another object – unique profiles may be created that may be composed of many millions of data events of all kind of objects.

This Panopticon in a modern form (totally decentralised in contrast to Jeremy Bentham's original idea of a totally centralised panopticon) will have severe privacy implications.[3] But to get a proper understanding of the issues at stake it is necessary to start at a more modest level, by looking at the privacy implications that can be straightforwardly perceived in today's RFID applications. There is no need to wait until RFID has reached the state of the item-level tag, in which each separate item is tagged. Today, most of us carry an RFID-based object, such as a public transport card, an electronic identity card, an electronic health insurance card, or simply an access badge for the buildings we work in. The pets we have can be implanted with an RFID-chip, in order to identify them in case of loss. In short, RFID is already with us and is here to stay, whether we like it or not. In order to guide its introduction such that one of the success factors is appropriately taken care of, namely privacy, we will pay due attention to the privacy impact of RFID.

2. The concept of privacy

The modern approach of privacy, and the use of it today has much to owe to the seminal contribution of Samuel Warren and Louis Brandeis in 1890 in which they argued for the need to have a separate law for what they called 'the right to be let alone'. Their plea for a right to privacy has not lost much of its power today. They refer to modern equipment that allows the intrusion of privacy: 'Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone'. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' [4] But Warren and Brandeis are remarkably modern in identifying the backgrounds of the need for privacy as well: 'The intensity and complexity of life, attendant upon advancing civilization, have

rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.' [4] Warren and Brandeis mention solitude separate from privacy. We propose to perceive solitude as one of the 'spheres of privacy', starting from the most outward sphere anonymity working inwards to reserve, intimacy and, finally, solitude. In public we may have a need for anonymity, we sometimes want to be able to withdraw from the public (reserve), we have an intimate circle in which we share our thoughts with those who are most intimate to us and finally we may have a need for contemplation just by ourselves in order to free our minds from the pressures of everyday life. The four spheres refer to the cornerstone of privacy, the right to be let alone. This right, which essentially is a social right based on social norms, values and conventions, is usually safeguarded by means of some kind of juridical regime. This, unfortunately, has led to a rather juridical notion of the panopticon. We will return to this issue.

Next to the four spheres – which as onion shells run from very intimate to very anonymous – we define two dimensions on privacy. We can distinguish between informational or relational privacy, spatial privacy and bodily privacy as the three main dimensions. Informational or relational privacy relates to information transferring something about ourselves or our relations to other persons, organisations or objects and thus revealing information about our personal relations to these persons, organisations or objects. Spatial privacy relates to the physical boundaries which we safeguard, such as our house, but also the spatial distance we keep to other people. Bodily privacy relates to the integrity of our body, which no one is allowed to touch or to invade except when granted access. These dimensions of privacy are laid down in the Universal Declaration of Human Rights and in other laws and have led to specific juridical regimes, such as the European Privacy directive (95/46/EC). We will return to the question how adequate these regimes are for safeguarding our privacy in relation to the dissemination of RFID. Before doing so, we will first present the technology at stake, RFID.

3. RFID – the technology

The basic elements of RFID have been known for many years and go back to the Friend or Foe devices that were in place during the Second World War. Airplanes had an identification signal which enabled the ground stations and other airplanes to identify whether the airplanes belonged to the 'friends' or to the enemy. The concept of Radio Frequency Identification has been adopted to enable a chip to communicate wirelessly with a device, and to identify itself by transmitting a unique number to the identifying device. An antenna is used to create the energy that can trigger the chip to read out its number and to send it via the antenna back to the reader. These passive RFID-chips are delivered in all kind of frequency classes, where each frequency class has its own distinct characteristics. Overall, one could say that the higher the

frequency used, the higher the energy and thus the higher the distance that the signal with the number can travel and the higher the complexity of data that can be transmitted. The lay-out of the antenna (a small one or a larger sophisticated one) plays a role as well. Simple passive tags only have a number to be read out which identifies the tag itself. Usually this number is 'printed' in the chip during fabrication. More sophisticated chips have processing capacities which enable the storage of more information and processing the information before it will be released. Usually, these more sophisticated chips have an external energy source (a battery) to power them for their processing capacities. When a sensor is attached to the RFID-chip, sensor information can be stored next to the identifying number. Processing capacity can also be used for encryption facilities. In case the battery is only used for internal processing capacities, the tag is called a 'semi-active' tag. When the energy source is used to increase the read range, the tag is called an 'active tag'. Read ranges from passive tags range from a few millimetres (proximity tags, such as those in electronic identity cards) to a few metres. Active tags can have a read range of up to hundred metres.

RFID tags come in different sorts and casings. Sometimes they are encased in plastic (such as access cards for buildings), sometimes they are embedded in paper labels, and today antennas become printed (printed electronics) in order to reduce costs of the tags. Chipless tags (which work on different physical principles which we will not spell out in this paper) are part of research into different modalities that may be cheaply produced in massive quantities.

The privacy implications of RFID tags will differ, depending on the kind of tag that is used and the circumstances in which it is used. We will now turn to discuss the privacy impact of RFID.

4. Privacy impact of RFID

The relation between RFID and privacy has been acknowledged by several organisations and institutes. The OECD states that : '[W]ithout addressing privacy related issues carefully, appropriately and transparently ... backlash by consumers and citizens is a potential risk that could limit long-term benefits and development.' [5: p. 15]. The European Article 29 Working Party on Data Protection emphasises several problems with the introduction of RFID and stresses the importance of indicating what kind of data should be processed under what conditions. Especially the notion of 'personal data', a pivotal concept in data protection legislation, is difficult to define unambiguously with respect to RFID, according to the Working Party. When a wristwatch carries an RFID tag, this by itself does not turn the RFID number into personal data. The number identifies the wristwatch, not the person who wears the wristwatch. But when the number is used to identify the person because one assumes the same person to carry the same wristwatch in different situations, the RFID number turns into personal data, i.e. in data that can be traced down to a specific person. This feature of RFID is very problematic in the context of privacy

laws. It will not be a surprise that the position of the Article 29 Working Party that *any* RFID number may turn into personal data has met fierce resistance.[6,7]

Given the fact that RFID relates to data, we could assume the privacy impact of RFID being mainly within the realm of informational or relational privacy. And indeed, the gathering of information about someone's travel behaviour on the basis of my use of the public transport card with an RFID chip can be seen as impacting on his informational privacy (information about him) and on his relational privacy (it may be used to relate him to other travellers who exhibit the same travelling pattern as he does). The fact that these travel patterns may reveal *where* he has been may impact on his spatial privacy, as can be illustrated by the case of using access control badges. Access control badges can be seen as devices that limit the spatial privacy of a person since they enable tracking him down in buildings. RFID-based access control badges have an impact on spatial privacy since they enable people to survey *where* other people are. The bodily dimension of privacy is at stake when RFIDs themselves are inserted in the body. A well-known example of this situation is the use of embedded RFIDs in the Baja Beach clubs in Barcelona and Rotterdam. Since these chips are inserted on a voluntary basis this specific use of RFID is not a real intrusion of bodily privacy. Many other examples can be given, especially the attempts of VeriChip, the first organisation in the USA that is licensed by the Food and Drug Administration to implant RFID chips in humans. VeriChip has offered several opportunities to use implanted RFID chips, for instance to tag illegal Mexican workers that trespass the USA borders and are trapped, or American soldiers who in specific events can not be identified anymore and who have lost their identification badge.[8] Again, when these chips are implanted on a voluntary basis, one can not proclaim that bodily privacy has been intruded. But the VeriChip examples show it is a thin line to walk.

A recently performed survey by the Dutch Rathenau Institute in cooperation with the Dutch Consumers Organisation and the Dutch ICT interest organisation ECP.NL details the opinion of people towards RFID.[10] 2000 respondents filled in the internet-based questionnaire. The results of the internet based survey are presented in Table 1.

Table 1: Attitude of Dutch population with regard to introduction of RFID [10]

Statement	Possession [%]	Agree/ (very) positive [%]	Not agree/ (very) negative [%]
RFID based access card at work	21		
Opportunity to show work attitude		40	20
Employer should not register everything that is possible		55	
Public transport card	7		
Personalised card (possession)	80		
Use of data by intelligence services		72	16
Use of data to track witnesses		61	25
Limit possibility to travel anonymous		58	32
Transborder use by intelligent services of collected travel data		52	26

Biometric identity card	23		
Biometric card will be illegally copied		71	
Centralised registration of finger print data		66	20
Centralised registration of facial recognition data		56	26
Use of facial scan to track people of video images		62	14
Shopping and commercial products			
Prices will rise due to introduction of RFID		62	
Use of RFID at Point of Sale (direct payment)		70	
Need for transparency and killer option		85	
Need for opt-in system		62	
Trust in appropriate use of RFID-data			
By medical services		62	8
By police, justice and intelligence services		51	18
By commercial entities		10	50

Overall, the Dutch population exhibited the feeling that the introduction of RFID and RFID-based applications can not be stopped. 47% expressed concerns with the kind of data that will be collected and used by RFID-systems, 25% did not express concerns in this respect. When asked for advantages and disadvantages of RFID, the following top 5s were mentioned:

Table 2: Advantages and disadvantages of the introduction of RFID [10]

Advantages	Disadvantages
1. Fighting criminality	1. Difficult to correct mistakes
2. Ease of use	2. Function creep
3. Determining identity	3. Misuse of data
4. Need for fewer cards	4. Criminals will circumvent the system
5. Prevention of theft	5. Use of data for direct marketing purposes

The results of the survey show that people welcome the opportunities RFID offers for surveillance purposes and do not oppose centralised systems that can be used to track down criminals or to search for people. Interestingly, they are less positive when the system will be used to track down witnesses (who of course can be everybody) in case of specific situations (a case of molestation in a train for instance). The Dutch survey shows that there may be two domains of discussion: a public domain, dealing with the applications and the opportunities of use and misuse, and a technological domain that deals with the underlying technological threats and opportunities (linking

of systems, opportunities for eavesdropping, security measures, developing opt-in systems and the like).

4.1 Towards a more detailed analysis of the privacy impact of RFID[1]

In the assessment on RFID which we have performed for the Institute of Prospective Technology Studies (IPTS, Seville, one of the Joint Research Centres of the European Commission) we have identified a set of threats to privacy. We based our assessment on previous research of Sarah Spiekermann of the Humboldt University in Berlin.[11] In Table 3 we indicate the threats that can be related to RFID, based upon a distinction between the threats that can be linked to the RFID reader-tag system and the threats that can be linked to the back-end systems (the data processing equipment).

Table 3: Direct and indirect privacy threats, related to RFID

Privacy threats	Reader-tag system	Back-end
Individual	Unauthorised reading of personal information Real-time tracking of individuals	Combining personal information Using data for purposes other than originally specified
Collective/Group	-	Profiling and monitoring

Unauthorised reading of tags: Simple RFID tags do not contain much more than a number. The number can be read out by readers that have access to the tag. Without specific security mechanisms (such as encrypting the data stored on the tag, or using a handshake protocol to recognise readers that are enabled to have access to a tag), all readers in the appropriate frequency range are able to read data from the tag. Reading ranges are dependent on frequency used: the higher the frequency the higher the read distance. Active tags (with batteries for energy supply) tend to have longer read out distances than passive tags (which are dependent on the energy of the transmitted waves for data processing and communication). Juels *et al.* have demonstrated that ranges for eavesdropping outpace the nominal read range which is specified in standards. UHF-tags, with frequencies in Mega- or Gigaherz domain, have nominal read ranges of 7-10 meters, but Juels *et al.* have demonstrated that they can be read out at a distance of several tens of metres [12]. Proximity cards work at close distance (a few millimetres) but can be accessed from greater distances as well. Especially in case of sensitive data (for instance the identification of specific nationalities in a row of tourists) unauthorised reading of tags can have severe consequences. Security measures, such as encrypting the data stored in the tag or authentication handshake protocols, may prevent unauthorised reading of tags. Not all tags will be interesting to read, since they will not reveal much (if any) personal information of the holder. Still, the principal position holds that one should be able to determine by oneself what

[1] The following sections are based on a previous paper 'Little sisters are watching you' which we have submitted as pre-conference paper to the IFIP Summerschool 'The Future of Identity in the Information Society' that was held 6-13 August 2007 in Karlstad, Sweden.

information under what circumstances will be communicated to other people and organisations. Unauthorised reading of tags is an infringement of this position.

Real-time tracking of individuals: On the basis of a single tag one can trace people. All that is needed is a unique tag that is linked to that person. An RFID tag attached to a wristwatch could be used. This wristwatch identification could be used to track a specific individual. Purposeful monitoring of people is used in hospitals, in schools and in prisons. In hospitals one experiments with RFID tags to identify new born babies, to locate people with Alzheimer diseases but also to locate doctors and nurses. In the USA a board of school has suggested to tag children so that the school could meet its juridical obligation to know whether a child left school yes or no. While this was seriously opposed by the parents these kind of practices are much less disputed in Japanese schools.[13] RFID based systems are used as an alternative to electronic handcuffs. Several of these applications are contested since they impinge on personal freedom and on the right to be let alone. In situation of electronic imprisonment, a small and relatively invisible RFID-tag may however be more humane than a much more visible scaffold. In principle, the purposeful real-time tracking of people against their will poses privacy problems. In case of new born babies (to prevent kidnapping of babies and accidental exchange of babies) the privacy infringements are less clear. Tracking people with serious forms of Alzheimer disease is more difficult to judge as well. RFID can be of use to offer these people more freedom, and to save costs in searching for them. In case of the school children the parents protested against this use of RFID; the company responsible for the trial backed off eventually [13]. The absence of communication with the parents about the benefits and pitfalls of use of RFID showed to be a showstopper. Use of RFID to track people in real time will have to be weighted against the infringement on privacy but it would be wrong to deny beneficial uses of RFID in all situations.

Combining personal information: At the back-end of RFID systems privacy infringements are comparable to 'ordinary' data collection systems that aggregate information about people from different sources. RFID is no exception to this situation, but the amount of data to be aggregated will explode. Having billions of RFID tags means that the back-end system will have the opportunity to aggregate data that belong to one and the same person by combining specific data. Once item-level tagging has become commonplace, the accompanying model to label all products in one encompassing mode will release an enormous amount of correlations between previously separated sets of data. The prime example here is the supermarket that identifies its customers by one specific item, an RFID tagged wristwatch for instance. Each time the customer enters the supermarket, all items that will be purchased will be linked. This information can be more detailed than the data that are now collected by loyalty cards, since also the route through the shop and the items that have been picked up but have not been taken can be monitored. There are numerous other places where this information can be aggregated such as libraries, on the road, in public transport, or in hospitals. The Article 29 Working Party has expressed its concern for these practices since it presupposes an increasing number of controllers that should audit all these situations.[6]

Using data for purpose other than originally specified: Function creep, the extension of the functionality of systems, lurks around the corner. Datamining technologies enable tracing specific patterns within large data heaps and revealing social networks on the basis of these patterns. Since the introduction of the Oyster card in London public transport, the Metropolitan Police has multiplied its request for specific travel data. In January 2006, it had requested travel information of Oyster card users 61 times, compared to only seven times over the whole of 2004 (before introduction of Oyster card). In March 2006 the frequency had risen to 243 times. By comparing travel patterns with travel patterns of suspect people, the Metropolitan police tried to identify social networks of suspect people [14, p.251]. The data that were collected for public transport purposes were not collected with the aim of surveying behaviour of people. Though in this situation data retention acts and lawful decisions support the attempt of the Metropolitan Police, one can also argue that with a different design of the data system function creep could be prevented.

Profiling and monitoring of people and behaviour: By analysing the various sources of data one can construct profiles of people. The more detailed and fine-grained the analysis is, the more difficult it will become to prove the incorrectness or impreciseness of the profile. Though this is not a new threat RFID may intensify the construction and use of profiles.

5 Strategies to cope with RFID privacy issues

Using RFID poses threats to privacy, especially but not exclusively related to the informational or relational dimension of privacy. Protecting the informational dimension of privacy is the purpose of the European privacy directive. Given the special classes of privacy threats of RFID we have to investigate the adequacy of the existing legal framework to safeguard our informational privacy. Commercial entities usually adhere more to schemes of self-regulation than to legal instruments. Self-organisation enables a more flexible approach that hinges on the recognition of specific threats and the need to build up a trust relation between commercial entities and their customers. Self-regulation is in the interest of all parties and thrives on well-understood self-interest of the commercial entities, seriously taking into account the needs and attitudes of their customers. Finally, but surely not in the last place, technology itself may be applied to safeguard privacy. When information or data sharing architectures are designed such that it is technically impossible to exchange personal data, privacy is best safeguarded. Immobilising an RFID tag when it is outside a predefined area may be such a technical solution.

These three approaches, the legal one, self-regulation and technology itself as counterforce, are discussed in more detail in the following sections.

Legal instruments: Whenever personal data are collected by RFID based systems they have to comply with the privacy regulations and laws at hand. In case of the European Union this implies compliance with Directive 95/46/EU and its adjacent national privacy laws. Dispute is arising around the appropriateness of the legal framework. The legal framework itself is based upon the OECD Guidelines on the

Protection of Privacy and Transborder Flows of Personal Data, which was published in 1980.[15] The OECD Guidelines comprise eight principles for fair information practices, of which the most important ones are: do not collect more than strictly necessary and only for well-described purposes; be sure that the data collection is transparent and that data subjects have appropriate instruments to check the validity of what has been collected. With respect to RFID two issues come to the fore: the first one relates to the notion of 'personal data'. When an RFID tag contains nothing more than a number, for instance the number that identifies a wrist watch, the borderline between whether this is information that can be attributed to a person or not, is very thin. In the future, when item-level tagging will have become commonplace, items will be classified according to a specific categorization such as the Electronic Product Code, which is yet under development. By means of the Electronic Product Code (EPC) classification (to stick to this example) each item tagged with an EPC tag will get an identifier, which uniquely identifies the category to which this item belongs (watches), the producer of the item and the unique serial number of the item. This unique tag number could be associated with a specific person (for instance, the tag of his/her wristwatch or of his/her glasses). In this way, the RFID tag becomes a tag which can be used to identify a person and is thus susceptible to the Data Protection Act. According to the Article 29 Working Party, *all* RFID tags have data which may sooner or later turn into personal data. All RFID tags thus should be treated as susceptible to the European privacy directive [6]. This position has met severe resistance of market parties which consider this position to be detrimental for the market potential of RFID [7]. A second problem is the informed consent which is required when collecting personal data. Consent should be freely given, should be specific, should entail an indication of the individuals effective will, should be informed and should be unambiguous. Information about the possible collection of personal data will have to be communicated, in all places where this is appropriate. Given the highly unspecific manner of data collection this may be problematic as well, especially given other elements of the privacy directive which requires transparency in data processing, openness to the data subject (right of access, right of refusal), the quality of data collected, etc. The Working Party warns of the danger that all these measures 'will cause a boost in data to be processed by a wide variety of controllers, giving cause to concern' [6: p. 6].

Self-regulation: Market parties point at the opportunity to regulate uses of RFID data by means of self-regulation which prescribes use of RFID data, of informing customers, of raising awareness for RFID tags and of offering choice to consumers. Various guidelines are available, mostly if not all US-based. EPC Global has released guidelines in which they point at the need of notice (marking objects which are tagged), choice (offering consumers the possibility to de-activate or remove the tag), security, record use and retention (relates to the assurance not to process personal data) and educating the public [16]. The American Centre for Democracy and Technology (CDT) has developed guidelines in cooperation with American technology suppliers and RFID users (Microsoft, Procter and Gamble, VISA USA) and the Consumer League [17]. Their approach is comparable to EPC's set of guidelines. CDT has identified five guidelines: give notice, choice and consent,

onward transfer (in case of third party transfer of data the third party must comply with at least a similar privacy regime or even better), access, and security. Though sympathetic in its approach, there is widespread agreement that self-regulation is not sufficient to safeguard privacy (see next section).

Privacy by design: The European Commission held an RFID Consultation process in 2006 in which it has consulted European citizens and companies about, amongst others, the privacy consequences of RFID [18]. Almost 2,200 participants delivered input to the consultation process. 65% of them were interested citizens, 15% were related to the RFID industry, and remaining respondents came from university and governments. Privacy was among the top level concerns (together with health and environmental risks). The questionnaire entailed a number of questions in which respondents were explicitly asked to rank measures to protect privacy. The respondents considered the development of technological solutions to allow or disable tags the best safeguard for privacy (67%). Legislation to regulate uses (50%) was ranked second, while self-regulation (15%) scored far less (more than one answer was possible).

Technological solutions relate to de-activating tags and removing them. Solutions are removal of antennas, creating Faraday cage to prevent transmission of data, removal of the tag from the object, and putting tags into 'deep sleep mode'. These are so-called 'end-of-pipe' solutions, they are add-ons instead of fully integrated at the early stages of development. The technological approach to safeguard privacy can however also be embedded in the design of the RFID system itself. The Article 29 Working Party 'considers that technology may play a key role in ensuring compliance with the data protection principles ...' and continuous referring to using specific design to enforce minimisation of collection and use of data [6: p. 12]. The OECD refers to this as the privacy by design approach. It considers this 'to be more effective in the long run', referring to legislation and self-regulation as other measures [5: p. 19]. Floerkemeyer et al [19] have demonstrated that the OECD privacy guidelines which are basic to the European privacy laws can be used as design criteria for EPC data collection systems. The design criteria relate to how specific Fair Information Principles (FIP) can be realised, such as collection limitation by an appropriate tag selection, use limitation by creating specific collection types, and purpose specification by identifying a specific set of possible purposes. Part of Floerkemeyer's approach is the empowerment of consumers by means of a so-called 'watchdog tag', a tag plus screen that identifies readers nearby and provides information about the reader. This idea of a watch dog has been developed by other parties as well.[20]

This EPC-based approach can be broadened to other domains as well. Within public transport, use of encryption technologies to decipher data that are stored on the public transport chip, may enforce compliance with the FIP. Technically, this is possible. Not all technical features to encrypt the data or to minimise data storage are however used. Given interests of companies to use the data for a broad range of purposes, there is a clear need for enforcement of using privacy enhancing technologies in all design stages of the RFID system. The example of the embeddedness of privacy principles in the RFID technologies itself, transferring

privacy protection from end-of-the-pipe approaches to integrated privacy enhancing technologies, poses interesting challenges to the academic community, public and private privacy commissioners and designers.

6. Conclusions

Awareness of RFID applications is growing and is reaching a level where the focus changes from mere informing the general public on what is going on towards addressing specific issues and debating the privacy consequences of these issues. RFID is considered to be a highly intrusive technology that will have severe impacts on our privacy. On the other hand, results from a Dutch survey show that in the trade-off between protecting one's own privacy and safeguarding society against criminal acts or terrorist threats the balance tips in the direction of sacrificing personal freedom. The underlying maxim seems to be that as long as people have nothing to hide they have nothing to fear as well. RFID is impacting on all dimensions of personal privacy, i.e. on the informational/relational dimension, the spatial dimension and the bodily dimension. This re-enforces the status of RFID as a highly intrusive technology. By gathering and disseminating information about objects and relating them to each other, unique profiles can be constructed that are difficult to deny. RFID enable locating people's physical location and thus impact on their spatial privacy. Finally, RFID implants are promoted heavily by specific parties who have beneficial business cases for specific implant applications.

The means to counter the privacy threats can be classified in legal instruments, self-regulation and technological means. The legal approach is still considered to be very worthwhile, though some very persistent problems are defined with respect to RFID. First, all RFID data may become personal data in the end, by means of some kind of linking of objects to persons. Second, because of the widespread dissemination of RFID it will become increasingly difficult to get informed consent about applications (of which it is difficult to predict whether and under what circumstances they will enter into the personal realm). The technological approach is considered to be very promising, as is indicated by specialist parties such as the Article 29 Working Party and which is supported by the results of the European consultation process on RFID. This is a very interesting outcome that lends support to the activities around Privacy Enhanced Technologies. The main challenge is to involve privacy considerations in the design process from the start on, in order to prevent end-of-pipe solutions but to include privacy as design criterion in any RFID-based information system.

References

1. See http://www.bigbrotherawards.nl/
2. ITU 2005. The Internet of things.Geneva: ITU.

3. Whitaker, R. 1999 The End of Privacy – how total surveillance is becoming a reality. New York: The New Press.
4. Warren, S.& Brandeis, 1890.The Right to Privacy.Harvard Law Review,15 December 1890.
5. OECD. 2006a. Radio-frequency identification (RFID): Drivers, challenges and public policy considerations. Report DSTI/ICCP(2005)19/FINAL, published on 27 February 2006.
6. Article 29 Working Party on Data Protection. 2005a. Working document on data protection issues related to RFID technology. 10107/05/EN, 19 January 2005.
7. Article 29 Working Party on Data Protection. 2005b. Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology, 1670/05/EN, 28 September 2005.
8. For illegal immigrants see http://scaredmonkeys.com/2006/06/01/i-am-sure-the-aclu-will-approve-of-this-proposal-to-implant-tracking-chips-in-immigrants/#more-2655; for using RFID in soldiers, see http://www.techweb.com/wire/ebiz/192203522
9. Capgemini. 2005. RFID and Consumers – What European consumers think about radio frequency identifications and the implications for businesses. Capgemini report
10. Heuvel, E.van den, Nagel, K.Hof, C.van 't, Schermer, B 2007.RFID-bewustzijn van consumenten: hoe denken Nederlanders over Radio Frequency Identification?. ('RFID awareness of consumers: how do Dutch people think about RFID?') http://www.rathenau.nl/showpageBreed.asp?steID=1&ID=2963
11. Spiekermann, S., Ziekow, H. 2006. 'A systematic analysis of privacy threats and a 7-point plan to address them'. Journal of Information System Security, vol. 1, no. 3.
12. Juels, A., Rivest, R. and Szydlo, M. 2003. The blocker tag: selective blocking of RFID tags for consumer privacy. CCS'03, October 2003, Washington.
13. See http://ubiks.net/local/blog/jmt/archives3/004343.html for a description of the Japanese pilot, see http://www.rfid-weblog.com/50226711/tagging_of_school_ students_halted.php for a description of the objections in a USA pilot and http://www.epic.org/privacy/rfid/children.html for an overview of pilots and objections.
14. Lieshout, M. van, Grossi, L., Spinelli, G., Helmus, S., Kool, L., Pennings, L., Stap, R., Veugen, T., Waaij, B. van der, Borean, C. 2006. RFID Technologies: Emerging Issues, Challenges and Policy Options. Sevilla: IPTS, EN22770. http://www.jrc.es/publications/pub.cfm?id=1476
15. OECD Guidelines for the protection of privacy and transborder flows of personal data. See http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00. html
16. EPC global, 2005. Guidelines on EPC for Consumer Products. Revised Sep. 2005 www.epcglobalinc.org/public_policy/public_policy_guidelines .html
17. Centre for Democracy and Technology. 2006. Privacy Best Practices for Deployment of RFID Technology – Interim draft, May 2006.
18. European Commission .2006c. The RFID Revolution: Your voice on the Challenges, Opportunities and Threats, Online Public Consultation. 16 Oct. 2006.
19. Floerkemeier, C., Schneider, R., Langheinrich, M. 2005. ,Scanning with a purpose – Supporting the Fair Information Principles in RFID Protocols'. Lecture Notes in Computer Science, Vol. 3598, pp. 214- 231.
20. Rieback, M.R.,Crispo, B. Tanenbaum, A.S. 2005. 'RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management'. Lecture Notes in Computer Science, vol. 3574. pp. 184-194.