Little sisters are watching you

A privacy assessment of RFID

Marc van Lieshout, Linda Kool
TNO Information and Communication Technologies;
Brassersplein 2; PO Box 5050; 2600 GB Delft; the Netherlands;
E-mail: marc.vanlieshout@tno.nl; linda.kool@tno.nl;
homepage: www.tno.nl

Abstract.

European citizens consider RFID to be the most intrusive technologies of the past decade. 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

RFID is one of the building blocks of what is known as the 'Internet of things' [1]. Radio Frequency IDentification is a technology that enables objects to identify themselves wirelessly to readers. The objects are equipped with an RFID tag, usually a small chip with an antenna and casing. RFID tags come in various modalities with various characteristics, such as being either passive or active, the frequency range for which tags are used, and whether tags have extra processing capacity beyond sending the identification code. The complexity of RFID and the corresponding information systems vary considerably over the application domains, with corresponding differences in the privacy threats applications of RFID may pose.

Though surveys indicate that RFID is not yet known to the public at large [2], the market forecasts about the dissemination of RFID are rather prosperous and indicate growth rates of 50% yearly (Gartner) and market revenues of 3.8 billion Euros in 2007 rising to 21,3 billion Euro in 2017 [3]. Most of RFID growth will be in logistics

on the basis of simple tags but smart cards and smart tickets will follow and will be available in very high numbers, trespassing a billion tags in 2011 with an estimated market value of some 900 million Euro [4]. That this is hardly an exaggeration can be demonstrated by the biggest contract that has yet been made and which is in the hands of the Chinese government. They have ordered over a billion identity cards based on RFID at a contract value of over 4,5 billion Euro [5].

RFID is an enabling technology. It helps to improve the efficiency of a wide range of activities, and it provides for added value for e.g. retailers, hospitals, farmers, and public transport. Item-level tagging – which has given rise to consumer concerns in recent years – will be something of the future but will not be available on a broad scale in all markets for the first five years. Smart cards, RFID-based identity cards, use of RFID in large scale environments such as hospitals, libraries and public transport are yet rolled out in several trials, pilots and real applications (see [5] for an overview).

RFID heralds a new stage in the discussion on technology and privacy. It poses threats to privacy but offers opportunities to contribute to safeguarding privacy as well. A retrospective glance over the past few decades shows that there is no reason to be too optimistic about the 'balance of power' between technological developments and their impact on privacy. Still, a number of signs indicate that RFID offers opportunities to improve the balance. In this paper we will shortly introduce our approach of the concept privacy. Having done so we will present the findings of a broad assessment we have performed on RFID in the past year with a focus on privacy. This will be discussed in the final section, with a specific view on the approach of 'privacy by design'.

2. Privacy assessment of RFID

In a recent OECD report, privacy is indicated as an important aspect of RFID-developments. 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." [6: p. 15]. The OECD memorizes a study done by the EU Article 29 Working Party on Data Protection, a group that has been installed in accordance with article 29 of the European privacy directive 95/46/EC. This study supports the findings of the OECD with regard to the privacy implications of RFID [7]. The OECD and the Article 29 Working Party share the view that in case of RFID privacy and security are two sides of the same coin and require an approach in which they are both tackled together. We will come back to this notion at the ned of this paper. For now, we focus on the concept privacy. In this paper we will use privacy as a concept that can be approached from two perspectives: relational privacy and informational privacy. The first perspective refers to the 'claim to be let alone', the second one to 'the claim of people to determine for themselves when, how and to what extent information about them is communicated to others' [8]. The greatest share of discussions related to privacy deal with the second dimension, i.e. privacy is equated with data protection. RFID is however not only a device that communicates data about objects but that

may function in localising the physical presence of objects as well. Due to the omnipresence of RFID and the connection of RFID to objects which can be related to people and sometimes are directly connected to people, RFID will broaden the discussion to include relational privacy as well. The European Data Protection Acts – based upon the European privacy directive – express the juridical dimension of privacy. This juridical dimension imposes a universal structure, dealing with rules and regulations of data collection and data use, accountability, security, quality of data, and rights of data subjects. They do not deal with socio-cultural interests, with the more encompassing dimensions of privacy such as intimacy and autonomy, concepts that we are used to refer to in ordinary daily societal practices as basic elements of our personal environment (an exception being the German law which defines 'Informationelle Selbstbestimmung' – 'informational autonomy' – as a guiding principle for determining the rights of people in protecting their private spheres. RFID may impinge on this socio-cultural dimension. RFID enables a direct monitoring of the location of someone in combination with monitoring of specific activities. RFID is part of a far more encompassing infrastructure that combines relational and informational infringements of privacy.

This is recognized in a survey of CapGemini [2]. Consumers consider the impact of RFID on privacy to be greater than the impact of several previous intrusive technologies, such as mobile phones, access control badges and camera phones (see table 1). The results indicate as well that the overall perception of RFID is blurred; in reality it is difficult to draw a strict boundary between access cards, smart cards and RFID technologies.

Consumers saying RFID has …	Greater impact	Same impact	Lesser impact	Don't know
Mobile phones	36	33	10	21
Debit cards	36	29	7	26
Credit cards	41	31	8	20
ATMs	41	32	8	19
Loyalty cards	42	33	7	18
Access control badges	45	31	6	18
Smart cards	46	28	6	20
Camera phones	34	32	10	24

Table 1: Impact compared between RFID and other technologies – Europe (Capgemini, 2005: 11]

In a study, performed at the Humboldt University of Berlin, people scored the potential major privacy risks of RFID [9]. They considered 'unauthorized access' to RFID data to be the most important privacy disruption, followed by 'tracking of objects' and 'retrieving social networks'. Number four and five were 'technology paternalism' (RFID enforcing specific behaviour) and 'making people responsible for objects' (tags enable tracing back objects to people). We used this typology of threats to construct our own typology. In table 2 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).

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

Table 2: Direct and indirect privacy threats, related to RFID

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 recognize 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 bigger 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 [10]. 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 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 one single tag one can trace people. All one needs 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 kid left school yes or no, and 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. RFID can be of use to offer these people more freedom, and to safe 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 [11]. The absence of communication with the parents about the benefits and pitfalls of use of RFID showed to be a showstopper.

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. Of course, 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.

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 [5]. 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 purport 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.

3. Strategies to cope with RFID privacy issues

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. 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 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 personal turn into personal data [7]. All RFID tags thus should be treated as susceptible to the European privacy directive. This position has met severe resistance of market parties which consider this position to be detrimental for the market potential of RFID [12]. 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 for 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" [7: 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 [13]. 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. 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 [14].

Privacy by Design

The European Commission has held an RFID Consultation process in 2006 in which it has consulted European citizens and companies about, amongst others, the privacy consequences of RFID [15]. Almost 2200 participants delivered input to the consultation process. 65% of them were interested citizen, 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 antenna's, creating a cage of Faraday to prevent transmission of data, removal of the tag from the object, putting tags into 'deep sleep mode'. These are so-called 'end-of-pipe' solutions. 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 [7: 12]. The OECD considers the privacy by design approach "to be more effective in the long run", referring to legislation and self-regulation as other measures [6: 19). Floerkemeyer et al [16] have demonstrated that the OECD privacy guidelines (the Fair Information Principles) 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 FIP regulations 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 Floerkemeyers 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 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 Fair Information

Principles. Technically, this is possible, in practice not all features that can be used, are indeed used to guarantee a level of privacy protection that is as high as possible. Given interests of companies to use the data for 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, transposing 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.

4. Conclusions

RIFD offers opportunities to introduce privacy as a design parameter. Since RFID is still in a preliminary stage of development, and grand scale application of RFID is to be expected in (semi-)public domains such as hospitals, libraries, public transport, passports, an interesting playing field is created for the development of integral PET-based RFID systems.

References

[1] ITU 2005. The Internet of Things. Geneva: ITU

[2] Capgemini. 2005. RFID and Consumers – What European consumers think about radio frequency identifications and the implications for businesses. Capgemini report

[3] http://www.the-infoshop.com/study/ix49177-rfid.html

[4] IDTechEx. 2006. RFID Forecasts, players and opportunities. London: IDTechEx

[5] 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

[6] OECD. 2006a. *Radio-frequency identification (RFID): Drivers, challenges and public policy considerations*. Report DSTI/ICCP(2005)19/FINAL, published on 27 February 2006

[7] Article 29 Working Party on Data Protection. 2005a. *'Working document on data protection issues related to RFID technology'*. 10107/05/EN, 19 January 2005.

[8] Westin, A. 1967. *Privacy and Freedom.* London: The Bodley Head

[9] 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.

[10]. Juels, A., Rivest, R. and Szydlo, M. 2003. *The blocker tag: selective blocking of RFID tags for consumer privacy*. CCS'03, October 2003, Washington.

[11] http://www.rfid-weblog.com/50226711/tagging_of_school_students_halted.php

[12] 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.

[13] EPC global, 2005. *Guidelines on EPC for Consumer Products*. Revised September 2005

www.epcglobalinc.org/public_policy/public_policy_guidelines.html

[14] Centre for Democracy and Technology. 2006. Privacy *Best Practices for Deployment of RFID Technology – Interim draft*, May 2006.

[15] European Commission .2006c. *The RFID Revolution: Your voice on the Challenges, Opportunities and Threats*, Online Public Consultation. 16 October 2006.

[16] Floerkemeier, C., Schneider, R., Langheinrich, M. 2005. *Scanning with a purpose – Supporting the Fair Information Principles in RFID Protocols*.