Science, Technology & Innovation Studies Vol. 2, March 2006

ISSN: 1861-3675

STI Studies

www.sti-studies.de

On the Potential Social Impact of RFID-Containing Everyday Objects

Kerstin von Locquenghien

received 8 November 2005, received in revised form 30 December 2005, accepted 16 February 2006

Abstract

Radio Frequency Identification (RFID) is a rapidly evolving technology. While industrialists hope that the use of RFID will bring about great benefits, civil rights activists warn against the dangers. Since RFID pervades everyday life more and more, this paper deals with its potential impact on individuals. Currently private persons are least included in the public debate, although perhaps they will be affected the most by potential negative effects.

Critics are especially concerned about the potential violation of privacy. Due to its informational infrastructure RFID could be used for surveillance purposes. Many people therefore fear a surveillance state. Looking at the use of RFID on the product level, completely dynamic pricing and business models could be developed. If everyday objects record and send context sensitive information via embedded RFID tags, this might strongly influence our perception of these objects and our emotional attitude towards them. This relationship between man and RFID containing smart objects is expected to differ from the relationship between man and machines as well as man and computers, as a new function as well as a new significance are added to already well-known objects.

Last but not least, this paper also points out RFID's potential impact on health and environment, which has barely been discussed in public so far.

The analysis shows that, apart from certain opportunities, considerable risks have to be dealt with. However, panic, as suggested by some critics, seems unreasonable as the development is still wide open. This should rather be considered a great chance: it offers the possibility to play an active role in the shaping of RFID within a legal democratic process. In this process all members of society are likewise responsible for future developments.

1 Introduction

Today Radio Frequency Identification (RFID) is a rapidly evolving technology and at the same time it is strongly disputed among experts. Some companies already use RFID while others plan its implementation in the near future (SOREON 2004). Enormous progress is predicted for the miniaturisation of chips, by lower costs, an increase of storage capacity and developments in materials sciences (Mattern 2003: 11). Thus, numerous innovative applications of RFID will become possible. Even today industry is highly committed to this technology, because it reckons with more efficient processing conditions in the long run.[1] Yet civil rights activists draw the attention to the risks of RFID concerning data protection and privacy.[2] Some even draw the attention to a possible fall of the democratic constitutional state regarding RFID (Brust 2004). Specifically alarming is the fact that the general public – especially in Germany – hardly knows anything about RFID (Capgemini 2005), while it pervades everyday life, continually and unnoticed by many people.

This paper wants to present a survey of some potential effects of RFID on everyday life with a special focus on questions and consequences from the individual's point of view. Furthermore, the different positions in the debate will be discussed as well as the question of accountability concerning the development of this technology.

[1] One of the most important publications in this field is the RFID-Journal. It presents a survey of the latest technological developments and pilot projects, www.rfidjournal.com [as at 28.12.2005].

[2] Among the main critics are, for example, Katherine Albrecht, chairperson of the Organisation CASPIAN (USA), www.spychips.org [as at 28.12.2005], Rena Tangens and padeluun, chairperson of FoeBud e.V. (Germany), www.foebud.org/rfid [as at 28.12.2005].

2 RFID: technological basis and examples of usage

2.1 Technological basis

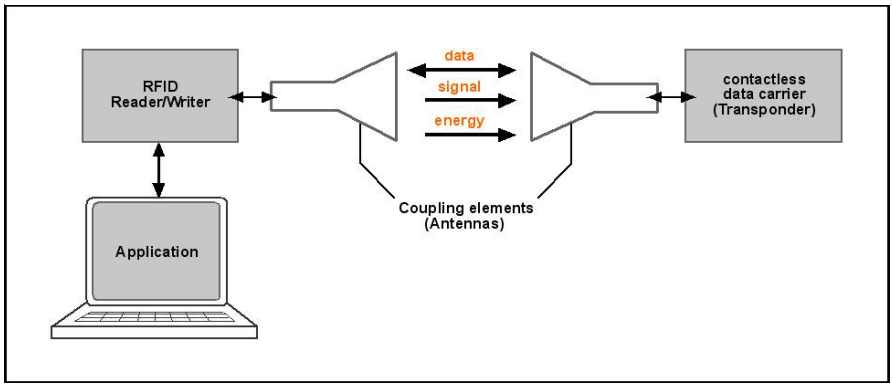
RFID technology is an automated identification technology. By means of RFID objects, animals or persons can be clearly identified over a certain distance. RFID systems always consist of two components: a transponder and a reader. The reader consists of a reading and possibly a writing unit[3] and an antenna. It transmits energy to the transponder, scans its data and possibly makes the transponder store additional data. A transponder only sends data if it is near a corresponding reader ("on call"). The transponder, also called 'tag', is the actual data carrier, consisting of an antenna and a chip. On this chip a unique identification number is stored. Between 16 and 64 kb of additional data can be stored, depending on the kind of transponder (Finkenzeller 2002: 8).

RFID tags exist in different sizes and shapes: as self-adhesive labels (so-called *smart labels*), as glass cylinder transponders, as plastic transponders, as watches, keychain pendants, or as plastic cards *(*so-called *smart cards).* There are numerous other types which can be adjusted according to usage (Finkenzeller 2002: 14-22). The forgery-proof nature of RFID tags is commonly considered as very high (Finkenzeller 2002: 8; Oertel et al. 2004: 90). RFID systems differ on frequency bands, transmission ranges, storing technologies, security systems[4] and means of power supply. All these factors together constitute the qualities of the system. Therefore one cannot speak of *the* RFID system. Transmission ranges often appear to

[3] Not every RFID system contains a writing unit, because not all kinds of transponders are rewritable and allow the storage of additional data on top of an unique identification number.

[4] There are different procedures for authentification and codification available.

Chart 1- Basic components of an RFID system
(based on: Finkenzeller 2002: 7)



be unclear. In exceptional cases a transmission range of up to one kilometre can be reached. However, the systems that are used in Europe only reach a few centimetres – because of legal restrictions on the one hand and the development status on the other hand – *smart labels* for instance which are applied to the product level, or 1.2 to 4 metres for applications in the logistics branch (RF-ID 2004; IDTechEx 2004; Oertel et al. 2004: 29).[5]

RFID systems still have technical deficiencies. Among them are

- the high costs,
- the low degree of standardisation concerning the compatibility of products from different manufacturers or of different frequency ranges,[6]
- gaps in the security systems used,[7]
- performance problems in the vicinity of metal and certain liquids
- as well as a lack of globally standardised regulations for radio frequencies.

All these problems have hindered global usage so far (Oertel et al. 2004: 101-111).

However, experts believe that the present technical problems will be largely overcome by 2010 (Oertel et al. 2004: 106) and they expect a further exponential increase in performance, according to Moore's law (Moore 1965).[8] For the European market a strong growth of the RFID sector has been predicted for the following years (SOREON 2004; Oertel et al. 2004: 104-111). Germany is even expected to become market leader by the year 2008 (SOREON 2004).

2.2 Examples of usage

In the following paragraph a few examples of today's usage will be presented to show how RFID works and can be used, also to start reflections on potential future usage. They are just examples, because the tech-

[5] The technical information of this chapter largely follows Klaus Finkenzeller`s "RFID-Handbuch" (2002), which I would like to recommend for further technical details.

[6] The use of multiple frequency readers could be a big step forward. One of the first of its kind was presented at the end of 2005, cf. http://ubiks.net/local/blog/jmt/archives3/004561.html [as at 28.12.2005]

[7] These are discussed in detail in the essay on "Risiken und Chancen des Einsatzes von RFID-Systemen", published by the Bundesamt für Sicherheit in der Informationstechnik (Oertel et al. 2004: 41-65).

[8] In summary Moore`s law from 1965 says that a computer`s CPU capacity will roughly double every 18 months. So far this prediction has also been confirmed in the field of storage capacity and communication range. Simultaneously prices for microelectronic components will fall radically while the CPU capacity remains the same. These facts facilitate a widespread use of a technology.

nology is rapidly evolving at present; consequently the number of pilot projects and new applications is constantly increasing.

Identification of animals, objects and people

The identification of animals belongs to one of the traditional applications of RFID. Especially cattle, sheep and goats are tagged with electronic ear chips or implanted transponders. If an animal passes a reader, it can be clearly identified and additional data on origin, diseases, sex and previous whereabouts can be read. According to a regulation by the EU all goat and sheep populations from a certain size are to be electronically tagged and all the data is to be stored in a central database by 2008 (Press releases 2003).

Similarly RFID is already being used for the identification of containers in transportation, of garbage containers and for the unique identification of products (Oertel et al. 2004: 67). Gradually, it is also used to identify people. In Japan RFID is used for the surveillance of school children, for example (Heise 2004). In a pilot project of the New York Jacobi Medical Center patients are kept under surveillance with an RFID wrist band. This application also enables hospital staff to access medical records directly on the patient (Fiutak 2004).

Protection against counterfeiting of documents

Since the end of 2005 Germany just like other countries has started introducing passports containing biometric data such as fingerprints. They are encoded in an RFID tag and when passports are controlled they can be scanned and compared with the features of the passport holder. This is supposed to increase the forgery-proof nature of the document (Die Welt 2004). The implementation of RFID in banknotes is also being discussed (Hascher 2003; Krempl 2004).

Protection against theft

Retail has already been using 1-bit transponders for the last 40 years. Transponders are attached to products and readers are installed in security gates near the exit. When a product is bought, the transponder is removed or re-set to "0".[9] The security gates can be passed with paid-for products, but a stolen article sets off an alarm. Libraries or electronic immobilisers make use of RFID in a similar way (Oertel et al. 2004: 81-82).

Access control

RFID has already been firmly established in the field of access control. Many companies use transponders in the form of cards or keychain pendants as electronic identification to control building access and record the working hours. In many holiday regions transponders replace hotel keys, ski passes or local credit cards. They also play a growing part in the sale of tickets for public transport or cultural events (Oertel et al. 2004: 76-80). Since the beginning of 2004 the Baja Beach Club in Barcelona, Spain, has offered guests a small, implantable glass cylinder chip to identify them. They in turn use it to pay for food and drinks (Gossett 2004).

Tracking and tracing

RFID is used more and more to track baggage and parcels, and for toll collection (Oertel et al. 2004: 76-80). However, from the industry's point of view the supply chain management is considered most important. The production and distribution of goods requires complex partner networks. RFID tags on the product mean that it can be individually tracked in real time as it moves from location to location. The supply chain management becomes transparent and can be organ-

[9] Which is not to be confused with "turned off" as the tags technically cannot be turned off in a reliable and safe manner, yet.

ised more efficiently in the future due to increasing automation. Today mainly car industries use this technology during the production process. In preliminary pilot projects it is also tested to track products until they are in the consumer's hands, for example in the Metro-Future-Store in Rheinberg, Germany (Oertel et al. 2004: 84-89).[10]

3 Potential impact of RFID on everyday life

All participants of the discussion seem to agree that huge changes will be brought about by new RFID applications. However, the quality of these changes and their intensity are widely disputed. In the following chapter some potential effects will be described.

3.1 Protection of the private sphere

Critics regard the invasion of privacy as one of the most crucial potential effects (Aspekte 2005; CASPIAN et al. 2005; Oertel et al. 2004: 110). Discussing this issue it is necessary to understand what the term *private sphere* means and why it is considered to be indispensable in a free democratic system. More over, it is equally necessary to establish criteria for the protection of privacy.

Description and value of the private sphere

The discussion about the effects of RFID applications is based on Beate Rössler's definition of *privacy* (2001; 2003). The term *informational privacy* refers to all data about a person, in general everything other people know about a person (Rössler 2003: 17). *Informational privacy* especially includes individual-related data.

In 1995 the European Union (EU) laid down a privacy policy which also says that the term *individual-related* refers to those data of a person which can directly or indirectly be used to clearly identify a person (Europäisches Parlament 1995).

Gary T. Marx offers a different approach by defining certain limits of privacy (Marx quoted by Bohn et al. 2003: 205-206):

- "natural limits" refer to the physical limits of observability;
- "social limits" refer to the basic confidence that social groups have in other people's attitude towards private data;
- "physical or temporal limits" refer to the fact that different areas of life can exist in isolation without influencing each other;
- "situational limits" refer to the fact that what is said or done unthinkingly may be forgotten after some time.

Accordingly a person's privacy is violated if one of these limits is crossed.

The protection of the private sphere is valuable, because it protects the individual's liberty and autonomy (Rössler 2003: 18). The protection of privacy is therefore founded on everyone's right to lead a free and autonomous life. This statement is also reflected in the argumentation of the Bundesverfassungsgericht (German Constitutional Court) concerning the so-called Census Verdict. The term "*informationelle Selbstbestimmung*" (control over one's personal data) and its value are expressed most clearly here:

"*If somebody cannot overlook with sufficient certainty which information concerning certain areas is known to his social environment (…) he can be significantly hindered from planning and deciding in a self-determined way. (…) If somebody has to reckon with the registration of his participation in a meeting or a citizens' initiative by the*

[10] More information on this project can be found online at www.future-store.org.[as at 06.11.2005]

authorities and with the danger that risks for him are involved, he will perhaps not exercise his corresponding basic rights (German Constitutional Law, Article 8, Paragraph 9)." *(Krisch 2005: 9)*

Therefore the *control over one's personal data* is a basic principle of the free democratic constitutional state. It is as important for the individual's chances for development according to the German Constitution as for the free democratic state which is based on the active participation of its citizens (Krisch 2005: 9).

Criteria for the protection of the private sphere

From the explanations above criteria for the protection of informational privacy and the use of personal data can be deduced. They were summarised and are internationally known as the "Principles of Fair Information Practice" (CASPIAN et al. 2003; OECD 2003). In principle personal data shall only be collected in a range as limited as possible, only if highly necessary and they shall only be used for fixed purposes ("collection limitation and purpose specification"). Personal data shall remain concealed as far as possible and only be passed on or published in a limited and selective way ("anonymity and pseudonymity"). It must be guaranteed that unauthorised persons do not have access to data which has been collected ("confidentiality"). Individuals have the right to know when and under which circumstances data is collected. This can be guaranteed by an obligation to obtain approval for example. Later on data subjects shall have access to their data as well as the possibility to correct or delete it and to object to its use ("transparency and access"). This means that the operators of RFID systems must be considered reliable in so far as they need to show a serious interest in keeping the data up-to-date, as well as complete and correct. They are also obliged to use only the amount of data agreed upon for the specific purpose agreed upon. There must be an entity to which individuals can complain in case of conflict ("confidence and security").

Example: RFID at retail

Many publications focus on the use of RFID at retail trade. The reason is perhaps that some companies plan on introducing RFID in the near future or they already test it (SOREON 2004). RFID in conjunction with the so-called Electronic Product Code (EPC) will be used for the globally unique identification and tracking of items from production to disposal (Krisch 2005: 4).[11] Apart from product-specific data, further information about the context of the product can be stored. The following paragraphs are to be understood as a demonstration of potential using possibilities.

The EPC system of tags in connection with so-called *smart shelves*, i.e. shelves equipped with readers, can record the shopping behaviour of a costumer without being noticed. In conjunction with the use of a personalised loyalty card, a credit card or surveillance cameras the data collected can be unmistakably be tied to the identity of this person. Classic "data mining"[12] methods allow the construction of detailed consumer profiles afterwards. It may contain information about a customer's habits, his potential spending capacity and his social environment. This information can be directly used for individual pricing as well as advertising measures.[13]

---

[11] Further information: www.epcglobalinc.org (6.11.2005)

[12] "Data mining" describes the systematic detection and extraction of unknown information, mostly automatic or semi-automatic, from a great amount of data, to analyse among other things a consumer's shopping behaviour and to develop targeted marketing strategies (Wikipedia 2005).

[13] This is demonstrated for example by a virtual tour through the Metro Future

As the tags remain functional after the products have been bought, they can be scanned by every reader which is equipped according to the same standards. As a result, without knowledge (or consent) someone can be identified via the products carried along. If a combination of data concerning place, time and identity of a person is automatically stored in a backend database, a person's movement from location to location can be retraced.

Moreover it is possible that alongside the global EPC network, more databases are set up by the operators for their own individual purposes. In general, this means: The more readers are installed in public space, the more detailed an individual can be profiled and tracked.

Potential restrictions on the private sphere

The example mentioned above shows that the afore-mentioned criteria which should guarantee the protection of the private sphere and the "Principles of Fair Information Practice" can all be easily violated.

The reason for this is mainly the technology's "invisibility", as the scanning and storing of data can go unnoticed by the person concerned. The readers can be placed invisibly. Tags can be incorporated into the packaging material or embedded in a way that goes unseen to the naked eye. Data transmission needs neither direct contact nor is it restricted to intervisibility, therefore it is virtually impossible for people to know when or where the reading process takes place and they are being identified.[14] Additionally the example of the Metro scandal at the beginning of 2004 shows that the use of RFID is not always disclosed to customers (FoeBuD 2004).[15] Hereby the criteria of reliability and security are also violated, as individuals cannot have confidence in unknown data processors and they cannot exercise their right to be informed about their data, to correct or cancel them, if they do not know who they are (cf. Krisch 2005: 15). Data processing is not transparent to private persons – this contributes to the "invisibility" of the technology. According to Krisch, the data collected can also be linked and retrieved without a directly known name. Thus the persons concerned do not have the opportunity to be informed about the storage of their data and check it, because they would have to know the product specificcodes. Yet this is impossible without special technical equipment (cf. Krisch 2005: 13).

Now and again cases are uncovered where the security systems of RFID operators fail when data is transmitted or stored in a backend machine. These cases can result in data abuse (Rentrop 2005). Yet experts believe that privacy is less put at risk by attacks on the RFID system, than by its normal operations (Oertel et al. 2004: 55).

Existing protection measures

The fact that RFID is being increasingly used on the product level may lead to a situation where nobody can escape the collection of personal data via RFID. In this case the simplest way to

---

Store, where the use of RFID is tested in a pilot project. Metro Future Store Initiative: www.future-store.org/multimedia/virtual tour mpeg1.zip. (10.4.2005)

[14] In comparison, if a barcode system is in use the customer will always know because a contact between barcode and scanner is necessary to read the code. Besides, the barcode only contains the name of the product (e.g. Philadelphia Cream Cheese), while EPC contains a globally unique ID (e.g. Philadelphia cream Cheese Nr. 9388485DCo).

[15] Metro had integrated RFID tags into customer loyalty cards without informing the customers. This practice was stopped after the scandal had been uncovered by the civil rights organisation FoeBuD und Katherine Albrecht from the organisation CASPIAN, because Metro feared that negative publicity would continue to harm its image (FoeBud 2004).

protect oneself by not participating would no longer be an option.

So far there are no serious protection measures from the technical point of view. Although customers in the Metro Future Store's pilot projects are offered the possibility to deactivate the tags, they cannot check whether the tags have been completely deactivated or whether they have only been rendered temporarily inoperable and can be activated again at a later time without being noticed (FoeBuD 2004). A further protection means propagated by the industry is the use of "blocker tags". They behave like transponders and disrupt transmission. However, they cannot be looked upon as reliable as the closeness to the reader is mostly accidental. Neither the reliability, nor whether it functions correctly, can be controlled (cf. Oertel et al. 2004: 53; CASPIAN et al. 2003). The removal of a tag from a product cannot be rated as an acceptable solution as well as consumers might thus exclude themselves from services or even be suspected of theft or forgery. Presently the only reliable method to prevent data transmission between tag and reader is to keep the tag wrapped in aluminium foil (Langheinrich 2004: 24). But this is not an acceptable and long-lasting solution by which consumers can be protected. Critics of the present situation are therefore primarily concerned with the fact that producers and traders simply shift the responsibility to customers who themselves have to pay attention not to suffer from disadvantages (Langheinrich 2004: 29; CASPIAN et al. 2003).

Another way to solve the problem could be found by the introduction of new laws. Although data protection acts on a national and European level exist, there are concerns that it will become more and more difficult to control and maintain them because data processing technologies are getting increasingly complex and miniaturised (Oertel et al. 2004: 109). As we have already seen, the use of RFID might result in conflicts with present data protection regulations (Laschet/Brisch 2005: 84). The authors of the study on the "Modernisierung des bundesdeutschen Datenschutzgesetzes", commissioned by the German Ministry of the Interior, conclude that the data protection law is by no means prepared for the development of omnipresent data processing (Roßnagel et al. 2001). Therefore existing deficiencies in the laws are to be found and new laws must be created, which are especially suited to the use of RFID. While this has not been realised by many politicians (FoeBud 2005), today the first attempts are (being) made.[16]

Comparison with other technologies

To assess the effects of RFID on the *informational private sphere* RFID ought to be studied in the context of similar technologies. There are huge differences in the experts' evaluation of the situation. It ranges from the opinion that the new systems do not really offer anything that has not been possible so far, to the concern that tracking via RFID implies a new quality of surveillance (Oertel et al. 2004: 55).

There are already numerous possibilities to collect data or observe private persons via the internet, surveillance cameras, the storage of telephone calls or the use of credit or payback cards to name but a few. It is already widely known that especially the internet can be used for the purpose of data-mining (cf. Reischl 2001). Moreover it is common practice today to sell personal data to third parties (Leuthardt 1996: 146). In all these cases data can be collected without being noticed by the user and the actual purpose can rarely be checked.

[16] There are examples on the EU-level (cf. Article 29 Data Protection Working Party 2005) as well as in the Federal Republic: The Ministry for Consumer Protection held a conference on "Verbraucherpolitik in der digitalen Welt. Der gläserne Kunde", where RFID was directly dealt with (cf. FoeBud 2005).

Likewise the definite aim of numerous projects is the tracking of individuals (Reischl 2001: 175). Many suppliers of mobile phones and radio networks offer the localisation of mobile phones and their owners as standard equipment that goes with *Location Based Services* (Reischl 2001: 173). The Global Positioning System (GPS) which is used in navigation systems can locate objects even more exactly.

Therefore it has to be emphasised that the private sphere can also be violated in similar ways by other technologies. Yet RFID is different from some of the other technologies because of "always being on", which means that there is no possibility to switch it off voluntarily.

3.2 The discussion about a possible emergence of a surveillance state

RFID like no other technology of *Ubiquitous Computing*[17] has led to concerns about surveillance in the population (Langheinrich 2004). In the following chapter the questions if and how RFID can be used for governmental surveillance and which role surveillance plays in a democratic society will be dealt with, as well as the issues of how on the one hand the government, on the other hand the population cope with it and which consequences may result from it.

Surveillance in western democracies

Due to certain specific qualities RFID can be used to observe individuals. But the adoption of RFID does not necessarily lead to surveillance. However, the informational infrastructure provided by RFID can generally create the demand for further interpretation, and, consequently, for surveillance also by the government (Rössler 2001: 226; Oertel et al. 2004: 47).

Foucault (1976) analyses Bentham's principle of the *panoptic* and transfers it metaphorically to the disciplinary techniques of modern society. Foucault understands the principle of the *panoptic* as an important organisational principle of western liberal societies. The permanent possibility of surveillance hereby causes the individuals to discipline themselves almost without the need for any social control. Deleuze further develops Foucault's idea of the *disciplinary society* in his theory on the *controlling society* (Deleuze 1993: 255). While surveillance techniques in Foucault's sense are linked with institutions, Deleuze emphasises the penetration of society with flexible and permanent control and surveillance techniques. He sees the basis for the change in the means, i.e. in new forms of communication and surveillance techniques (Deleuze 1990: 259). From today's point of view RFID can be regarded as such a technique in many ways.

Mass media often deal with surveillance only in connection with totalitarian regimes. This leads to the impression that surveillance necessarily leads to a totalitarian regime, i.e. that only this kind of regime would use it. But surveillance is not absolutely negative and does not only exist in totalitarian regimes. It may have very different effects in different kinds of cultural contexts with different value systems (cf. Lyon 2001: 26). For example, it can also serve the protection of individuals and groups, as well as the safeguarding of liberty, equality and social justice. Moreover it is indispensable for the protection of the democratic constitutional laws (cf. Lyon 2001: 31).

But the abuse of surveillance by the government can never be excluded. Abuse occurs, if the government uses its power inadequately and does not

[17] *Ubiquitous Computing* describes the omnipresence of digital data processing and can be understood as the enhancement of the Internet Era. It contains the possibility to retrieve data anywhere at any time (Mattern 2001). Mark Weiser is looked upon as father of the *Ubiquitous Computing* theory. He decisively determined this term in his essay from 1991 (cf. Weiser 1991).

act in the interest of the majority of the population, or violates civil liberties. This would be the case if data were collected and used for controlling purposes secretly or against a person's free decision (cf. Rössler 2001: 226). Selection processes which are based on the scientific interpretation of data and which may result in the discrimination of entire groups of the population constitute another significant problem (cf. Peissl 2003: 13). Schulzki-Haddouti (2004: 170) mentions the example of the discrimination against religious minorities, for example after the terrorist attack of September 11, 2001 in the United States, which was caused by indistinctly defined computer search. This process is also called *social sorting* (Lyon quoted in Mattern 2003: 25). The protection of the population from crime and the protection of privacy both require a careful act of balancing. Furthermore, to which extent the preventive collection of data is regarded legitimate, also depends on the subjective impression of a threat posed by criminal attacks on the one hand or a violation of constitutional rights by the government on the other hand.

In the last few decades a gradual reversion of attitude towards law and order could be noticed. The original presumption of innocence has changed more and more into a general presumption of guilt (Leuthardt 1996: 110). This change of the searching principle can be realised when looking at the change of legal regulations in the last few years. While formerly unlawful behaviour had to precede the search, today preventive observation is commonly established in law (cf. Leuthardt 1996: 109). The most recent trend is the adoption of *profiling* methods. Therefore one might suppose that the data aggregation caused by RFID will also attract the government's attention.[18]

Citizens and surveillance

Citizens have become used to surveillance and do not reflect it very critically anymore, an attitude which might become dangerous. Especially the terrorist attacks on September 11, 2001 have raised awareness about issues of national security. For many people the individual's need for security seems to outweigh the interest in the protection of privacy. Therefore Greiner (2005) considers the population's need for security to be the actual "enemy of freedom". On the other hand many citizens are aware of surveillance but do not feel disturbed or restricted in their privacy (cf. Winsemann 2005).

The wide-spread acceptance of surveillance leads some authors to speak of a "nothing to hide mentality" (cf. Winsemann 2005).[19] This behaviour can obviously be attributed to the common concern to arouse suspicion by refusing observation measures. Jutta Limbach, former president of the German Constitutional Court, is worried that people will lose the pleasure of expressing their different opinions and committing themselves, if the government electronically observes its citizens in all domains of life (cf. Schulzki-Haddouti 2004: 159). Whether the

[18] This is exemplified by the latest legal changes, for example the abolition of confidentiality in banking in Germany on April 1, 2005 (Kaiser 2005), the demand for a prolongation of storage time for telephone data to three years by the German Minister of the Interior Otto Schily (cf. Deutschlandradio 2005), the demand for an extension of DNA analyses and the setting up of a nationwide gene database (cf. WDR 2005), or the decision of April 12, 2005, which permits police and public prosecutors to profile and track individuals via GPS (Bundesverfassungsgericht, 2005).

[19] Winsemann mentions as examples the widespread use of pay-back cards in spite of public information campaigns, web cams in discotheques and pubs or a chip implanted into the upper arm as a method of payment. She comes to the conclusion that these measures are rather looked upon as "fashionable accessories" and that the consequences concerning data protection and privacy are ignored (cf. Winsemann 2005).

individual citizens consider the purpose of observation to be legitimate *(positive observation)* or a restriction on their civil rights or even a threat *(negative observation)* depends on their respective threat assessment.

Historical context: Technologies and fears of surveillance

The debate about RFID and surveillance should be seen in historical context. Since the 1980s there has been a debate about fears of surveillance in context with technological development (Lyon 2001: 31). Leuthardt examines the historic development of surveillance methods and fears in correlation with electronic data processing strategies. He shows that from the first databases to the development of chip cards to the introduction of the internet the possibilities of data aggregation and interpretation have been continually improved and therefore also have been accompanied by fears of surveillance (Leuthardt 1996). During the last decades slogans like "electronic panoptic" or the "transparent citizen" or the "transparent society" were coined which also re-appear in today's debates. We already leave electronic data tracks permanently which can be used for observation and controlling purposes by interested parties (cf. Leuthardt 1996: 129). Therefore the question if RFID leads to a surveillance state is obsolete. More important is the question whether RFID and its embedding into a network of existing surveillance technologies will cause a new quality of surveillance. But this question could not be answered clearly so far.

3.3 RFID and consumer goods

Products equipped with RFID tags can, to a certain degree, be called "smart", because they offer the use of further functions and because there are processes which can be automated.[20] Especially in networks with other technologies RFID-"smart" objects can trigger far reaching changes in everyday life which have been hardly issued in the public media so far.

Dynamic pricing

The existence of highly automated networks of RFID equipped devices can lead to an economy in which the information about the "location and quality of goods, the means of production and people is available in real time and unprecedented accuracy" – a "*now-economy*" (Müller et al. 2003: 172).[21] This might result in an approximation to the so-called "*perfect market*" (ibid.). Besides, the pricing system can be controlled in a highly dynamic way in real time on the basis of analysis in supply and demand (Bohn et al. 2003: 212-213). In practice this could involve an automatic change of a product's price at very short intervals. This kind of pricing might mean in turn that the predictability of prices becomes more difficult or even gets impossible for customers who might become confused. Moreover, the question arises whether this model is fair. Will a dynamic pricing system discriminate against certain groups of consumers, maybe because their working hours do not allow them to go shopping at a favourable time? Or is it more likely that the shelves will always be refilled according to demand without the need for higher prices? Even

[20] "Smart" has become an in-term and is therefore insufficient for a clear definition of the qualities implied (von Locquenghien 2005: 4-10). In this paper "smart" only refers to the limited technical qualities and possibilities of RFID unless else specified.

[21] Three qualities identify a "perfect market" in the classic micro-economic theory: 1. the exchangeability of goods, 2. the complete overview of all market participants over the latest information and procedures and 3. the abolition of temporal or physical advantages for certain competitors. With this explanation Bohn et al. refer to David Krep's "A course in microeconomic theory" (cf. Bohn et al. 2003: 213).

today dynamic pricing models are used in other branches. Bohn et al. mention for example the hotel prices at the time of a fair, ski passes in the high season or on weekends, flight prices and internet auctions (2003: 213). But the acceptance of these examples cannot automatically be assumed for other products, as these mentioned goods could be considered luxury goods, which are dispensable if necessary. Basic food does not allow this option, however.

It has already been explained that prices can be established individually on the basis of customers' profiles. Here as well the question arises as to how far social inequalities might be strengthened or more justice can be created. In this case the retailers' attitude would be crucial.

Silent commerce

Objects which "purchase" certain things themselves because of their context sensitivity are called "*autonomous purchasing objects*" (Bohn et al. 2003: 216). A frequently cited example is the fridge that checks its contents and takes care of the refill according to the consumption behaviour of its owner. The term used for this procedure is "silent commerce" (ibid.). It shows that things happen in the background without a person directly being involved in the decision-making process. While on the one hand this passive way of shopping can be very comfortable, it might also lead to a feeling of loss of control. To avoid this danger, the procedures should be made as transparent and comprehensible for the user as possible. Another problem is the accountability issue. What happens if the fridge has ordered the wrong product? Who is responsible for the damage? There are fears that "the reasons for the damage which is done because components from computer hardware, programmes and network data working in combination can usually not be cleared up, because the complexity of these systems cannot be controlled, neither from a mathematical nor a legal point of view" (cf. Behrendt/Hilty/Erdmann 2003: 20-21). This is a basic problem of partly autonomous systems. However, considering the fact that up to now there are hardly any autonomous purchasing objects in private use, I consider exaggerated fears of this kind of risks to be wrong. The factors mentioned can still be taken into account when these products are designed and there is a realistic chance that most of them can be regulated by the functioning market itself.

Pay-per-use business models

Bohn et al. consider an extension of the pay-per-use business model onto all kinds of everyday objects possible via objects which would be uniquely identifiable and equipped with the latest communication technology (2003: 217). Thus the producer of a sofa might automatically get a transfer of a few cents when it is used., i.e. when sensors coupled with RFID tags and wireless internet connection would report this. Bohn et al. mention different examples of already working pay-per-use business models, e.g. charges for telephone, electric current and water as well as public transport and television. Before every use a conscious decision concerning the financial consequences is necessary.

While one might assume on the one hand that this leads to stress as these decisions about the use of everyday objects would have to be made very frequently, one has to keep in mind on the other hand that the conscious decision making concerning the consumption of electric current or water has also been shifted to the background. But simultaneously this example shows that the charges arising can hardly be checked afterwards. This could become a problem with everyday objects and increases the possibilities of abuse. Users might fall into a debt trap, a development which could be observed when mobile phones were

introduced on a large scale (cf. Schufa 2004: 172). Yet there is proof that the increase of information and the fact that people got used to the terms of payment resulted in a decrease of debts (ibid.). It might be possible that the wide-spread use of these terms of payment for everyday objects would also lead to this effect. Besides, the social consequences would be interesting: Will fewer guests be invited if each use of the sofa is charged? Will other seating habits be developed? Will this lead to a change in the cultural significance of property?

Specified services

If RFID tags are embedded into objects, it is possible to assign all the single parts of a machine to a producer. It is conceivable that a function could be incorporated into machines which would prevent spare parts from another firm being put in. This would severely restrict the free choice of spare parts and it would imply the exclusion of certain services for customers with lower incomes. This principle can also be transferred to other services like maintenance and repair. It is questionable, however, if companies would be interested in such a function at all, as they would risk a damage to their image if customers did not accept the principle. On the other hand the question would have to be studied whether the use of the prescribed parts would even increase the safety of the product significantly and thus bring about an advantage for the user.

Dynamic and personalised insurance models

Insurances might also be interested in personalised data which reflects the everyday behaviour of individuals (Bohn et al. 2003: 218). RFID and sensor containing objects can be able to record the individual consumption and behavioural habits of their owners, to transmit these to insurances that in turn could offer dynamic and highly personalised insurance bonuses. The smart refrigerator could transfer information about eating habits, the sensor-equipped car would be able to transmit detailed data about the driving habits of its owner to the insurance (cf. Langheinrich 2005). However, the question must be raised, if these data produce a true picture of reality and if this could lead to a fairer billing system. In general, problems could arise comparable to those in the previous examples concerning verifiability, abuse and financial calculability. Yet a positive effect based on individually measurable data could be an increased awareness for issues of health and risk in the population.

Digitally upgraded everyday objects

By means of RFID every object can be assigned specific information. This information can be retrieved automatically via the internet and transmitted by different media. So far mainly producers and operators can make use of data storage on the object, but in the future consumers might also reap the benefits. These could be operating instructions for electronic devices, recipes for cooking, information about the ingredients of food, instructions for care and maintenance, guarantee information, advertisements, bonus features or personal comments which can be scanned by privately owned readers. Presumably the additional digital features will increasingly influence the assessment of products' qualities.

"*What is displayed in every single case, may depend on the context, i.e. on the question whether the consumer is a long-time customer and has paid a lot for the product, whether he is over 18, which language he speaks, or his present whereabouts – maybe even on the question whether he belongs to the right party.*" *(Mattern 2003: 9)*

Mattern's statement shows that the information can be offered in a very flexible and personalised way, but at the same time he refers to the risks involved. He also raises the question of

who determines the contents of the object's statement, and who guarantees their objectivity and accuracy (Mattern 2003: 11). An objection would be that the contents of every mass media, e.g. television or internet, can be ideologically prejudiced just as well and in a certain respect are always shaped by subjective interests. Likewise the accuracy of information can rarely be completely guaranteed and proved. In this sense RFID containing objects are simply a new medium which will be affected by an already existing problem. Besides, this issue of acceptance of digitally upgraded objects will also depend on the influence a customer can exercise on the display of the data. An advertising film constantly showing on a display of the refrigerator would most likely be disapproved of, yet occasional requested information on a certain product might be welcomed.

3.4 RFID's influence on health and environment

Consequences for health and environment must also be considered a factor influencing everyday life. Little research has yet been done in this field. Generally speaking,

"*the influence on environmental aspects like disposal, consumption of resources and energy by a large scale implementation of ubiquitous computing technologies […] is hardly predictable, especially because a change of lifestyles, more dynamic economic circles and new consumer habits as a consequence of the new technology will react upon these parameters*" *(Bohn et al. 2003: 231).*

With good reason this statement can be transferred to RFID, as it is looked upon as one of the key technologies of ubiquitous computing.

Electromagnetic radiation

RFID being a radio technology is connected with electromagnetic radiation when operated. Health risks caused by radiation have been researched and debated in public so far only with reference to mobile phones and their effects. RFID's radiation effects on health have not been clarified as yet and long term effects in particular have not yet been researched (cf. Hilty et al. 2003: 240). Furthermore it is well-known that the distance between the source of radiation and the body has a strong influence on the intensity of the exposition. Future applications like the integration of RFID tags into clothes or their implantation into the human body may therefore raise the level of exposition to radiation. Advocates of RFID object that the radiation of RFID is lower than that of mobile phones and that it is not always active but only "on call", and therefore not or significantly less dangerous (cf. Cisco 2004). However, in workplaces where RFID systems are constantly in use, the radiation might have a much more negative effect than expected. This demonstrates the "urgent need for research" (Behrendt/Hilty/Erdmann 2003: 18).

Implantation of transponders

Medically, the implantation of RFID tags into a human body is already feasible, but it is not widespread yet. There are no accurate research results concerning harmful effects of RFID tags implanted into the body. First concepts for medical applications of RFID are now being developed, for example the implantation of a sensor and transponder to permanently measure and monitor the intraocular pressure of patients with glaucoma permanently (cf. IMS 2005). For chronically ill people, the monitoring of different physiologic parameters could mean a higher degree of safety and a better quality of life. Moreover, an implanted RFID chip could incorporate personal medical information, which might be life-saving especially in cases of emergency. However, there is a critical objection that the implanted medical information could create a problem concerning data protection laws. For chronically ill people the

advantages might outweigh the disadvantages, for many others, however, the dangers would be considerably higher than the advantages. Furthermore it has to be dealt with the issue that the implantation of RFID tags might lead to negative psychological consequences.[22] What does a person feel about an implanted and simultaneously linked tag which sends data from inside the body: would it be perceived as a prosthesis, as a foreign body, as an unwanted intruder or traitor? Or even as a fashionable accessory as can be seen in the case of the Baja Beach Club? The question if RFID tags are implanted voluntarily, is definitely one of the most crucial issues for their acceptance.

Health management

A tag on food and medicine containing detailed information on the product may help to promote applications which compare the ingredients automatically with individual incompatibilities and give warning signals in case of danger. Besides, a check could be kept on the correct taking of medicine. The first prototypes of smart medical cupboards reminding users of taking their medicine or informing them about medicine that expired have already been developed (cf. IMS 2003). Yet it has to be criticised that the devices for dispensing them are difficult to operate for the intended target group, i.e. mainly senior citizens. The interface would have to be improved and become better suited to the target groups.

The genuineness of medicines

The pharmaceutical industry in the United States plans to integrate RFID tags into the packaging of medicine in order to document their genuineness and location because many products are forged (cf. Computerwoche 2004). This could mean a higher security standard for patients as fakes can be distinguished from originals, if patients get the possibility to scan the tags. But the question remains if the problem of fakes will not simply be transferred. If criminals for example used empty original packaging and filled it with forged products then the possibility to distinguish this mediciation from originals would be considerably lower. The problem could only be solved by killing the tags after the consumption of the medicine. But this is technically not yet possible and it would probably not be easily implemented.

Stress

RFID has the potential to reduce stress in everyday life. Automated admission control might shorten waiting queues for example. If people were reminded of their everyday tasks they might carry them out more reliably. But, depending on the use of the technology, this might also lead to negative stimulus satiation (cf. Hilty et al. 2003: 245). It has to be emphasised that even the uncertainty of potential risks might result in a physical health risk. The feeling of being threatened can for example lead to insomnia, and correspondingly involve health problems (ibid.: 238). This feeling may be caused by fears of radiation, surveillance or of losing control likewise.

Electronic waste

During my research I did not find any plans for the disposal of RFID electronics. Today RFID applications are mainly confined to closed systems. "Disposable labels" in the form of *smart labels* on products at retail for example are not widely in use.

"*If smart labels were affixed to all supermarket products in the future, then billions of these chips would get into the household waste. Although a single chip weighs far less than a gram the total sum of all these chips would add up to several thousands of tons of*

[22] Paul Virilio (1999) extensively considers the relationship between technology and the body, yet without giving attention to a special technology (also see Misoch 2005).

electronic waste." *(Bohn et al. 2003: 231)*

Separate disposal could become a problem because tags can be integrated into packaging materials. On the other hand, RFID offers the possibility to optimise recycling processes because waste materials could be identified and separated more efficiently with the help of the data stored (ibid.). This might simplify waste disposal for the individual as machines could do the separating automatically. But up to today this concept cannot be technically realised yet.

Monitoring of the environment

In the future tiny sensors and RFID equipped devices might be able to monitor and document environmental phenomena in a so far unprecedented way. These data collections could lead to a potentially new understanding of certain processes in nature which in turn could enable scientists to find out about environmental disasters at an earlier date. Accordingly early warning systems could be used in a more targeted way. In the same way information about the populations of threatened species might be collected which could lead to new scientific findings. But apart from the tagging of animals there can hardly be found any applications in this sector until now (Oertel et al. 2004: 95).

3.5 The relationship to RFID containing objects

If embedded RFID tags can make everyday objects smart, then this can influence the perception of these objects as well as the individual's relationship to them. Psychologists and sociologists have only just gained interest in RFID. For a more detailed analysis the existing and future pilot projects would have to be studied extensively. The following chapter deals with the factors that might influence the relationship between man and RFID containing objects.

Recognition of RFID containing objects

It is important to know whether the individual can realise at all that an object has been changed i.e. that it represents more than its physical appearance and its conventionally known functions. Only then the difference in the relationship to an RFID containing object can be examined. The following factors are decisive:

- *The visibility of the technology*: many tags which are in use today are so small that they can hardly be noticed, and are placed invisibly or integrated into packaging material. The same can be said for readers, as well.
- *The visibility of the reaction to the reading process*: even if the technology itself is not visible, the reaction to the reading process can be noticed, for example when a ski pass automatically releases the turnstile.
- *Knowledge about the use of the technology*: this can be achieved by information about the use of smart labels on a shelf in the supermarket, on the packaging of products or by public notice, for example.

It can be assumed that those different ways of recognition will influence the individual realisation of the object and the emotional relationship to it. Yet if the object does not seem changed at all, RFID will probably neither directly influence the way the object is perceived nor the relationship between man and smart objects. It would also be necessary to study delayed or indirect effects which are not in first place linked with the visibility of the change.

Benefits of the application

Furthermore it is important to know whether the new quality is seen positively or negatively. Hereby a few elements might be of importance:

Personal advantage:[23] If the additional quality or function is seen as an advantage, it can be assumed that the object will be looked upon in a more positive and confident way than one without this technical upgrading. The degree of the positive realisation would grow accordingly if the function was used frequently and the positive result confirmed. It is different with applications which are complicated or do not function in the expected way and therefore lead to frustrations. The user might become mistrustful and finally see the object in a negative light (cf. Norman 1988: 11).

Advantage for others: Not every application implies a direct advantage for the user of the object. If a customer profile is created for marketing purposes the subjective advantage can only be perceived indirectly, if at all, or might even be seen solely on the operator's side. If users don't accept this kind of external benefit, they might feel to be at the mercy of the object or even feel threatened by it.

Impression of autonomy and aliveness

For different reasons electronically upgraded everyday objects are attributed the ability to act autonomously or being alive. On the one hand the way of communication about smart objects influences the perception of their qualities. In related literature human qualities are often used to describe so-called smart objects. This kind of rhetorical description produces the picture of a strongly emotional and socially aware autonomous acting object, which in reality simply executes certain pre-programmed functions without any reflection (Reeves/Nass 1996: 4).

Apart from the descriptive attribution of human qualities, observable features also contribute to the perception and evaluation of smart objects (Rammert/Schulz-Schaeffer 2002: 29). The impression of autonomy furthermore depends on the degree of context sensitivity and the actual autonomy of decision making behaviours, as has been briefly shown by the examples above. If the technological process is unknown, a person easily gets the impression that the object itself is "speaking" or "acting" and therefore appears to be "intelligent", because of the reaction caused by the object directly being attributed to the object itself.[24] In this context Adamowsky speaks of a re-emerging so-called "magic effect" (2003: 4), which is even emphasised by the "invisibility" and complexity of technologies such as RFID. Turkle (2004) also deals with the effects of "affective computing". Especially children tend to react emotionally to "intelligent" toys and clearly attribute to them a certain kind of "aliveness". More and more this effect can also be observed with grown-ups. However, the problem of grown-ups ascribing "aliveness" to "intelligent" artefacts is by no means new: it has already been noticed and analysed by Weizenbaum in the 1970s (cf. Weizenbaum 1977). From today's perspective the topic becomes even more relevant than ever before because of the development of new advanced technologies and their integration into highly complex systems.

The physical as well as the communication design can therefore be considered as one of the most influential factors for the relationship between man and RFID containing objects. When looking at today's applications, it becomes clear that the design options for RFID containing smart objects and their communication interfaces are still wide open.

---

[23] Here I transfer Donald A. Norman's (1988) results from his psychopathologic study of everyday things to RFID containing everyday objects.

[24] For a detailed analysis of technical artefacts and their perception as acting objects, I would like to refer to the paper of Werner Rammert and Ingo Schulz-Schaeffer (2002) who extensively deal with relevant concepts.

A smart card implying the function of a key is most likely regarded as a new physical form of a key or a type of switch. The card would be looked upon as an instrument, which would not result in a closer emotional relationship (cf. Krämer 1998: 83-84).

If the object's physical or communication design gives the impression of being alive however, it would most likely lead to a greater emotional reaction of the user.

Therefore RFID containing objects should first be separated into different categories before being analysed. As a result it has to be taken into account, that the relationship between man and RFID containing smart objects can probably neither be treated like the man-machine-relationship nor like the man-robot or the man-computer-relationship. In these cases the function and the significance of newly introduced objects had been altogether new. Thus they could be perceived as a unity, and new ways of man-machine interaction could be acquired step-by-step. Comparatively, RFID applications are expected to lead to unfamiliar situations because of the fact that everyday objects with already well-known qualities will additionally gain one or more so far unknown qualities.

4 Conclusion

The consideration of potential future applications and their possible effects shows, that RFID has the power to bring about considerable changes. Apart from some chances, serious risks are to be expected. Today the extent of the changes can not yet be assessed as the future development of RFID technology and applications is still widely open.[25] It is exactly this openness as well as the awareness of potential risks which offer the chance to the people to deeply influence future developments and to actively take part in this process. A generalisation of concerns about RFID should be avoided, however, because of the diversity of existing technical systems and different applications in connection with their intentions. All members of society likewise have to take on the responsibility regarding the further development of RFID.

Developers: They can dictate, facilitate or exclude certain ways in which a technology can be used by creating the technical and organisational framework. "What is technically prevented, does not have to be outlawed." (Roßnagel/Lütge 2005) as soft- and hardware regulate the rules in cyberspace in a similar way as laws do in the real world (Lessig 1999: 6).

Operators:[26] Their attitude decisively determines the way RFID systems are deployed and how they treat those people who are affected by the applications. Operators should be greatly interested in maintaining the trust of customers and staff (cf. Capgemini 2005: 16). Therefore they should keep their specific application of RFID as transparent as possible and allow affected people to make a conscious decision about their participation as well as the option to permanently deactivate their tags. Operators should equally pass on some of the benefits resulting from the application of the RFID system (ibid.).

The government: It is the government's task to mediate between the different interest groups in society and to intervene if necessary. This includes the revision of existing laws in order to guarantee their applicability in the context of new technologies as well as

[25] In the TA-Swiss paper on the precautionary principle in the information society from the year 2003, this open potential for development is called "Januskopf chances" as the situation offers chances as well as risks (cf. Hilty et al. 2003: 265).

[26] The term shall include everybody who operates an RFID system and/or uses the data collections produced hereby for data mining purposes.

the establishment of new laws. Hereby the government should apply the methods of technology and risk assessment and include experts in their discussions. At the moment the impression that German data protection officials are not taken seriously is alarming.[27] Furthermore, globalisation processes lead to a legislation, which is tremendously under pressure due to international requirements or other internationally powerful states. Even though national governments oftentimes have an area of discretion concerning international laws, they rarely make use of it, but follow the general trend, without investing much time in a critical reflexion.[28] The close tie between politics and industries also state a severe influence on political decision making. Last but not least the responsibility of states also implies the protection of the individual's rights. A fact which nowadays sometimes seems to be eclipsed.

Citizens: They also bear part of the responsibility by their attitude towards new technological developments and applications, a fact which is often underrated. At present the population does not seem to be well informed about RFID. This might be due to a bad information policy on the part of the operators, but also due to a lack of interest on the part of the population. This attitude is alarming, because a passive behaviour neglects the chances of shaping the path of new technologies. However, this can lead to the dreaded imbalance in the consideration of different social interests. Civil rights activists, for instance, have already proved that and how the population can actively exercise its influence through various actions.[29]

"*While the analysis of a technology only answers the question of what the future can bring, the question of what the future may bring must be answered by a societal process.*" *(Mattern 2003: 29).*

Although controversies about risks and conflicts are often perceived as disturbances for society, economy and democracy, they should rather be seen as a learning process, as a productive element and a basis of democracy (cf. Petermann 2001: 7). Therefore the present discussion about the spreading of RFID should be regarded as an important occasion to re-negotiate the different interests occurring within a society and to discuss the fear of an omnipresent surveillance by the government. Basis for this process should be a balance of considering personal advantages as well as potential social costs. The democratic system is not a rigid structure; on the contrary it requires negotiation and must be understood as a never-ending permanent re-shaping process (cf. Marchart 2002: 296-297). Panic related to RFID technology, like some authors try to spread, is not justified at this time. However, they make an important contribution by bringing the topic to public attention and by taking part in the public debate.

The most important issues at stake should be to objectify the discussion, to inform and involve the public, to abolish existing myths about the technical potential of RFID, to intensify

[27] For example the data protection official of the Federal Republic, Peter Schaar, had criticised the Federal Government in his progress report published in April 2005. The Minister for the Interior, Otto Schily, countered that Schaar "had gone beyond his competence, and that it was not his task to assess technical questions and comment on political decisions" (DPA 2005).

[28] A good example is the quick implementation of biometric data in passports for example. (cf. DPA 2005; Die Welt 2004). Biometric data is stored on RFID tags integrated into the cover of the passport. The functionality of RFID tags as well as their potential health risks have not been assessed yet especially in long term use. Additionally they have been implemented regardless of emerging concerns about privacy issues.

[29] E.g. CASPIAN (www.spychips.com) or FoeBud e.V (www.foebud.org/rfid).

the interdisciplinary debate about potential effects of the technology as well as to commonly work on a stable societal solution.

5 References

Adamowsky, Natascha, 2003: Totale Vernetzung – totale Verstrickung? In: *Bundeszentrale für politische Bildung* (ed.) 13. Oktober 2003: *Aus Politik und Zeitgeschichte – Beilage zur Wochenzeitung Das Parlament*. B 42/2004, 3-5.

Article 29 Data Protection Working Party 2005: *Working document on data protection issues related to RFID technology,* 19.1.2005. <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf> [as at 24.5.2005]

Aspekte (ZDF), 2005: *Überwachungswahn – Was übermorgen aus den Bürgerrechten wird*. In: ZDF-Kulturmagazin "aspekte" 16.04.2005.

Behrendt, Siegfried; Hilty, Lorenz M.; Erdmann, Lorenz, 2003: Nachhaltigkeit und Vorsorge – Anforderungen der Digitalisierung an das politsche System. In: *Bundeszentrale für politische Bildung* (ed.): *Aus Politik und Zeitgeschichte – Beilage zur Wochenzeitung Das Parlament.* B 42/2004, 13-20.

Bohn, Jürgen et al., 2003: Allgegenwart und Verschwinden des Computers. In: Grötker, Ralf (ed.) 2003: *Privat! Kontrollierte Freiheit in einer vernetzten Welt.* Hannover: Heise Zeitschriften Verlag GmbH & Co. KG., 195-245.

Brust, Friedhelm 2004: *RFID und die Arbeitswelt.* <www.rifid.de/neu/analysen/arbeitswelt.html> [as at 16.3.2005]

Bundesverfassungsgericht 2005: Leitsätze zum Urteil des Zweiten Senats vom 12. April 2005 – 2 BvR 581/01. <www.bundesverfassungsgericht.de/entscheidungen/frames/rs20050412_2bvr058101> [as at 7.11.2005]

Capgemini (ed.) 2005*: RFID and Consumers – What European Consumers Think About Radio Frequency Identification and the Implications for Business*. <www.capgemini.com/news/2005/Capgemini_European_RFIDreport.pdf> [as at 22.2.2005]

CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) et al., 2003: *Positionspapier über den Gebrauch von RFID auf und in Konsumgütern*. <www.foebud.org/rfid/positionspapier> [as at 15.3.2005]

CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering), 2005: *How spychips pose a threat to privacy*. <www.spychips.com> [as at 15.3.2005]

Cisco (ed.) 2004: Wireless Systems and RF Safety Issues. <www.cisco.com/en/US/products/hw/wireless/ps4570/productswhite_paper09186a0080088791.shtml> [as at 2.5.2005]

Computerwoche Online (ed.) 2004: *Mit RFID gegen Viagra-Fälscher.* <www.computerwoche.de/index.cfm?pageid=256&artid=67648> [as at 2.5.2005]

Deleuze, Gilles 1993: Postskriptum über die Kontrollgesellschaften. In: Gilles Deleuze 1993: *Unterhandlungen 1972-1990*. Frankfurt am Main: Suhrkamp, 254-261.

[Deutschlandradio 2005] Forderung nach längerer Speicherung von Telefondaten findet Unterstützung, 15.3.2005 <www.dradio.de/dkultur/sendungen/interview/356278/>

Die Welt 2004: *Ab 2005 Fingerabdruck im Reisepaß*. <www.welt.de/data/2004/10/27/351895.html> [as at 24.5.2005]

DPA 2005: *Schily weist Datenschützer-Kritik zurück.* <www.stern.de/computer-technik/computer/?id=539278> [as at 8.5.2005]

Europäisches Parlament/Rat der Europäischen Union 1995: *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*. Amtsblatt Nr. L 281, 23. November 1995. 31-50. <www.dsk.gv.at/31995L0046d.htm> [as at 9.4.2005]

Finkenzeller, Klaus 2002: *RFID-Handbuch – Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten*. München: Hanser.

Fiutak, Martin 2004: *Siemens: RFID-Armband funkt Patientendaten*. <www.zdnet.de/news/tkomm/0,39023151,39124434,00.htm> [as at 3.4.2005]

[FoeBuD 2004] Der Metro-Skandal. <www.foebud.org/rfid/metro> [as at 14.03.2006]

FoeBuD 2005: Newsletter Nr. 8: *RFID – Verbraucherschutz entdeckt den Datenschutz*. <www.foebud.org/aboutus/newsletter/newsletter-06-2005#5> [as at 8.6.2005]

Foucault, Michel 1976: *Überwachen und Strafen*. Frankfurt am Main: Suhrkamp.

Gossett, Sherry 2004: *Paying for drinks with wave of the hand – Club goers in Spain get implanted chips for ID, payment purposes.* <http://worldnetdaily.com/news/article.

asp?ARTICLE_ID=38038> [as at 26.4.2005]

Greiner, Ulrich 2005: Polizei im Kopf. In: *Die ZEIT* 3.3.2005. <www.zeit.de/2005/10/Freiheit?page=all> [as at: 8.2.2006]

Hascher, Wolfgang 2003: Identifikation mit Mini-Chips. In: *Elektronik Net*. 19/2003. <www.elektroniknet.de/topics/kommunikation/fachthemen/2003/0021/index_b.htm> [as at 3.4.2005]

Heise Online, 2004: *Funketiketten für japanische Schulkinder.* <www.heise.de/newsticker/meldung/49004> [as at: 3.4.2005]

Hilty, Lorenz et al., 2003: *Das Vorsorgeprinzip in der Informationsgesellschaft – Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt.* <www.taswiss.ch/www-remain/reports_archive/publications/2003/030904_PvC_Bericht.pdf> [as at 21.2.2005]

IDTechEx 2004: *RFID System Frequencies. An Overview of RFID frequencies for chip based tags.* <www.idtechex.com/products/en/article.asp?articleid=7&topicid=79> [as at 30.3.2005]

IMS 2003 (Fraunhofer Institut für Mikroelektronische Schaltungen und Systeme), 2003: *Annual Report 2003*. <www.ims.fhg.de/institut/pdf/IMS_Annual_Report_2003.pdf> [as at 2.5.2005]

IMS 2005 (Fraunhofer Institut für Mikroelektronische Schaltungen und Systeme): *Transpondersystem zur Messung des Augeninnendrucks (Datenblatt),* <www.ims.fraunhofer.de/datenblaetter/wcs/IODS/iods.html> [as at 2.5.2005]

Kaiser, Tobias 2005: Was der Staat wissen darf. In: *Die ZEIT* 31.03.2005. <www.zeit.de/2005/14/Argument_14> [as at 6.4.2005]

Krämer, Sybille 1998: Das Medium als Spur und als Apparat. In: Krämer, Sybille (ed.): *Medien, Computer, Realität: Wirklichkeitsvorstellungen und neue Medien*. Frankfurt/Main: Suhrkamp, 73-94.

Krempl, Stefan 2004: Das Internet der Dinge. In: *Computerworld* 5/2004. <http://viadrina.euv-frankfurt-o.de/~sk/Pub/rfid-cw04.html> [as at 29.3.2005]

Krisch, Andreas 2005: *Die Veröffentlichung des Privaten – Mit intelligenten Etiketten vom grundsätzlichen Schutz der Privatsphäre zum Selbstschutz-Prinzip.* Wien: Institut für Technologiefolgeabschätzung (ITA), Österreichische Akademie der Wissenschaften. <www.oeaw.ac.at/ita/pdf/ita_05_01.pdf> [as at 7.4.2005]

Langheinrich, Marc 2004: *Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID Technologie.* <www.vs.inf.ethz.ch/pupl/papers/langhein2004rfid.pdf> [as at 11.4.2005]

Langheinrich, Mark, 2005: "*Visionen, Potenziale und Folgewirkungen des Pervasive Computing*", paper presented at the conference " Pervasive Computing – Totale Vernetzung. Visionen eines neuen Verhältnisses von Technik und Gesellschaft", Dortmund, April 22-23, 2005.

Laschet, Carsten/Brisch, Klaus, 2005: RFID: Fluch oder Segen – Ein rechtlicher Annäherungsversuch. In: *StoffR* 2/2005. Berlin: Lexxion Verlagsgesellschaft mbH, 80-84.

Lessig, Lawrence 1999: *Code and other Laws of Cyberspace.* New York: Basic Books.

Leuthardt, Beat 1996. *Leben online – Von der Chipkarte bis zum EuropolNetz: Der Mensch unter ständigem Verdacht.* Reinbeck bei Hamburg: Rohwolt Taschenbuch Verlag GmbH.

Locquenghien von, Kerstin 2005: *Tagged! Über die potentiellen Auswirkungen von RFID-"smarten" Alltagsgegenständen* <www.bewegungsfrei.de/tagged/material/kvl_EMMA_TAGGED_eps.pdf/> [as at 28.12.2005]

Lyon, David 2001: *Surveillance Society – Monitoring everday life*. Buckingham: Open University Press.

Marchart, Oliver 2002: Demonstrationen des Unvollendbaren. Politische Theorie und radikaldemokratischer Aktivismus. In: Enwezor, Okwui; Barsualdo, Carlos; Bauer, Ute M. 2002 (eds.): *Demokratie als unvollendbarer Prozess*. Ostfildern: Hatje Cantz, 291-306.

Mattern, Friedemann 2001: *Pervasive/Ubiquitous Computing*. <www.gi-ev.de/informatik/lexikon/inflex-pervasive-computing.shtml> [as at 21.2.2005]

Mattern, Friedemann 2003: Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing. In: Friedemann Mattern (ed.): *Total vernetzt – Szenarien einer informatisierten Welt*. Berlin: Springer, 1-41.

Misoch, Sabina, 2005: "*Von der extrakorporalen zur intrakorporalen vernetzten Technik: mögliche Folgen einer Entwicklung*", paper presented at the conference "Pervasive Computing – Totale Vernetzung. Visionen eines neuen Verhältnisses von Technik und Gesellschaft", Dortmund, April 22-23, 2005.

Moore, Gordon 1965: Cramming more components onto integrated circuits. In: *Electronics* 38 (8), 114-117. <ftp://download.intel.com/research/silicon/moorespaper.pdf> [as at 25.2.2005]

Müller, Günter et al., 2003: Geduldige Technologie für ungeduldige Patienten: Führt Ubiquitous Computing zu mehr Selbstbestimmung? In: Friedemann Mattern (ed.): *Total vernetzt – Szenarien einer informatisierten Welt*. Berlin, Heidelberg: Springer, 159-186.

Norman, Donald A. 1988: "*The psychology of everyday things*". New York (USA): Basic Books.

OECD 2003: *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* <www.oecd.org/dataoecd/16/7/15589558.pdf> [as at 9.4.2005]

Oertel, Britta et al., 2004: *Risiken und Chancen des Einsatzes von RFID-Systemen.* Bonn: Bundesamt für Sicherheit und Informationstechnik – BSI. Ingelheim: SecuMedia Verlags-GmbH. <www.bsi.bund.de/fachthem/rfid/RIKCHA.pdf> [as at 22.2.2005]

Peissl, Walter 2003: *Privacy: Ein Grundrecht mit Ablaufdatum? Inderdisziplinäre Beiträge zur Grundrechtsdebatte.* Wien: Institut für Technikfolgeabschätzung (ITA) der Österreichischen Akademie der Wissenschaften. <http://hw.oeaw.ac.at/3232-8a> [as at 15.4.2005]

Petermann, Thomas 2001: Technikkontroversen und Risikokommunikation. In: *Büro für Technikfolgeabschätzungen beim Deutschen Bundestag (TAB) (ed.)* Juni 2001: TAB-Brief Nr. 20, 5-7. <www.tab.fzk.de/de/brief/brief20.pdf> [as at 7.4.2005]

Press Releases 17.12.2003: *Tierseuchenbekämpfung: Byrne begrüßt die Verabschiedung von Kennzeichnungsvorschriften für Schafe und Ziegen durch den Rat.* <http://europa.eu.int/rapid/pressReleasesActon.do?reference=IP/03/1761&format=HTML&aged=0&language=DE&guiLanguage=en#file.tmp_Ref_1> [as at: 2.4.2005]

Rammert, Werner/Schulz-Schaeffer, Ingo 2002: Technik und Handeln. Wenn soziales Handeln sich auf menschliches Verhalten und technische Abläufe verteilt. In: Rammert, Werner, Schulz-Schaeffer, Ingo (eds.) 2002: *Können Maschinen handeln?* Frankfurth/New York: Campus, 11-64.

Reeves, Byron/Nass, Clifford 1996: *The Media Equation*. Cambridge: University Press.

Reischl, Gerald 2001: *Gefährliche Netze*. Wien: Ueberreuter.

Rentrop, Christian 2005: *Autos knacken mit RFID.* <www.netzwelt.de/news/69631-autos-knacken-mit-rfid.html> [as at 26.4.2005]

RF-ID.com 2004: *869 MHz RF-ID Tags Read Only and Programmable.* <www.rf-id.com/rfidit.html> [as at 30.3.2005]

Rössler, Beate 2001: *Der Wert des Privaten.* Frankfurt/Main: Suhrkamp.

Rössler, Beate 2003: Der Wert des Privaten. In: Grötker, Ralf (ed.) 2003: *Privat! Kontrollierte Freiheit in einer vernetzten Welt.* Hannover: Heise Zeitschriften Verlag, 15-32.

Roßnagel, Alexander et al. 2001: *Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Inneren.* Berlin: Eigenverlag des Bundesinnenministeriums

Roßnagel, Alexander/Lütge, Gunhild , 2005: Ist der Datenschutz tot? (Interview). In: *Die ZEIT* 17/2005: 31.

Schufa 2004: *Schuldenkompass 2004: Empirische Indikatoren der privaten Ver- und Überschuldung in Deutschland.* Wiesbaden: Schufa Holding AG. <www.schuldenkompass.de/downloads/sk04_gesamt.pdf> [as at 25.4.2005]

Schulzki-Haddouti, Christiane 2004: *Im Netz der inneren Sicherheit – die neuen Methoden der Überwachung*. Hamburg: Europäische Verlagsanstalt.

SOREON Research 2004: *Überholspur: RFID-Markt Handel in Europa 2004-2008.* <www.pressrelations.de/new/standard/result_main.cfm?r=155879&sid=&aktion=jour_pm&print=1> [as at 2.4.2005]

Turkle, Sherry 2004: *Computers and the Human Spirit.* <www.aec.at/de/archives/festival_archive/festival_catalogs/festival_artikel.asp?iProjectID=12934> [as at 24.2.2005]

Virilio, Paul 1999: *Die Eroberung des Körpers*. München: Carl Hanser.

WDR 2005: *Erfolgsgarant Gen-Analyse? Diskussion um Erweiterung der Gen-Datenbank.* <www.wdr.de/themen/politik/recht/gendatenbank/index.jhtml> [as at 16.4.2005]

Weiser, Mark: *The Computer for the Twenty-First Century, Scientific American* 265 (3): 94-104, also available online: <www.ubiq.com/hypertext/weiser/SciAmDraft3.html>, as at: 5.2.2006)

Weizenbaum, Joseph 1977: "*Die Macht der Computer und die Ohnmacht der Vernunft*", Frankfurt am Main: Suhrkamp.

Wikipedia 2005: *Data Mining.* <http://de.wikipedia.org/wiki/Data-Mining> [as at 10.4.2005]

Winsemann, Bettina (Twister) 2005: *Auf dem Weg in die "transparente Gesellschaft" des David Brin?* <www.heise.de/tp/r4/artikel/19/19328/1.html> [as at 16.4.2005]