Privacy Enhancing Technology Concepts for RFID Technology Scrutinised

Jan E. Hennig, Peter B. Ladkin, Bernd Sieker
{jhennig|ladkin|bsieker}@rvs.uni-bielefeld.de

RVS Group, University of Bielefeld, Germany

Abstract. Radio Frequency Identification (RFID) technology is currently being tested and partially deployed for use in supply-chain and retail-shop management at the item level. It is seen as a means to enhance efficiency and introduce new functionality in products such as intelligent fridges or washing machines, who may query their contents.
However, concern has arisen about the possibility of (mis)using RFID technology for tracking and profiling individual people. Privacy, data security and civil rights concerns expressed at some RFID consultation conferences, including those that follow from existing law, may lead to the failure of RFID technology to realise its promise.
We present these concerns and compile a checklist against which we compare proposals to enhance RFID technology to gain privacy protection. Three recent concepts for changing the physical RFID design in order to implant so-called Privacy Enhancing Technolgies (PET) are scrutinised.
Index Terms—Privacy, Privacy Enhancing Technologies (PET), Radio Frequency Identification (RFID), Civil Rights, Security.

1 Introduction

Radio Frequency Identification (RFID) technology uses radio waves to automatically identify objects which, or people who, have an RFID tag attached. It consists of two parts: a tag that contains an identification number and a scanner that triggers the tag to broadcast its identification number. This number usually acts as input to further data processing. RFID is currently used in automatic toll collection systems and livestock identification. There are recent trials to use RFID technology for mail tracking, for product tracking in retail industry, and for tagging human beings in prisons, schools and elsewhere, either by carrying an item with the tag attached or embedded or by direct implantation of such a tag beneath the skin. Future applications could see RFID tags used in passport and identification cards and embedded into money.

Much research is being conducted on improving the technical abilities of RFID technology, such as increasing reading range and improving failure-free operation in environments with a lot of liquid or metal [1,2]. However, although many concerns and even complaints have been expressed about how RFID technology affects personal security, there are few studies that address these concerns.

We use the terms "*security*" and "*secure*" throughout this paper in a limited sense to refer to personal security issues such as privacy, data protection and civil rights, i.e. that no personal rights are restricted.

1.1 The situation today

Supply chain efficiency has become essential for companies to survive in an increasingly competitive business environment. RFID technology is expected to enhance supply chain management. RFID tags and scanners can automatically collect exact data on products and processes in the supply chain. This data allows more efficient management, simply through enabling more awareness of what is currently going on.

1.2 RFID and its peculiarities

RFID tags are very small items that provide an unique identification number to a RFID scanner via a radio transmission if queried by the scanner. This "unique serial number (ID) from RFID tags makes it easy for database and archiving companies to store and associate data by linking to this ID. Information previously only available, if at all, through complex data mining is becoming available through fast database queries." [3]

Variants of microprocessor-based tags are common, but the ID can also be provided chipless by other means such as magnetic interferences. There are active and passive variants. Active tags need a battery to power themselves. This makes them expensive compared with passive tags[1] but allows long reading ranges. Passive tags consume and use the electromagnetic energy sent during a scanner request to power themselves. Although this method only allows very low energy consumption, passive tags are known to be readable at up to 2.5 metres[2]. All such RFID tags are small enough to be easily attached to or even embedded in products or product packaging.

Although there are tags capable of storing several kilobytes of data, the main purpose of a RFID tag is to provide its small[3] ID to a scanner. EPCglobal [4] is leading the standardisation of the so-called "Electronic Product Code" (EPC) with which the IDs are encoded. During the production process it is assured that the ID for each tag is unique worldwide. Labelling products with these tags makes it easy to identify them later by just bringing the product into the range of a scanner. Being unique, the ID can act as a primary key in any database. All additional data, e.g. about the product or its path in the supply chain, can be stored in the database with reference to the key ID. Data processing with such a key reference can be performed quickly. Automatic ID reading avoids human errors such as mistyped numbers.

[1] ASK sells passive tags for €0.15, stated at ETSI workshop in May 2004, see [2]

[2] Demonstrated live with a portable RFID scanner and a tag embedded in a customer card by Alien Technologies at an ETSI workshop in May 2004, see [2]

[3] common are 96 or 128 bit values

Another convenience is that radio communication avoids the need for line-of-sight, which is a clear benefit over barcode scanning. A strong enhancement over barcode scanning, the IDs provided by RFID tags contain not only the product category such as "shampoo from company X" but clearly identify each individual item, e.g. additionally "bottle number 12345", which is a new quality.

1.3 RFID uses

With all these benefits it is understandable that industry is trying to deploy RFIDs as soon as possible. RFID application is not limited to the retail and supply chain industry. Stephan Engberg et al. write in their concept proposal: "RFID technology is already used to prevent shoplifting and the tamper resistance of RFID tags (similar to smart-cards) makes them well suited to protect against counterfeiting, e.g., the European Central Bank is known to consider embedding RFID chips in the larger denomination bank notes for this purpose. Finally, when RFID tags are embedded into artefacts of everyday life, they will enable a wide range of innovative end-user applications, e.g., in the areas of home automation and ambient intelligence environments." [28]

1.4 Outlook

There are an increasing number of concerns, and even some resistance, related to consumer tracking and profiling using RFID technology. We focus in this paper on aspects related to consumer contact with RFID tags and scanners in a retail store environment. Section 2 introduces the privacy and security problems that arise from the deployment of current RFID technology. Section 3 focuses on three approaches that aim (and claim) to heal these problems by introducing different kinds of Privacy Enhancing Technologies (PET) into RFID. We highlight only the main issues. For a complete review, we recommend consulting the original papers. We scrutinise these approaches to evaluate how completely they fulfill their promises. Finally, section 4 discusses the results and draws some conclusions.

2 RFID and Privacy today

Several privacy and civil rights groups are concerned about, and have even protested against, RFID technology deployment [7,9] among them FoeBuD e.V. [10], which plays the major role in the German stopRFID campaign [11]. This campaign proposes that RFID technology use be halted until major privacy issues have been effectively resolved. There are severe problems concerning privacy and data security through deployment of RFID technology in its current form.

2.1 What are the concerns?

Industry representatives speak mostly of barcode enhancement, and barcodes are widely accepted. It is the new capability of RFID tags, not implemented in barcodes, which leads to the perceived threats:

– **Worldwide unique IDs enable tracking**: RFID tags store an unique ID for every item on earth. While technically only a few more bits are stored than with barcodes, this enables every single item, and thus everyone who carries at least one so-tagged item, to be tracked worldwide.
– **Unnoticed remote reading without line-of-sight**: RFID tags can be read without line-of-sight, and without overt evidence that they are being read. For barcode reading there has to be visual contact between tag and reading device. This usually leads to every reading operation requiring the consent of the person carrying the tag by holding the item in front of the reading device. With RFID tags the data can be accessed without a person's consent.
– **Small hidden tags and readers**: Small size and the ability not to need a power supply for the tags makes it possible to install hidden tags, and even readers. For example, RFID tags have already been hidden in packaging.
– **Tracking and profiling through sporadic surveillance**: Some claim that tracking would not be possible because of the limited reading ranges of RFID tags. But for tracking and profiling there is no need for continual surveillance. It is sufficient to read a tag at strategic points such as entrances and exits to buildings and other public structures. At such bottlenecks the reading ranges of existing tags suffice for this purpose.

2.2 Why is this a problem?

Tracking without consent, or even without knowledge, by means of hidden tags or readers directly conflicts with the privacy imperative. Regarding this issue, RFID technology does not stand alone, but another technology comes into play: databases and their supersets—archives. In principle, databases are independent of RFID technology. The main threat to privacy lies in the combination of both technologies (see [5]).

Where this is possible, strict privacy concerns entail that certain kinds of databases and data collections are to be avoided, since inferences that can be made from them can violate privacy imperatives. If data were to be collected, a variety of data-protection laws apply. Katherine Albrecht addresses three different uses of databases in the RFID environment [8]:

– "*Manufacturer's "supply chain" database* poses no consumer privacy threat
– *EPCglobal product info database* poses obvious consumer privacy threats
– *Retailer's POS purchase database* poses invisible consumer privacy threat"

In Germany the legal situation concerning datasets and privacy is well-known since the population census ruling of 1983 (see [6]). "The right for informational self-determination includes the individual's control over relinquishment and utilisation of personal data, including withdrawal: the right to know which data is being collected, where it is being collected, stored, connected to other data and processed, and who has access to the data. It also includes the right to designate what may be done with one's data and the right to instruct institutions storing

someone's data to delete it or to correct data that is wrong. This right of informational self-determination that is currently threatened by RFID technology" [5] due to hidden tags and scanners and due to tag reading without consent.

2.3 How could this data be used?

Plausible scenarios for how these features could be used for attacking privacy and data security are:

- **In-store tracking and profiling**: Privacy also applies to in-store behaviour. RFID scanners are already embedded into "intelligent shelves" [12] so there can be a tight network of RFID scanners installed in a shop, which can be used to detect how customers are interacting with products.
- **Person-related tags**: Tags are already embedded into products that are usually directly linked with a particular individual, e.g. shoes are usually only worn by a single person. Here the tag ID can directly serve as an identifier for the product owner.
- **Tag presence spotting**: Spotting the presence of a tag, e.g. noticing that there is a scanner-tag-conversation happening, can reveal important aspects even if the data contents of the interaction are not known.
- **Combination of tag information**: Individuals can not only be tracked through single tags but also through a combination of tags. For short-period tracking, multiple tag information even with incomplete data can be sufficient. Multiple tags provide for a kind of individual "fingerprint" even if the unique ID cannot be read: Tag presence spotting and the combination of more than one tag presence is enough.
- **Following a unique ID**: This is the intended purpose for RFID application today. Therefore if the tag gets into contact with any citizen, e.g. by him/her carrying the product to which the tag is attached, some degree of personal privacy is lost. The only solution which currently works is to disable the tag permanently, also referred to as "tag killing".

So, RFID technology facilitates the collection of diverse data from everyday life, and in conjunction with database technology enables its combination, and thereby inferencing. RFID technology in combination with database technology thus enables the compilation of movement-, interests- and consumption-profiles of citizens.

2.4 How could this be harmful?

There are many ways in which such data inferencing can be harmful. We mention two. First, if tags were embedded in money, anyone with a RFID scanner could know how much money is in someone's purse. Second, profiling is possible if at least one tag is carried around. Profiling leads to the possibility of performing the following kinds of manipulation:

– **Discrimination**: Purchase and price discrimination, for example, are plausible scenarios. Upon entering a store, the entrance scanner will identify a person and in-store management can adjust purchase offers upon the person's credit worthiness or whatever they choose as criteria. People are thereby treated on the basis of automated prejudices: those treated badly may not even know why they are refused service.
– **General surveillance is possible**: Anyone with a tag could be tracked, even if he/she does not want to be followed. Those whose careers depend upon their perceived creditability, public figures such as politicians, could be tracked clandestinely as they go about their private lives.
– **Tags can act as a trigger for unwanted action**: With such a trigger special personalised advertising could take place[4]. An even more dangerous possibility could be a terrorist action or assassination attempt through a bomb aimed at an individual or group target which is known to carry such a tag. Here a simple presence detection of a tag could result in death.

2.5 Social consequences

Easy data collection can lead to a concentration of power: whoever has access to their data has power over the citizens. In the census ruling of 1983 [6] it was found that citizens might change their behaviour when they believe their data is recorded. This directly conflicts with citizen and human rights guaranteeing freedom of choice and, if RFID promoters pushed this through, it would widely impact society.

With RFID use today, "consent" of the consumer is assumed without the consumer being informed. Construction of de facto constraints in order to promote acceptance of RFID technology is pushed forward. Consumers are lead into temptation to surrender their rights to gain a small rebate. If done en masse this would result in a change to society as well.

Another consequence for society lies in the increasing automation of decision processes through delegating decision responsibility to database inference and analysis programmes. RFID enhances the possibilities for such decision automation.

2.6 What does customer contact mean for RFID?

Customers come into contact with RFID tags and scanners not only at the point of sale but also before then in the store. This has already proven to be problematic: in the USA in a Walmart store in Broken Arrow, there have been tests with RFID in customer space without notifying the customers[16], which action we regard as perfidious: photos were automatically taken of customers in the process of buying lipstick, triggered by embedded RFID tags upon leaving the shelf.

[4] there is a famous scene in Steven Spielberg's movie "Minority Report" [15,14] in which irritating personalised advertising follows the leading character.

Current law deals with data that is explicitly related to the person. At a first glance, RFID product IDs look to be anonymous. But this data becomes person-related as soon as someone engages that product, which is after all the main purpose for a product: it gets into contact with a customer willing to buy it. This is person-relatable data, a new quality not yet covered by law. While in theory one might consider that all data that is broadcast could be regarded as person-relatable, it is here the main purpose of the product to which a tag is attached to get into contact, and stay in contact, with individual customers.

2.7 Secure RFID applications

In-store RFID application can be regarded as secure if tags were only to be used in the storage area and automatically, verifiably deactivated before entering the sales area. However, strict application of this notion would disable some current logistical advantages such as rapid, automated payment assessment at point of sale, and automatic shelf-stock tracking.

In other applications in which it is guaranteed that no citizen will get into contact with them, the use of RFID tags could be regarded as secure, e.g. luggage markings in air traffic use that are removed before the luggage is handed back to the owner.

2.8 Data security guidelines demanded by the concerned groups

We enumerate here some proposed guidelines on how to deal with data so that the application could be regarded as privacy-friendly[7,11]:

- **Avoidance of data collection and making sparing use of data**: Protection of data privacy does not only demand regulation on how data is being stored, processed and passed on, but also on how to avoid certain data being collected in the first place.
- **Transparency**: RFID readers and RFID tags must be clearly labelled.
- **Intended purpose**: The intended purpose for data collection must be explicitly declared.
- **Prohibition of clandestine reading**: Clandestine reading of RFID tag data, tracking of persons either directly or indirectly, tags in shared space such as in sales rooms and tags embedded in money, or personal identification documents must be prohibited or otherwise rendered intractable.
- **No additional burden for the citizen**: There must be no additional burden on citizens to protect themselves, e.g. the long-winded and yet incomplete deactivation procedure at the Metro Future Store [20].
- **Privacy must be the default**: Privacy should not be an optional extra feature, but the core property to be preserved in any application.
- **Legislation must be forward-looking**: Data being collected today even if regarded uncritical may get a different meaning in the future. For example, consider a point in Norwegian-German history: data that was collected at registry offices included religious affiliation and thereby brought death to some during World War II [21].

2.9 Methods

Privacy protection cannot be left to the law alone, because the legal system does not necessarily *prevent* actions such as fraudulent use, but rather deals with the consequences of and *after* the misuse. Misuse is, though, so easily enabled with RFID technology that we believe that preventive measures are needed. There are concepts that deal with privacy protection becoming part of the RFID technology itself, the next sections deal with three of them. If proposed means for privacy protection could be proven to work without enabling backdoors, this would be our preferred solution. A combination of prevention technologies and law enforcement seems advisable.

2.10 Checklist for privacy enhancing concepts

Since privacy concerns are rising, some Privacy-Enhancing Techology (PET) concepts have been developed. We analyse three recent ones. We created a checklist based upon the principles presented above, addressing the issues and their causes, such as avoidance of data collection and transferring control to the citizens. The checklist has also been devised to cover incidents and scenarios that have already occurred [17,18,16] as well as fictional but conceivable scenarios proposed in several discussions and email exchanges [19]. In addition, the checklist includes questions about the complexity and costs of the proposed method.

We created this checklist specifically to evaluate the proposed PET concepts for privacy-conformity, since at least some concepts contain significant privacy misconceptions. We use it as the basis for scrutinising these PET concepts in the following sections.

- O enforces making sparing use of data?
- O makes privacy the default?
- O transfers control to citizens?
- O sends tags to a secure mode automatically?[5]
- O can prove automatic secure mode activation always works?
- O prevents eavesdropping of communication?
- O protects citizens from producer?
- O protects citizens from retailer?
- O protection includes in-store problem?
- O protects tag against presence spotting?
- O does not rely on active protection means?
- O does not interfere with active protection means?[6]
- O avoids use of central database(s)?
- O avoids use of databases at all?
- O enables functionality after point of sale in a secure way?[7]
- O needs to change RFID technology?
- O makes tags much more expensive?
- O makes tags a little more expensive?
- O additional harm to privacy?
- O additional benefits for privacy?
- O retailer also benefits from concept?

[5] unsafe tags are disabled forever ("killed") automatically

[6] e.g. blocker tags [13]. Active protection means are controversial but there should be no loss in privacy protection through interference with other privacy protection

[7] e.g. intelligent fridges or washing machines

3 PET concepts

3.1 PET concept 1

The first PET concept presented here is from Dirk Henrici et al. [22,23,24] (hereafter the proposers). the proposers describe a concept according to which an RFID tag stores a reassigned new ID from a central database on every access. The database would be operated by the tag manufacturer. The authors describe in detail how the necessary transmissions must be performed for the tag to remain anonymous to an eavesdropper. The ID would only be locally valid for a single session. The original ID and a consecutive update number would be encrypted using a hash function and sent over the channel that is regarded unsafe.

Henrici's approach does not deal with the more basic problems such as the trackability of tag-carrying persons through non-authorised RFID scanners, i.e. scanners that are not connected to the central database.

The proposed concept is capable only of detecting successful attempts to block the transmissions, and not unsuccessful attempts. The blocking concept is used e.g. by RSA blocker tags, which are intended to provide an active means of protection to consumers[8]. Blocking through such means is complicated, as the ID changes every time, so the blocker tag could not easily be adjusted to block only a specific number range, as in the RSA concepts. Another issue is that each successful blocking of a write operation for updating the ID can be recognised at the next non-blocked access at the central database. For this purpose the proposers suggest maintaining two entries for each RFID tag in the database: the previous and the current update number. If the former number is transmitted again later, this would show that the previous update procedure had failed. Upon considering other tracking methods than eavesdropping for an ID, the proposers write: "Tracking an individual cannot be prevented employing the proposed scheme if traffic analysis (counting the number of items carried etc.) is used" [22].

Checklist

- O enforces making sparing use of data?
- O makes privacy the default?
- O transfers control to citizens?
- O sends tags to a secure mode automatically?
- O can prove automatic secure mode activation always works?
- X prevents eavesdropping of communication?
- O protects citizens from producer?
- O protects citizens from retailer?
- O protection includes in-store problem?
- O protects tag against presence spotting?
- X does not rely on active protection means?
- O does not interfere with active protection means?
- O avoids use of central database(s)?
- O avoids use of databases at all?
- O enables functionality after point of sale in a secure way?
- X needs to change RFID technology?
- O makes tags much more expensive?
- X makes tags a little more expensive?
- X additional harm to privacy?
- O additional benefits for privacy?
- O retailer also benefits from concept?

[8] The RSA blocker tag concept is controversial, see [13]

Additional harm to privacy arises from:

- **Certain applications of protection means such as RSA blocker tags are rendered useless**
- **Further centralisation of data in manufacturer databases**: If someone breaks into such a database a lot of transactions could be eavesdropped from that point onwards. Using several decentralized databases could help spread that risk.
- **Does not protect the consumer from the retailer at all**: Everyone must still fully trust his/her retailer who utilises this technology and the company operating the database. As this is the crux of the matter, this concept cannot be regarded as a privacy-enhancing technology concept, even if it claims to be.

3.2 PET concept 2

The second concept is presented be Sarah Spiekermann et al. [25,26,27] (hereafter the proposers). The proposers state that they use a "customer-oriented view of the tools of retail marketing"[9]. RFIDs shall not generally be destroyed but designed to be reactivatable later e.g. for handling warranty cases. To ensure privacy the RFID tags shall be sent to a dormant mode at the point of sale. The tags could then be re-awakened by a codeword. This codeword shall be automatically generated by the cash register and printed on the sales slip. Once RFID technology were widely deployed, one could get a portable device for managing the different codewords and the cash register would transfer the codeword directly to this device. The proposers also suggest that a single codeword could be used for an entire household.

Following the proposal, printing of the codewords can always be a fall-back and the customer would thereby stay anonymous. But according to the proposers anonymity would be undesirable from a retail-company point of view: "Only those anonymous customers who pay their items with cash will remain anonymous. Indeed there will be a shopping profile for the anonymous, too. [...] Anonymous customers could understandably not be displayed a shopping history and will not receive personalised rebates". So for a retailer interested in customer profiles general rebates are no longer recommended. The proposers also address the tag costs. They propose using tags with only a weak method of cryptography for cheap products such as bottled milk and more advanced cryptography, resulting in more expensive tags, for more expensive products such as a stereo.

So, the dangers to privacy shall be resolved by disabling the RFID tags at point of sale. From that point on a customer will again be anonymous until he/she reactivates the tag with the codeword printed on the sales slip. In-store tracking is not recognised as a danger here.

[9] "kundenorientierte Betrachtung der Instrumente des Handelsmarketing"

Checklist

- O enforces making sparing use of data?
- X makes privacy the default?
- X transfers control to citizens?
- X sends tags to a secure mode automatically?
- O can prove automatic secure mode activation always works?
- X prevents eavesdropping of communication?
- X protects citizens from producer?
- O protects citizens from retailer?
- O protection includes in-store problem?
- O protects tag against presence spotting?
- X does not rely on active protection means?
- X does not interfere with active protection means?
- O avoids use of central database(s)?
- O avoids use of databases at all?
- O enables functionality after point of sale in a secure way?
- X needs to change RFID technology?
- O makes tags much more expensive?
- X makes tags a little more expensive?
- X additional harm to privacy?
- X additional benefits for privacy?
- O retailer also benefits from concept?

An additional benefit for privacy is:

- **realisation that retailers must not force people to carry "live" RFID tags after the point of sale**

Additional harm to privacy results from:

- **No guarantee of codeword confidentiality**: codewords are generated by the retailer's cash register system so that they could still be known by the retailer
- **Tags retain their unique ID (EPC)**: RFID tags hold the EPC ID number in their memory. This is an unnecessary risk and an attack possibility: The parts of the ID that describe manufacturer and product category can easily be guessed or looked up so that only a smaller part of the number would need to be broken by a brute-force attack
- **protects the products, not the customers**: there is a misconception that cheaper products need not be secured as much as a more expensive product. The key point is not to protect the privacy of the product but to protect the privacy of the customer. The customer privacy should be valued in a way that does not depend upon the price of the product bought.

3.3 PET concept 3

The third concept presented here is from Stephan J. Engberg et al. [28,29,30] (hereafter the proposers). Similar to Henrici's concept the proposers suggest using only locally valid IDs for communication instead of globally valid ones. But here there is no central database to store those IDs. The idea is that any connection between the tag and person is to be rendered impossible from the very beginning. If this can be achieved there won't be any person-related data and no problems with privacy and data security, according to Engberg.

The proposers use two modes for the tags. The first one is a public mode called "epc mode" where the tag will behave similar to today's tags; the second mode is called "privacy mode", in which the tags remain silent. With this

approach the tags would be set to privacy mode automatically at the point of sale and can change back to epc mode on successful key reception later e.g. for handling warranty requests or product recycling.

To achieve this, and especially to deal with the problem of tag presence spotting, the proposers suggest a method that makes the tags not answer any request in privacy mode until the correct activation sequence key is received. This is called *zero knowledge device authentication* as the tag is actually prohibited from doing any transmission at all until the correct key sequence is received. If there were such a transmission, someone could spot the presence of the RFID tag and draw his/her conclusions.

The proposers point out that both sides could benefit if but only if the shop would check for active tags for theft protection at the exit: if the tag enters privacy mode it can no longer be detected by the theft protection devices; if it remains in epc mode the alarm would ring. An alarm would either alert the shop personnel that something is being stolen or show the customer that the tag had not entered privacy mode. If no alarm rings, both shop personnel and customer could relax. Important for privacy protection is that the tag will enter privacy mode before it comes into contact with any citizen.

Checklist

- O enforces making sparing use of data?
- X makes privacy the default?
- X transfers control to citizens?
- X sends tags to a secure mode automatically?
- O can prove automatic secure mode activation always works?
- X prevents eavesdropping of communication?
- X protects citizens from producer?
- X protects citizens from retailer?
- O protection includes in-store problem?
- X protects tag against presence spotting?
- X does not rely on active protection means?
- X does not interfere with active protection means?
- X avoids use of central database(s)?
- X avoids use of databases at all?
- X enables functionality after point of sale in a secure way?
- X needs to change RFID technology?
- O makes tags much more expensive?
- X makes tags a little more expensive?
- O additional harm to privacy?
- X additional benefits for privacy?
- X retailer also benefits from concept?

An additional benefit for privacy is

– **realisation that retailers must not force people to carry "live" RFID tags**

4 Discussion

None of the concepts that has been proposed is yet capable of addressing all relevant issues, even though the situation concerning privacy aspects is much improved over the situation a year ago. We have noted that there are still some misconceptions regarding privacy and data protection. A valid understanding of

the legal and social concept of privacy is a necessary prerequisite to handling privacy issues.

Misconceptions we have identified in one or more of the PET concepts are:

- **Only concerned about eavesdropping**
  Other types of privacy violation are not discussed. This applies to Henrici et al. Privacy protection is, however, a much wider area including, for example, protection of a customer from the retailer.
- **Data protection associated with the product, not the customer**
  This applies to Spiekermann et al., where there is the misconception that cheaper products need not be secured as much as a more expensive product. The key point of privacy protection is not to protect the product but to protect the privacy of the customer. It is hard to see how customer privacy could depend upon the price of the product he/she buys.
- **In-store tracking is not seen as a privacy problem**
  This applies to Henrici et al. and Spiekermann et al. Engberg et al. have recognised in-store tracking as a privacy problem but do not deal with it in their approach. In the store it would be easy for a retailer to install a lot of RFID scanners and start profiling. But customers are no unprotected game: data privacy applies to shared space, too.

Aside from these misconceptions, the PET solutions discussed could solve large parts of the problem. No concept deals with all of them. It may be possible to combine several aspects from different concepts. Still, unsolved problems include in-store tracking and making sparing use of data. Both the concepts of Spiekermann et al. and Engberg et al. take it as crucial that the RFID tag will enter the secure mode before it gets into contact with any citizen. There seems be no technical solution as yet to ensure that this will happen. The only possibility today would be a new law to deal with this issue. Current legal development deals with deactivation at point of sale and thereby thinks of killing the tags. With tags that do not implement PET functionality, killing is the only feasible mechanism. If one of the PET concepts were to be applied to RFID tags, deactivation could be implemented by sending the tag into secure mode. But to cope with in-store tracking issues, this deactivation at the point of sale is too late, except for old-style shops in which products are collected by store personnel instead of the customer him-/herself.

There were thoughts expressed at the ETSI RFID and Telecommunications Workshop [2] about introduction of a type approval standard. During type approval of RFID scanners, automatic deactivation could be implemented through type testing. This, together with tags including proven PET functionality, could be a method of dealing with all interests in the product life cycle. There is no way around the mechanism that tags without PET functionality are killed before getting into citizen contact.

In this paper we looked only at privacy issues. Still, all stakeholders must be part of the consensus process. For the privacy side there are possible solutions in sight. But these are neither complete nor are they proven yet. Our checklist is a

start to a method of evaluating different concepts but it is not known whether it is complete. Research must be undertaken to solve the outstanding problems and to verify existing solutions, especially when combined from different approaches. PETs, once shown to address all privacy problems mentioned, could be a way for gaining acceptance for a sustainable RFID technology which no longer poses threats to the privacy of citizens.

References

1. European Commission Information Society Technologies Group (ICT): "*Wide consultation on wireless tags research needs and workshop*" Presentations page, April 20, 2004, http://www.cordis.lu/ist/directorate_d/ebusiness/workshop.htm
2. European Telecommunications Standards Institute (ETSI): *RFID and Telecommunication Services Workshop – Documents page*, May 25, 2004, http://docbox.etsi.org/ERM/open/RFIDWorkshop/
3. Jan E. Hennig: "*Statement on Digital Wireless Technologies Prepared for the EU 6th Framework Consultation*", RVS-S-04-01, April 2004, http://www.rvs.uni-bielefeld.de/publications/Reports/EU-RFID.pdf
4. EPCglobal Homepage, http://www.epcglobalinc.org/
5. Jan E. Hennig: "*Preserving Privacy in RFID Deployment*", RVS-Occ-04-01, March 2004, http://www.rvs.uni-bielefeld.de/publications/Papers/RFID/preserving_privacy_in_rfid_deployment.pdf
6. Benda, Simon, Hesse, Katzenstein, Niemeyer, Heußner, Niedermaier, Henschel: "*BVerfGE 65, 1 - Volkszählung: Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden*", http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm
7. CASPIAN, ACLU, EFF, EPIC et al: "*Position Statement on the Use of RFID on Consumer Products*", November 2003, http://www.spychips.com/jointrfid_position_paper.html
8. Katherine Albrecht: "*SPYCHIPS: Laying the groundwork for pervasive consumer surveillance*", June 22, 2004, http://www.ftc.gov/bcp/workshops/rfid/albrecht.pdf
9. CASPIAN, FoeBuD e.V.: "*The METRO "Future Store" Special Report – Backlash: German Consumers Demand an End to RFID Experiments!*", March 2004, http://www.spychips.com/metro/protest.html
10. FoeBuD e.V.: Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V., founded 1987, http://www.foebud.org
11. FoeBuD e.V.: Stop-RFID campaign main website, since February 2004, http://www.stoprfid.de
12. Nedap Library Solutions: "*Real time inventory in libraries – Now possible with Nedap's Intelligent Shelf*", May 2004, http://www.nedaprs.com/library/news.asp?ne_id=16
13. Jan E. Hennig, Harald Manninga: "*What are RFID blocker tags? Should I go and get such a thing?*", March 2004, http://www.foebud.org/rfid/blockertags/en
14. Pamela Parker: "*Interactive Ads Play Big Role in 'Minority Report'*", June 21, 2002, http://www.clickz.com/news/article.php/1369861
15. Steven Spielberg: *Minority Report*, 2002, http://www.imdb.com/title/tt0181689/

16. CASPIAN: "*Scandal: Wal-Mart, P&G Involved in Secret RFID Testing*", November 10, 2003, http://www.spychips.com/broken_arrow.htm
17. CASPIAN: "*Gillette reverses position on RFID spy chips at mach 3 speed*", August 19, 2003, http://www.boycottgillette.com/pressrelease8-19.html
18. RFID Journal: "*Benetton to Tag 15 Million Items*", March 12, 2003, http://www.rfidjournal.com/article/articleview/344/1/1/
19. Several personal private discussions including email conversation with members of FoeBuD e.V. (March-October 2004), stop1984.org (2004-09-08), RVS Group (August-October 2004), Monika Ermert (2004-06-25, 2004-04-22), Karl Prince (2004-06-09), Dirk Henrici (2004-05-04), and Stephan Engberg (2004-04-30, 2004-06-03, 2004-08-19)
20. FoeBuD e.V.: "*RFID-FAQ Frage 4.5: Es gibt doch ein De-Aktivator-Gerät, reicht das denn nicht?*", 2004, http://www.stoprfid.de/htm/faq.html#frage4.5
21. Thomas Mathiesen: "*Die Globalisierung der Überwachung*", June 20, 2000, http://www.heise.de/tp/deutsch/special/enfo/6861/1.html
22. Dirk Henrici, Paul Müller: "*Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers*", January 2004, http://www.icsy.de/~archiv/DPArchiv.0080.pdf
23. Dirk Henrici, Paul Müller: "*Tackling Security and Privacy Issues in Radio Frequency Identification Devices*", April 2004, http://www.icsy.de/~archiv/DPArchiv.0086.pdf
24. Dirk Henrici, Jochen Müller, Paul Müller: "*Sicherheit und Privatsphäre in RFID-Systemen*", June 2004, http://www.icsy.de/~archiv/DPArchiv.0096.ps.gz
25. Sarah Spiekermann, Oliver Berthold: "*Maintaining privacy in RFID enabled environments – Proposal for a disable-model*", April 20, 2004, http://www.vs.inf.ethz.ch/events/sppc04/papers/sppc04_spiekermann.pdf
26. Sarah Spiekermann, Uta Jannasch: "*RFID Technologie im Einzelhandel der Zukunft: Datenentstehung, Marketing Potentiale und Auswirkungen auf die Privatheit des Kunden*", April 2004, http://www.wiwi.hu-berlin.de/iwi/internetoekonomie/deutsch/publikationen/index.php
27. Sarah Spiekermann: "*Zwischenbericht 2004 Projekt InterVal*", August 2004, http://www.wiwi.hu-berlin.de/iwi/internetoekonomie/deutsch/publikationen/040815_interval_zwischenbericht.pdf
28. Stephan J. Engberg, Morten B. Harning, Christian D. Jensen: "*Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience Protocols.*", September 2004, http://dev.hil.unb.ca/Texts/PST/pdf/engberg.pdf
29. Stephan J. Engberg: "*A new Approach to RFID Privacy Zero Knowledge Device Authentication*", April 2004, http://obivision.com/Papers/EU_RFID_Workshop_20040420_obi.pdf
30. Stephan J. Engberg: "*Privacy through virtual identities in Infrastructure*", November 2002, http://obivision.com/Papers/Ist_Living_with_Security_20021106.pdf