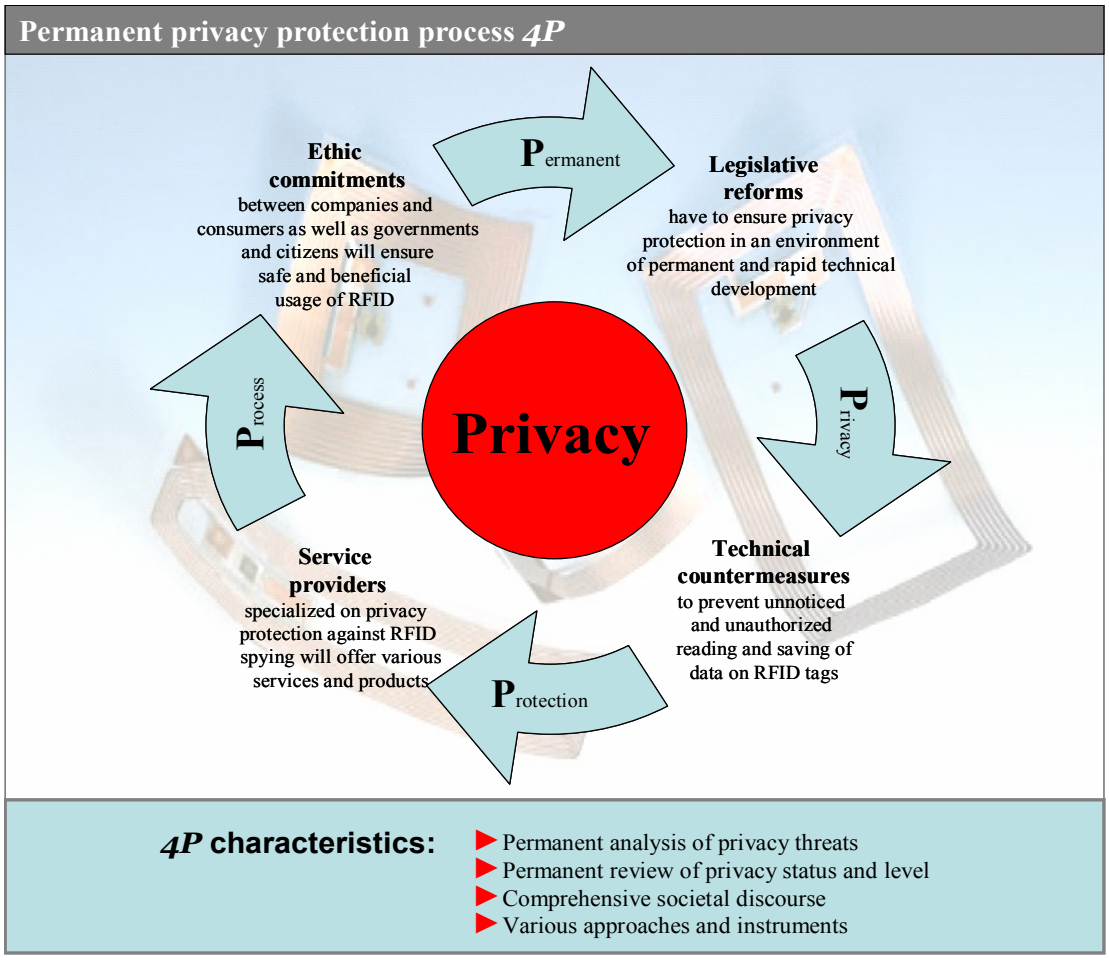
IWI Discussion Paper Series
11 (July 5, 2004)[1]

ISSN 1612-3646

Privacy Protection against RFID Spying: Challenges and Countermeasures[2]

Marcel Heese[3], **Günter Wohlers**[4] und **Michael H. Breitner**[5]



---

[1] Copies or a PDF-file are available upon request: Institut für Wirtschaftsinformatik, Universität Hannover, Königsworther Platz 1, D-30167 Hannover, Germany (www.iwi.uni-hannover.de).

[2] Paper submitted to the „7. Internationale Tagung Wirtschaftsinformatik 2005", Bamberg, February 23 – 25, 2005, see http://www.wi2005.de.

[3] Graduate Student (marcel.heese@web.de).

[4] Senior Lecturer (wohlers@iwi.uni-hannover.de).

[5] Full Professor for Information Systems Research and Business Administration (breitner@iwi.uni-hannover.de).

Table of contents

Privacy Protection against Ubiquitous RFID Spying: Challenges and Countermeasures

Marcel Heese, Günter Wohlers, Michael H. Breitner
University of Hannover

Abstract: The privacy threats of Radio Frequency Identification (RFID) as inevitable ubiquitous computing technology require new approaches to avoid scenarios as the "Orwell 1984 State" or the "transparent citizen". This paper introduces a new comprehensive approach: A permanent privacy protection process named "4P" or also "Fo(u)r P(rivacy)", here. The process 4P consists in a holistic societal discourse including individuals as well as business and government. Beyond technical countermeasures, specialized service providers will gain in importance. RFID using companies may be forced to establish ethic commitments and the legislative is supposed to protect privacy by law adapting technological developments.

Keywords: Radio Frequency Identification, RFID, privacy protection, ubiquitous computing, pervasive computing

1 Introduction

Headlines as "Bugging operation on cereals" or "Your products are watching you" are descriptive statements of many international consumer and privacy protection organizations. Privacy threats can result from the widespread usage of RFID as ubiquitous computing technology. The 20th century was characterized by many economical crises and wars between nations. Will the diffusion of ubiquitous devices in our daily environment result in an informational war within the society of the 21st century? The battlefield of the 21st century could be the supermarket of our neighborhood.

After mainframe computing and personal computing, "ubiquitous computing" names the third wave in computing [Weis96] and stands for the actual trends of information processing. In 1991 M. Weiser had the vision of an invisible technology, embedded in the devices of our everyday life that would be able to remove annoyances from the daily routine. The technology should be used as means to an end, indistinguishable from the device itself, allowing the human to concentrate on the essential basics of his action [Weis91, pp. 66-75]. The industry adopted the

expression “pervasive computing” as a more pragmatic approach for the penetration of all branches with the omnipresent information processing already today, by using today’s technology of mobile computing [LangMat03]. Because of the fast developments in microelectronics, the internet and wireless technologies, a permanent presence of smallest, networked computers in our “everyday devices” is likely in a short term. These “smart devices”, also called “things that think (3T)”, can autonomously share information, have access to resources in the internet and can operate adapted to their environment [Mat+03].

In this paper we discuss the characteristics and applications of RFID as ubiquitous computing technology and we evaluate privacy offenses, violations and intrusions. RFID allows the contact-less reading and writing of data stored on tiny tags. It will be used in various applications like product tracking in warehouses or logistic chains, but could also be realized in passports and banknotes. Business sees a high potential of efficiency increase by closing the gap between reality and information processing. That will make RFID an inevitable bulk commodity and will anchor it in our everyday devices. International consumer and privacy protection organizations raise an alarm and proclaim ubiquitous RFID will have direct impact on privacy. Without considerations of data and information security RFID will offer a perfect surveillance infrastructure. Approaching are, e. g., the scenarios of the “transparent consumer” in retail trade [MeySchü04] and a state creating complete movement schemes of its citizens. The latter may be provoked by the evident threads of today’s global terrorism including massive assaults with ABC-weapons.

A new comprehensive approach is necessary to decrease these technological dangers: A permanent privacy protection process named “4P” or also “Fo(u)r P(rivacy)”, here. 4P includes a holistic societal discourse including individuals as well as business and government. Beyond technical countermeasures, specialized service providers will gain in importance. RFID using companies may be forced to establish ethic commitments and the legislative is supposed to protect privacy by law adapting technological developments. 4P is characterized by a permanent analysis of privacy threats, an execution of various and adequate countermeasures and a review of the privacy status and level.

2 RFID and privacy

2.1 Function and technology of RFID systems

RFID is a technology for the contact-less reading and writing of data. It is used in automated identification applications that can provide information systems with the identity of a physical object. RFID describes a whole technological infrastructure including the RFID tag, a read/write device and the integration with servers, services or other systems, for example payment or resource planning systems [Fi02, p.7; FarShe03, p. 8].

Active vs. passive RFID tags

		Active RFID	Passive RFID
Technical Description	**Tag Power Source**	Internal to Tag	Energy transferred from the reader via Radio Frequency
	Tag Battery	Yes	No
	Availability of Tag Power	Continuously	Only within field of reader
	Required Signal Strength for Reader to Tag	Low or 0 (undetectable reader)	High (must power the tag)
	Required Signal Strength from Tag to Reader	High	Low
	Lifetime	Depending on the battery, 10 years maximum	Theoretically unlimited lifetime
Functionality	**Communication Range**	Long (up to about 100m)	Short (up to about 3m)
	Tag Collection while Moving	Tags moving at more than 150 km/h	Tags moving at 5 km/h or slower
	Sensor Capability	Ability to continuously monitor and record sensor input	Ability to read and transfer sensor values only when tag is powered by reader
	Data Storage	Large read/write data storage	Small read/write data storage
	Typical Applications	Cars: Tall collect, parking	Item tracking in supply chains and retail trade
	Costs	**High, about 100 Euro/Tag**	**Low, less than 0,1 Euro/Tag**

Table 1: Active vs. Passive RFID Tags, in parts adapted from [AutoID02]

The information is stored on the RFID tag and can be read out by the reader via radio waves. The tag itself consists in general of an antenna and a microchip, but can have various designs and sizes. The most important differentiation is between active and passive tags. Active tags bear their own energy source against what passive tags receive their energy form the emitted radio waves of the reader [Jul+04]. Most of the capabilities of an RFID system like costs, range, storage capacity and the integration of sensors depend on whether active or passive tags are used [AutoID02].

The memory of the RFID tag is in most of the cases used to store a globally unique identifier also called electronic product code (EPC). This allows a worldwide identification of for instance products that are labeled with a RFID tag. As a result of these characteristics, applications of ubiquitous RFID systems arise in many different fields [Fi02; FarShe03, p. 9].

2.2 Applications of RFID in an ubiquitous computing environment

Generally ubiquitous computing applications focus not only on business-to-consumer applications like the “smart toaster”, but also on business-to-business scenarios like the further integration of business information processing [FleiDi03, p. 611-612]. The potential benefits are new services and products and an opera-

tional increase in efficiency [Flei+03, p. 1]. Most important for the increase in efficiency is the reduction of media brakes in information processing. That happens by closing the gap between information systems and reality [Flei+03, p. 11] and the resulting simplified access to information [Flei+03, p. 6].

RFID as ubiquitous computing technology allows realizing many of the visionary ubiquitous computing applications already today. Beyond the most important fields supply chain management and retail trade [Fi02, p. 1; KräKad03], RFID gains importance in safeguarding banknotes and international passports. The main task of RFID is the supply with information on persons and goods [Fi02, p. 1]. Because of the high variety of applications it is just possible to give an overview on a small selection, which is related to privacy concerns later in this paper:

- **Logistic chains, warehouses and retailers:** Various companies plan to use RFID systems in their logistic chains and warehouses to track products on their way from the factory into the shops [AutoID03]. Inside the shops all shelves will be automatically monitored for expired products and adequate fill levels. This will connect the commodity flows directly with the information systems and leads to an increase of efficiency. Additionally the consumer will benefit from a quicker payment, because he can move his shopping cart just through the reader and all products are detected and automatically charged from his credit card [FarShe03; Krä02, pp. 106-114].
- **Banknotes:** RFID Tags will become embedded in high banknotes. This prevents counterfeiting and makes it easier to follow money in illegal transactions. Further the RFID tag's ability to read and write information makes it very difficult, for example, for kidnappers to ask for unmarked bills [Yosh01; Ha03;].
- **Passports:** International passports will have an embedded RFID tag that allows the storage of the owner's biometrical data. With a capacity of 32 or 64 kilo byte it is possible to store the raw data of the owner's face, fingerprints and a personal description [Rob03b].
- **Public transportation:** RFID could be an instrument to solve the deficit situation in many country's public transportation systems. The usage of contact-less RFID cards as tickets could increase efficiency in payment and control against misuse. The customers can pre-pay the RFID card and will automatically be charged by use. The cities Tokyo[1] and Soul already use these kinds of payment systems [Fi02, p. 355-366].
- **Washable tags in clothes:** Tags could be used for the identification of working clothes or costumes in factories or theatres. For instance that would help workers to find their clothes after laundry [MeySchü04].

[1] http://www.eurotechnology.com/store/suica/index_nl.html.

- **Car tires:** Michelin considers the usage of RFID tags in car tires to enable them to be tracked automatically. That could increase supply chain efficiency for car manufacturers as well as allow fast call-backs in case there are production errors. Philips introduced RFID tags to continuously measure tire pressure [Rob03a].

2.3 Privacy

One concept of privacy was first defined in 1890 by Samuel D. Warren and the later American supreme court judge Louis Brandeis in the article "The right to privacy" as the "individual's right to be left alone" [WaBra90]. Similar to today's discussions the authors expected privacy threats to arise from the technological developments of that time. However, the challenges of today's information age demand a wider understanding of the topic. Privacy is the active right to decide which information about one to be used by others and which information should affect oneself [Kuh99, p. 262]. The international law considers the right to privacy even in the human rights declaration.[2] New technologies have always been an influencing factor to privacy by offering new possibilities of surveillance and counter-surveillance [Rot99]. For each case, that demands an adapted approach for privacy protection. This paper will introduce a comprehensive approach that targets on preserving the control of privacy related information use at each individual itself.

3 Ubiquitous computing: Arrangement with the inevitable

3.1 Inevitable RFID Ubiquity

The widespread of ubiquitous computing and of RFID as technology of ubiquitous computing is inevitable [Mat+03; KräKad03, p. 8]. Driving forces are the fast development of the technological basis and the potential of ubiquitous RFID applications.

Hardware trends are characterized by miniaturization and a further fall in prices, still following Moore's law.[3] In addition, there is a permanent advancement of software in terms of mobile applications and global standards [Flei+03, p. 2]. The fast and contact-free identification and gathering of data from many RFID tagged items at the same time drive companies as well as governmental organizations to

[2] The "Universal Declaration of Human Rights" was passed by the United Nations in 1948. http://www.un.org/Overview/rights.html.

[3] ftp://download.intel.com/research/silicon/moorespaper.pdf.

see a big potential for business and security applications. Under these circumstances, RFID has good chances to become a bulk commodity [KräKad03, p. 7].

International market leaders in industry and retail trade like Metro, Procter & Gamble, Kraft or Gillette continuously promote the change from barcode to RFID. Wall Mart and the American ministry of defense require their suppliers to tag their pallets and product cases from 2006. Many other international retailers have similar plans on the way [AutoID03; Pf01, p. 12].

Business Consultants predict that the retail trade could reduce its personnel expenses at 10% and its warehouse charges at 5% by an improvement in logistics with the implementation of RFID. Further, the improved availability of products in the shop's warehouses and shelves would increase yearly profit by another 70 million euro per billion euro sales.[4]

From business consultant's point of view the estimated market volume of RFID technology will increase within the EU from 385 million Euro in 2004 to approximately 2,6 billions Euro in 2008.[5] An RFID manufacturer expects to increase his sales from under 1 billions tags in 2004 to about 20 billions tags per year in 2008 [MeySchü04]. That leads the RFID market to the fastest growing part of radio industries, including mobile phones, and will lead to a significant decrease of prices [Fi02, p. 2; Krem04].

3.2 RFID threats against privacy

For some time the internet was seen as eroding individual privacy [MeBr02, pp. 3-4]. Today, many of the various ubiquitous RFID applications awake similar concerns of international privacy and consumer protection organizations. These concerns are based on the characteristics of the RFID technology, and lead critics to describe them as "attempt at a violent penetration of our everyday life" [Ara95]. Also the scientific literature sees "the potential to create an invisible and comprehensive surveillance network."[Mat+03, p. 9] arising with the widespread use of ubiquitous computing networks in the daily business- and private life. The privacy relevant technical characteristics are described in the following:

- **Hidden RFID tags:** The tags are very tiny and can be integrated into various products and items, so that it is very difficult for the owner even to know, if there is an RFID tag in the product he just bought or not [Alb02].
- **Unnoticed readout**: The information stored on RFID tags can be read or modified from the distance, without line of sight between reader and tag. This can happen without knowledge of the tag's owner [FoeBuD04a, p. 2; Casp04].

[4] The management consultancy A.T. Kearny offers a study analyzing the impact of RFID on German manufacturers and retail trade. http://www.atkearney.de.

[5] The company Soreon Research offers a study analyzing the development of European RFID market. http://www.soreon.de.

International overview: RFID privacy protection organizations

Name	Country	Website	Aims / Activities
C.A.S.P.I.A.N. Consumers Against Supermarket Privacy Invasion and Numbering	USA	http://www.nocards.org http://www.spychips.com	•Fight against consumer spying in retail shops •Offer information on RFID privacy risks •Boycott of Gillette for employing RFID tags •Draft of legal regulations, RFID right to know act 2003
European Digital Rights	Europe	http://www.edri.org/	•Roof association for European privacy and civil rights •Defense of civil rights in the information society
FoeBuD e.V.: Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.	Germany	www.foebud.org www.bigbrotherawards.de	•No unregulated RFID implementations •Stop tests with RFID tags embedded in consumer products •Awarding the „Big Brother" award to Metro •Demonstration against RFID •Offer information on RFID privacy risks •Development of Data Privatizer as countermeasure
VIBE!AT: Austrian Association for Internet Users	Austria	http://www.vibe.at	•Encourage for the responsible use of internet applications •Offer information on RFID privacy risks
Spy.org.uk	United Kingdom	http://www.spy.org.uk	•Offer information on RFID privacy risks
Junkbusters Corp.	USA	http://www.junkbusters.com	•Fight against junk mail •Offer information on privacy in general •Offer information on RFID privacy risks
Privacy International	UK, USA	http://www.privacyinternational.org	•Publication of an international privacy survey
EPIC: Electronic Privacy Information Center	USA	http://www.epic.org	•Public interest research center •Offer information on RFID privacy risks
Electronic Frontiers	Australia	http://www.efa.org.au/	•Protecting and promoting online civil-liberties
Privacy Rights Clearinghouse	USA	http://www.privacyrights.org/	•Providing information and practical tips on consumers privacy protection

Table 2: International overview: RFID privacy protection organizations

- **Electronic Product Code (EPC):** Each RFID tag contains the electronic product code, which is a globally unique identification number. The EPC will displace the currently used barcode and will become the most important identification solution for every product in future [FarShe03, pp. 1-11].

The above described characteristics of RFID systems allow imagining various scenarios that would endanger privacy.

- **Re-identification and tracking:** Any organization could use the absent awareness for the RFID tag and the possibility to read the tag unnoticeably for tracking and re-identifying people [FoeBuD04a, p. 2; Ju03; Alb+03].
- **Surveillance:** Anybody with a reader device can read RFID tags from distance, trough wallets, clothes or bags, without being in line of sight with the tag and without knowledge of the owner [Casp04]. Reader devices attachable to an ordinary PDA are already available today.[6] A pickpocket could use a mobile reader to scan the items in the bag of his victim to decide whether it is worse to commit the crime or not. As described in the chapter RFID applica-

[6] http://www.omroneurope.com.

tions, the European central bank is considering the embedding of RFID tags into high value currency notes. That would allow the pickpocket even to evaluate in advance, how much money he might earn with his next victim.

- **Creating of individual profiles:** If identification data of anybody is linked to the EPC of an RFID tag, it will be possible to create movement profiles of individuals, without the individual's knowledge and consent. That could cause difficulties for the future moving in public anonymously. For instance, marketers could be interested to use RFID to explore the individual buying habits of their customers [Alb+03]. If scanning a credit- or payback card at the same time with any RFID items, it is possible to create records of exact movement profiles in a shop and use it to send customized advertisements to the customer afterwards [Casp04; FoeBuD04b; Rob04]. The case of embedding RFID tags into customer cards in the Metro chain without consent or knowledge of the consumers shows that such kind of scenario could become reality very soon.
- **Bugging:** Non-involved persons could bug the communication between reader and tag. The reader sends information back to the tag with a much higher range than the tag to the reader [Lang04]. Especially with the use of RFID in passports or credit cards this becomes a serious danger for privacy. Even so decryption is used, that doesn't make it absolutely save. Every code can be saved and cracked a posteriori.

4 Countermeasures

4.1 A comprehensive approach

This chapter introduces a new approach to counter the above-described privacy threats of ubiquitous RFID technology: The "permanent privacy protection process 4P". A successful protection of privacy can only be achieved with a comprehensive concept that includes an overall societal discourse. Involved must be various societal institutions like governments, business and individuals. With countermeasures split in many different fields, a broad set of instruments stands against the penetration of everybody's privacy. Beyond laws, also technical instruments and specialized services as well as ethic commitments will be part of 4P. An important characteristic of 4P is the permanent analysis of upcoming privacy threats and the following comprehensive search for solutions. The timely execution of countermeasures can minimize the dangers caused by new technological developments and can ensure success on the long term.

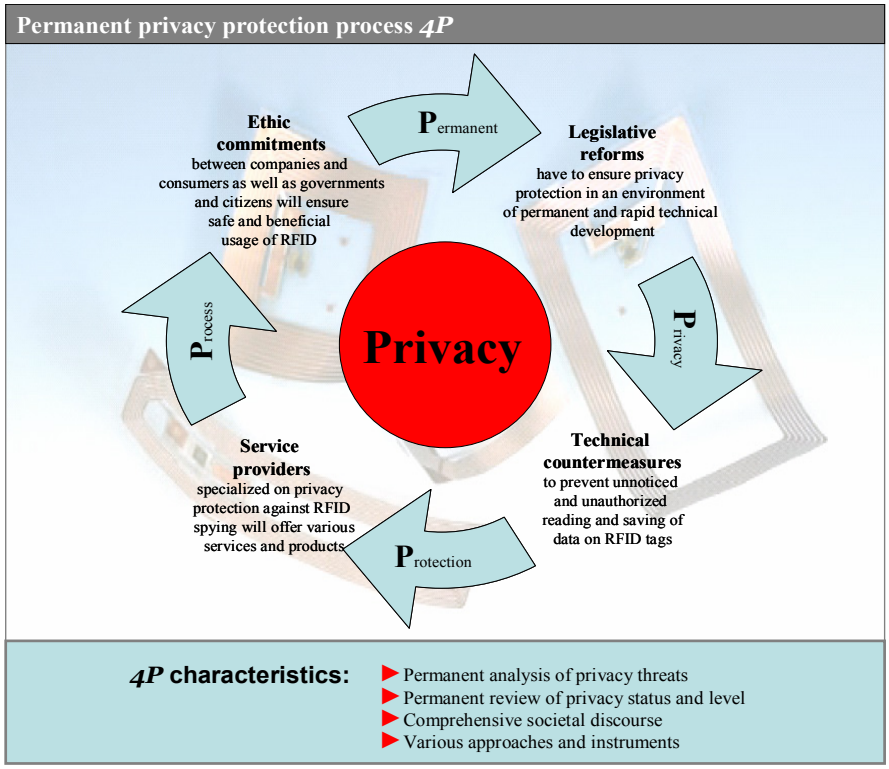


Figure 1: Permanent privacy protection process 4P

4.2 Technical options against RFID risks

The first step of 4P is to establish technical countermeasures against RFID spying. All technical countermeasures against RFID privacy threats have in common, that an unnoticed and unauthorized readout of RFID tags should be prevented [Lang04, p. 13]. Technical countermeasures can be split into measures to be taken by any individual or to be taken by the institutions that use RFID applications, in the majority of cases companies or governmental authorities.

Any individual should permanently analyze where his privacy might be endangered, for example while using the new introduced RFID customer card for public transportation payments or a RFID payback card for the daily shopping. After identifying privacy risks in different daily situations, various technical countermeasures adapted to the respective situation should be taken, for instance keeping the customer card in a special wallet that is not penetrable by radio waves:

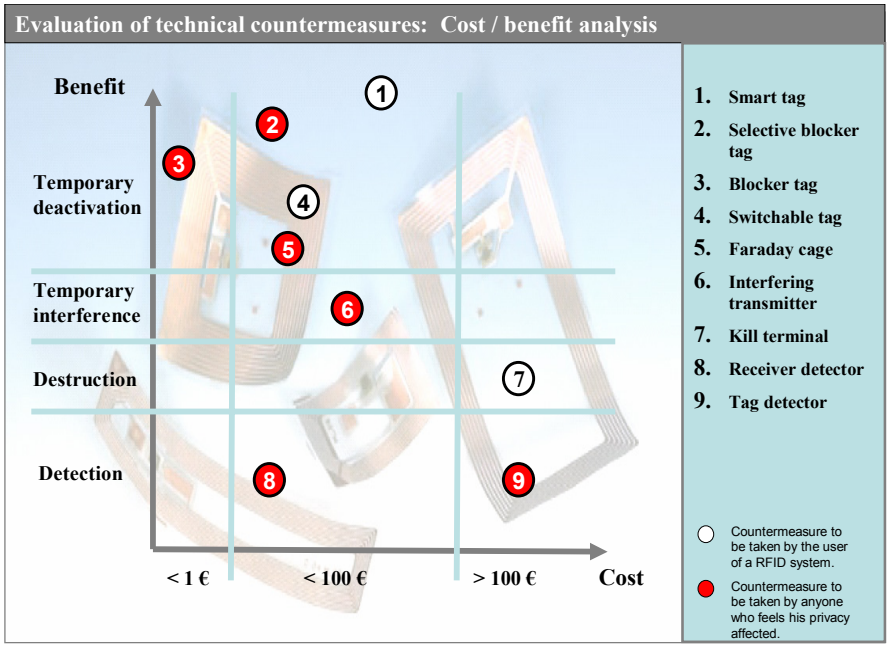


Figure 2: Evaluation of technical countermeasures: Cost / benefit analysis

- ***Blocker tag:*** The idea of blocker tags is not to disable ordinary RFID tags, but interfering with the data transmission between RFID tags and the receiver. The blocker tag can be placed in short distance to any RFID tagged items, for in a shopping bag. By simulating many ordinary RFID tags simultaneously, it is sending more data to the receiver than it can read. Through this it prevents the receiver from scanning the information transmitted by an ordinary tag [Jul+04].[7] Despite the advantages which are the easy use and low costs, consumer protection organizations criticize that the use of blocker tags would enforce the spread of RFID tags and they could be forbidden by law or by business policy of the retailers [Alb+03].[8]
- ***Selective blocker tag:*** Since a universal blocker tag can be counterproductive in an environment of many useful RFID systems, the selective blocker tag creates no disruption of RFID systems that are not relevant for privacy concerns, for instance inventory control. Instead, it creates a zone of privacy protection by blocking only a predetermined range of tag identification numbers. Similar

[7] The blocker tag is developed by RSA Security Inc. and the first prototype was presented on Cebit 2004. http://www.rsasecurity.com/rsalabs/node.asp?id=2060.

[8] The cost of blocker tags will be very low, because it is only slightly necessary to modify ordinary RFID tags, about 0,1€ [Jul+04].

to the universal blocker tag its costs are very low, because only slight modifications of ordinary tags are necessary to create selective blocker tags [Jul+04].

- ***Tag detector:*** The tag detector is a tool to detect any RFID tags in its environment. At present the detector is challenging to design, because today's RFID tags use various protocols and frequencies. Once international RFID standards are established it will become affordable. However, it does not give a solution for the proceeding after detecting RFID tags in anyone's everyday devices.[9]
- ***Receiver detector:*** A detector offers the possibility to detect RFID receivers for instance in supermarkets or shopping malls. A receiver that meets ISO 15693 standard, emits radio waves on 13,56 MHz. Passive RFID tags receive their energy form this electromagnetic field. The detector uses this electromagnetic field to track down a receiver. This technology will be a cheap way to detect RFID surveillance,[10] but it will not solve the privacy problem itself. The question is still what to do after detecting an RFID receiver.
- ***Faraday cage:*** The idea of a faraday cage is to shield the RFID tag from unwanted scanning by a receiver. A faraday cage could be a container or a bag made of metal mash or foil that is impenetrable by radio signals. An example of use is to put high-value-currency notes, which will be supplied with RFID tags in future [Ha03], into a foil-lined wallet to prevent other persons of scanning how much money is in one persons wallet [Jul+04]. Advantage of this technology is its easy use and the relative low costs. Nevertheless, there are limitations, because not all kind of RFID equipped items can be put into such a container, for example big size items.[11]
- ***Active Jammer:*** A jammer actively broadcasts radio waves that interfere with all receivers in its environment disabling them from scanning RFID tags. Beyond disabling also legitimate applications, where privacy is not a concern, it would cause even more electromagnetic pollution and may be illegal if the broadcast power is too high [Jul+04]. On the other hand, the costs for the transmitter would be low and it would be easy to construct and use.
- ***Microwave tagged item:*** Some privacy protection organizations suggest to microwave items that include RFID tags, for instance banknotes. In general, this solution will destroy next to the RFID tag also the item itself.

[9] The German privacy protection organization FoeBuD is developing a device called "Data Privatizer". Its function is to find hidden tags and read out the stored information. http://www.foebud.org.

[10] The c't magazine offers an construction plan to self construct a detector with material costs of about 15€ [BaAh04, p. 132].

[11] Some companies already offer bags that block signals form reaching wireless devices for about 30€. http://startsimple.com/mobilecloak/mobilecloak/index.html.

Evaluation of technical countermeasures

	Functionality	Advantages and disadvantages	Benefit and costs
Blocker tags	When placed close to a regular RFID tag, it prevents a receiver from scanning information transmitted by a tag by sending the receiver more data than it can read. Simulating many ordinary RFID tags simultaneously	Advantage: • easy to use Disadvantages: • could be prohibited by law • need to use the same data transfer protocol as receiver • have to be in short distance to tag	• temporary interference with all nearby RFID systems • low costs, less than 0,1 €
Selective blocker tags	Blocking only a restricted range of serial numbers.	Advantage: • interference only with specified RFID systems Disadvantages: • could be prohibited by law • need to use the same data transfer protocol as receiver • have to be in short distance to tag	• temporary interference with specified nearby RFID systems • low costs, less than 1 €
Detectors for RFID receivers	Detection of RFID sensors in supermarkets or shopping malls	Advantage: • relatively easy to construct and use Disadvantages: • short range • requires technical experience of consumers	• discovering of RFID receivers • self construction price approximately 15 € today
Detectors for RFID tags	Detection of RFID tags in any products or items	Advantage: • easy to use Disadvantage: • what is to do after identifying a tag in your shoes?	• discovering of RFID tags • self construction price approximately 15 € today
Kill tags	Tags designed to self destruct after receiving an 8 bit password. That should happen before they are placed in the hands of consumers.	Advantage: • the consumer doesn't have to fear RFID spying after leaving the shop Disadvantages: • the consumer cannot verify the tag is really deactivated • stores can't rescan if product is returned by customer • consumers can't use tags at home anymore (orgnizing baseball card's collection, microwave that can read cooking instructions)	• RFID tags will be deactivated when leaving the shop • costs below 1 €
Active jammer	Sending of radio signals interfering with receiver.	Advantage: • nearby RFID tags cannot be read Disadvantages: • it may be prohibited by law • it could cause damage to all nearby RFID systems, even to those in legitimate applications, where privacy is not a concern	• interfering all nearby RFID systems • cost approximately 20-30 € today
Destroying of tags before leaving the shop	Shop offers special machines which destroy the tags when leaving the shop.	Advantage: • deactivation of tags when leaving the shop Disadvantages: • offers no protection against observation inside the shop • customer has no evidence, that the tags are really destroyed • destroying of tags could be prohibited by law • line in front of chip killer?	• RFID tags will be deactivated when leaving the shop • cost approximately 100-500 € today
Data safety package "Faraday cage approach"	Storage of RFID tagged products in a special packing, that prevents receivers to read data from the tags. A container made of metal mash or foil that is impenetrable by radio signals.	Advantage: • prevents the reader from scanning the tag Disadvantages: • big products or clothes cannot be stored in a package • inconvenience for consumer	• prevents the reader from scanning the tag • cost approximately 30 € today
Smart RFID tags	Make RFID Tags smarter, so that they interact in a way that protects privacy better	Advantage: •RFID tag can only be read by a priori determined readers Disadvantage: •challenging to design	• tag cannot be read by any reader anymore • cost below 100 € today
Microwave items containing RFID tags	http://www.prisonplanet.com/022904rfidtagsexplode.html	Advantage: • chip will be destroyed Disadvantage: • chip may explode and start burning • tagged item could be destroyed	• no additional costs
Boycott	Boycott of non trustable companies and shops	Disadvantages: • boycott of few individuals does not have a big impact on company policy • individual becomes restricted in its consumption and life quality	• loss of quality of life

Table 3: Evaluation of technical countermeasures

Next to individuals, also some of the users of RFID applications will be interested to avoid an unauthorized spying against their customers or citizens. Especially companies are interested to preserve the trust of their consumers and governments have the duty to ensure privacy protection for their citizens. The RFID technology can be modified in different ways to prevent an unauthorized readout:

- ***Switchable tag:*** RFID tags can contain a switch for deactivation. After deactivation, the tags should not answer any signals from the reader. At the time a customer is leaving a shop, he will be asked if he wants to have the radio identification features of the RFID tags, embedded in the items he just bought, dis-

disabled. The proposed tag design of the AutoID Center is, that a tag can be switched off by sending it a "kill command" including an 8-bit password [Sar+02]. The kill command is part of the RFID protocol [Yosh03]. For reasons of cost efficiency in most of the cases the "kill command" will be only a software solution. That means the customer has no opportunity to check whether his RFID tags are really deactivated or not. Further, it would theoretically be possible to reactivate the tag later without knowledge of the customer. An electromagnetic deactivation would improve the switchable tag solution. However, even with deactivation at the counter, still a tracking inside the shop is possible [Lang04, p. 14].

- ***Smart RFID tag:*** The idea behind smart RFID tags is that only selected receiver should be able to read the information on the RFID tag. This can be realized by using cryptographic methods. Because of its complex design this will result in higher cost for the tag and limit its spread, since the budgets for RFID tags are very tight [Jul+04].
- ***Kill terminals:*** The user of a RFID system, for instance a retail trader, could offer a possibility to his customers to destroy the RFID tags on the purchased items physically before leaving the shop. But that would mean an additional effort for the customer. In addition small shops like kiosks probably cannot effort to buy expensive kill-terminals, even they get RFID tagged goods from the wholesale trader.

These countermeasures are effective solutions for various situations, but because of the expected widespread of RFID tags, they are not sufficient to encounter the privacy risks on the long term in a sustainable manner [Lang04]. Therefore, the RFID privacy protection process 4P has to be followed to its next steps.

4.3 Privacy service provider

In the age of ubiquitous information processing privacy becomes a limited good. Not everybody has guaranteed access to it. Such a scenario is the base for the development of business models that trade or protect the limited good privacy. Accordingly, the second step of 4P is to integrate professional service providers in protecting everybody's privacy. In the medium-term, modern privacy service providers will offer various products and services on the privacy market.

Already today, many companies work in the field of protecting the privacy of their clients in the internet. Offers reach from anonymous web surfing and anti-spam programs to spy-ware removers and ID-theft prevention.[12] These business ideas can be transferred to RFID privacy protection. When RFID networks become pre-

[12] Internet privacy providers: http://www.pcprivacycentral.com/; http://junkbusters.com; http://www.anonymizer.com/index.cgi; http://www.makemeinvisible.com/.

sent in the daily life of everybody, new services and products could be the following:

- **Information provider:** Similar to the German "Stiftung Warentest" who evaluates consumer products and sells the results, a RFID information provider will offer services that inform about how various "ubiquitous situations" endanger privacy, which commercial products and items contain RFID tags and how to encounter the privacy threats.
- **Counter devices merchant:** Various companies will arise who sell the technical counter devices described in 4.2. For example, blocker tags or faraday cage bags could be ordered in online shops specialized on privacy technology or even in regular shopping centers next to other electronic or home entertainment devices.
- **Exterminator:** Similar to the traditional vermin exterminator who comes out to houses or offices to find and expel annoying insects, the RFID exterminator will find and deactivate unwanted RFID tags for his clients.
- **Privacy Lawyer:** A RFID privacy lawyer will be specialized on RFID laws. If everybody feels unfairly treated concerning the use of RFID technology in his personal environment, the lawyer helps to fight for everybody's rights at courts.

Above was discussed what everybody can do against RFID privacy threats by himself and with the help of specialized service providers. However, 4P must be necessarily an overall societal discourse to be most effective. Therefore, the next steps involve the business world and the politics.

4.4 Ethic commitments

The third step of the permanent privacy protection process 4P is to pass ethic commitments between the parties that are affected by the use and the users of RFID technology. The commitments regulate how RFID technology and the collected information can be used. Since commitments mostly result from agreements between opponent parties, this may be an even more efficient and economic way to encounter RFID risks than the countermeasures described above. With an increase of transparency, the expenses for privacy countermeasures in general will decrease. Ethic commitments will be passed especially between companies and consumers, but also between governments and citizens.

Within today's information society public relations of companies as well as governmental organizations, become more and more important, since the new media allow fast and cheap information gathering for anybody. Public Relations are an instrument to establish trust and mutual understanding between an organization and its publics [Be01, p. 600]. The misuse of RFID technology will have a large negative impact on public relations of any company, once the society is sensitized

for the privacy topic. Examples for that can be found already today. Gillette was confronted with a worldwide call for boycott by the privacy protection organization CASPIAN[13] and the image to use "spy chips" will follow them for years. In a similar way, the Italian clothing manufacturer Benetton was forced to remove any RFID tags from their products [Hill04]. In addition, the German Metro Group, who used RFID customer cards for identifying customers wanting to view movie trailers in the metro future store, was forced to reject the RFID tags after being heavily criticized by press and privacy protection organizations for several weeks.[14] In the internet, companies must guarantee the privacy of their online customers. Otherwise the survival of the company is endangered on the long-term [MeBr02]. Similar rules will apply for RFID.

Ethic commitments, a group of rules and standards that voluntarily govern the use of RFID technology in the economic world, will avoid negative public relations for companies and create transparency and trust at the consumers. Analog to biological cultivated and produced groceries, RFID controlled products could increase in popularity in the same way. The commitments should contain similar principles as the later described RFID law, with the important difference that the commitment is agreed on a voluntarily base:

- Companies inform their customers that they use RFID technology that they can track and collect information about them;
- Customers have to express their consent before RFID can be used;
- RFID tags are destroyed before the customer leaves the shop.[15]

In situations were no commitments can be established, for instance if one party doesn't have the necessary natural interest or bargaining power, rules for the use of RFID have to be established by law.

4.5 Protection by law

Elementary considerations of a new data security law are necessary to avoid the way to an "Orwell 1984 State" [Mat01, pp. 8-9]. The above-described privacy concerns against the usage of ubiquitous RFID applications are resulting in clear demands of the privacy protection as well as IT organizations on juridical regulations [GfI04]. Most of the international privacy protection organizations signed the "RFID right to know act of 2003" [Casp03] outlining their requirements for laws regulating the widespread use of RFID systems. The legislative has to escort the technical development at an early stage to prevent abuse [GfI04] and to assure

[13] CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering). http://www.spychips.org ; http://www.nocards.org.
[14] http://www.computerweekly.com/Article128846.htm.
[15] http://www.out-law.com/php/page.php?page_id=rfidprivacyconcern1077793996.

its beneficial use "without simply allowing a blanket ability to track people" [Rob04]. The main ideas for RFID laws as part of a comprehensive privacy protection process are introduced in the following:

- **Labeling of products with embedded tags:** If companies use RFID systems beyond internal supply chains in consumer products, these products must bear a label stating that the item contains a RFID tag and that the tag can transmit a unique identification to any reader before and after sales. The label should be in a conspicuous type and size and in a prominent location on the item. Further, the label should be in print that contrasts with its background [Casp03; Bec04, p. 3]. If the tag is inseparable and invisible connected to the item, its position must be marked [Bec04, p. 3].
- **Ownership:** The consumer who buys a product also becomes owner of the tag and the data stored on it. He must have access to all data stored on the tag. The consumer has the right to demand deactivation or removal of the tag given at no charge [Bec04, p. 3].
- **Information for the consumer:** Every company must inform the consumer in advance, why and where his data will be used and which data will be stored in a database [Bec04, p. 3].
- **Linking and disclosing consumer data:** It must be forbidden to link individual's personal data with the unique identification information contained in the RFID tag [Casp03]. Further, it must be forbidden to disclose an individual's personal data to third parties in association with RFID tag identification information [Casp03].
- **Identifying individuals:** It must be forbidden to use RFID gained information to identify individuals directly, or through third parties [Casp03].
- **Treatment of non-RFID products:** Every company should offer all services at the same conditions for RFID marked products and non-RFID marked products. Guarantee claims have to be fulfilled independent from the function of the tag [Bec04, p. 3].
- A **federal authority** should establish security guidelines to ensure the confidentiality of individual's records, to ensure that records do not identify individuals and to ensure that the individual is protected.
- **Violations:** Violations against the rules resulting from RFID laws must be penalized [Casp03].

After introducing the theory of future RFID laws, the actual state of privacy regulations shall be addressed.

Europe uses traditionally more extensive and general privacy laws against what the USA lean on voluntary self-control and on specific laws. Europe has guidelines for private and public databases, the "Agreement for the Protection of Individuals Against Automatic Information Processing" and finally the European Privacy Directive from 1995. The Organization for Economic Co-operation and De-

velopment (OECD) published the "Fair Information Practices" in the beginning of the 80ies. They most important principles can be summarized as follows: data quality, use limitation, purpose specification, and individual participation [Lang04, pp. 3-13; OEC80]. The international RFID privacy conference 2003 published a resolution that generally says these privacy regulations have to be applied as well to RFID applications [ICDP03].

In contrast to that, the USA is gone furthest on the way to a specific RFID privacy law so far. In several states, for example California and Utah, concrete RFID laws are discussed in the senate or already passed. The main intention in the discussion is not to ban the RFID technology or to limit its potential positive uses for the companies, but definitely to protect consumer privacy [Rob04]. The laws of California require companies and governmental agencies to inform consumers whenever RFID systems are used. The companies must obtain consumer's consent before they can use RFID to track purchases and collect information about them. Also it requires the RFID tag to be detached or destroyed before consumers leave the shop with it [Rob04; Gil04]. Introduced to the senate in February 2004 by Senator Debra Bowen, the "bill 1834" passed the senate with 22:8 majorities in May. Next steps will be the decision of California's parliament about the bill in June. [16] Utah's House of Representatives passed the first RFID privacy law in February 2004 and the law will take effect from May 2005. It requires all products containing RFID tags to be labeled as such.[17]

5 Conclusions and outlook

The discussion of this paper clearly shows that it is too early to accept the scenarios of the "transparent citizen" or the "Orwell 1984 state" as inevitable. The "information war" can be controlled by a comprehensive societal discourse supported by privacy protection processes. A permanent evaluation of upcoming privacy threats and the timely execution of countermeasures will minimize the impacts caused by new technological developments. Various societal institutions like governments, business and individuals must be involved. With various countermeasures split in different fields, a broad set of instruments against the penetration of everybody's privacy is available today. Besides acts and laws also technical instruments and specialized services as well as ethic commitments can be part of a permanent privacy protection process, e. g. 4P presented here. 4P allows companies and governments, e. g., to realize efficiency increases and launch new products without threatening privacy.

[16] Download the RFID bill of California: http://www.leginfo.ca.gov/pub/bill/sen/sb_1801-1850/sb_1834_bill_20040220_introduced.pdf.

[17] Download the RFID Right to Know Act of Utah: http://www.le.state.ut.us/~2004/bills/hbillamd/hb0251.pdf.

References:

[Alb+03] Albrecht, K.; McIntyre, L.; Givens, B., et al.: RFID Position Statement of Consumer Privacy and Civil Liberties Organizations. http://www.privacyrights.org/ar/RFIDposition.htm, 2003, Download 2004-04-25.

[Alb02] Albrecht, K.: RFID: Tracking everything, everywhere. http://www.spychips.org/rfid_overview.htm#24, 2002, Download 2004-05-19.

[Ara95] Araya, A. A.: Questioning Ubiquitous Computing. In: Proceedings of the 1995 ACM 23rd Annual Conference on Computer Science. http://portal.acm.org/citation.cfm?id=259560&dl=ACM&coll=portal, 1995, Download 2004-05-19.

[AutoID02] AutoID.org: Active and Passive RFID : Two Distinct, But Complementary, Technologies for Real-Time Supply Chain Visibility. http://www.autoid.org/2002_Documents/sc31_wg4/docs_501-520/520_18000-7_WhitePaper.pdf, 2002, Download 2004-05-26.

[AutoID03] AutoID Center: WallMart details RFID requirements. http://www.autoidcenter.cn/news/viewNews.asp?newsID=%2056, 2003, Download 2004-06-15.

[BaAh04] Bartels, O.; Ahlers, E.: Gegenspionage: RFID - Detektor im Taschenformat. In: c't 2004, (9), p. 132.

[Be01] Becker, J.: Marketing-Konzeption. 7. Auflage. Vahlen: München, 2001.

[Bec04] Beck, A.: RFID-Verfassung. http://www.pruefziffernberechnung.de/Attraktor/Atraktor_2004_02.pdf, 2004, Download 2004-05-19.

[Casp03] CASPIAN: RFID Right to Know Act of 2003. http://www.spychips.com/press releases/right-to-know-ill.htm, 2003, Download 2004-05-19.

[Casp04] CASPIAN: What is RFID. http://www.spychips.org/what-is-rfid.html, 2004, Download 2004-05-19.

[FarShe03] McFarlane, D. C.; Sheffi, Y.: The Impact of Automatic Identification on Supply Chain Operations. University of Cambridge: Cambridge, 2003.

[Fi02] Finkenzeller, K.: RFID-Handbuch: Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten. 3. Auflage. Hanser: München et al., 2002.

[Flei+03] Fleisch, E.; Mattern, F., Billinger, S.: Betriebswirtschaftliche Applikationen des Ubiquitous Computing. http://www.vs.inf.ethz.ch/publ/papers/BW_ApplUbicomp.pdf, 2003, Download 2004-06-14.

[FleiDi03] Fleisch, E.; Dierkes, M.: Ubiquitous Computing aus betriebswirtschaftlicher Sicht. In: Wirtschaftsinformatik, 2003, (6), pp. 611-620.

[FoeBuD04a] FoeBuD: Positionspapier über den Gebrauch von RFID auf und in Konsumgütern. http://www.foebud.org/texte/aktion/rfid/positionspapier.html, 2004, Download 2004-05-26.

[FoeBuD04b] FoeBuD: FoeBuD unveils: Hidden spychips cover-up of Metro-Group's "Payback" customer cards. http://www.foebud.org/texte/aktion/rfid/pe-gb.html, 2004, Download 2004-05-19.

[GfI04] Gesellschaft für Informatik: Sachverständige der Gesellschaft für Informatik warnen vor möglicher Überwachung der Bevölkerung durch RFID-Chips. http://www.gi-ev.de/informatik/presse/index-presse-aktuell.html, 2004, Download 2004-06-15.

[Gil04] Gilbert, A.: California Lawmaker introduces RFID bill. http://news.com.com/2100-1014-5164457.html, 2004, Download 2004-05-14.

[Ha03] Handelsblatt: Chip soll Euro sicher machen. http://www.handelsblatt.com/hbiwwwangebot/fn/relhbi/sfn/buildhbi/cn/GoArt!200104,201197,631871/SH/0/depot/0/index.html, 2003, Download 2004-05-14.

[Hill04] Hillenbrand, T.: Der Feind in meinem Schuh. http://www.spiegel.de/wirtschaft/0,1518,262774,00.html, 2004, Download 2004-06-14.

[ICDP03] International Conference Of Data Protection & Privacy Commissioners: Resolution On Radio-Frequency Identification. http://www.privacyconference2003.org/commissioners.asp, 2003, Download 2004-06-15.

[Ju03] Junkbusters Corporation: RFID Devices and Privacy. http://www.junkbusters.com/rfid.html, 2003, Download 2004-05-19.

[Jul+04] Jules, A.; Rivest, R. L.; Szydlo, M.: The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy. http://www.seas.upenn.edu/~msherr/presentations/blocker_tags.pdf, 2004, Download 2004-05-10.

[Krä02] Krämer, K.: Automatisierung in Materialfluß und Logistik – Ebenen, Informationslogistik, Identifikationssysteme, intelligente Geräte. 1. Auflage. Deutscher Universitätsverlag: Wiesbaden, 2002.

[KräKad03] Krämer, W.; Kadner, C.: Investment Perspective IV/2003. Trend-Monitor R.F.I.D.. http://www.lazardnet.com/lam/de/pdfs/Inv_Perspective_0104.pdf, 2003, Download 2004-06-15.

[Krem04] Krempl, S.: Das Internet der Dinge. http://viadrina.euv-frankfurt-o.de/~sk/Pub/rfid-cw04.html, 2004, Dowload 2004-06-15.

[Kuh99] Kuhlen, R.: Die Konsequenzen von Informationsassistenten. http://www.inf-wiss.uni-konstanz.de/People/RK/Publikationen1995-2000/informationsassistenten.pdf, 1999, Download 2004-05-19.

[Lang04] Langheinrich, M.: Die Privatsphäre im Ubiquitous Computing: Datenschutzaspekte der RFID Technologie. http://www.vs.inf.ethz.ch/publ/papers/langhein2004rfid.pdf, 2004, Download 2004-06-15.

[LangMat03] Langheinrich, M.; Mattern, F.: Digitalisierung des Alltags: Was ist pervasive computing? http://www.bpb.de/publikationen/48VKPV,1,0,Digitalisierung_des_Alltags.html#art1, 2003, Download 2004-05-19.

[Mat+03] Bohn, J.; Coroama, V.; Langheinrich, M.; Mattern, F.; Rohs, M. (2003): Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. http://www.vs.inf.ethz.ch/publ/papers/socialambient.pdf, 2003, Download 2004-05-19.

[Mat01] Mattern, F.: Allgegenwärtigkeit des Computers, in: 5. Berliner Colloquium der Gottlieb Daimler- und Karl Benz Stiftung. http://www.daimler-benz-stiftung.de/home/service/press_releases/de/statements_bk5.pdf, 2001, Download 2004-05-19.

[MeBr02] Merkow, M. S.; Breithaupt, J.: The E-Privacy Imperative. Protect Your Consumers' Internet Privacy and Ensure Your Company's Survival in the Electronic Age. American Management Association: New York et al., 2002.

[MeySchü04] Meyer, A., Schüler, P.: Mitteilsame Etiketten. In: c't 2004, (9), pp. 122-129.

[OEC80] Organization for Economic Co-operation and Development (OECD): The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.datenschutz-berlin.de/gesetze/internat/bde.htm, 1980, Download 2004-06-15.

[Pf01] Pflaum, A. (2001): Transpondertechnologie und Supply-Chain Management. Deutscher Verkehrs-Verlag. Hamburg.

[Rob03a] Roberti, M.: Michelin Embeds RFID Tags in Tires. http://www.rfidjournal.com/article/articleview/269/1/1/, 2003, Download 2004-06-15.

[Rob03b] Roberti, M.: RFID solution secures passports. http://www.rfidjournal.com/article/articleview/522/1/1/, 2003, Download 2004-06-15.

[Rob04] Roberti, M.: Bowen seeks Balance in RFID law. http://www.rfidjournal.com/article/articleview/812/1/1/, 2004, Download 2004-04-25.

[Rot99] Rothenberg, M.: Privacy in the information society. http://www.unesco.org/webworld/infoethics_2/eng/papers/paper_10.rtf, 1999, Download 2004-05-19.

[Sar+02] Sarma, S. E.; Weis, S. A.; Engels, D. W. (2002): RFID Systems, Security & Privacy Implications. http://www.autoidlabs.com/whitepapers/MIT-AUTOID-WH-014.pdf, 2002, Download 2004-05-14.

[WaBra90] Warren, S. D.; Brandeis, L.: The Right to Privacy. In: Harvard Law Review. 1890-12-15. http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html, Download 2004-06-15.

[Weis91] Weiser, M.: The computer for the 21st century. In: Scientific American, 1991, (9), pp. 66-75.

[Weis96] Weiser, M.: Ubiquitous Computing. http://www.ubiq.com/hypertext/weiser/ UbiHome.html, 1996, Download 2004-05-19.

[Yosh01] Yoshida, J.: Euro Bank Notes to Embed RFID Chips by 2005. http://www.eetimes.com/story/OEG20011219S0016, 2001, Download 2004-06-15.

[Yosh03] Yoshida, J.: RFID backlash prompts "kill" feature. http://www.eetimes.com/story/OEG20030428S0074, 2003, Download 2004-05-14.

IWI Discussion Paper Series

ISSN 1612-3646

Michael H. Breitner, *Rufus Philip Isaacs and the Early Years of Differential Games*, 36 p., #1, January 22, 2003.

Gabriela Hoppe and Michael H. Breitner, *Classification and Sustainability Analysis of E-Learning Applications*, 26 p., # 2, February 13, 2003.

Tobias Brüggemann and Michael H. Breitner, *Preisvergleichsdienste: Alternative Konzepte und Geschäftsmodelle*, 22 p., # 3, February 14, 2003.

Patrick Bartels and Michael H. Breitner, *Automatic Extraction of Derivative Prices from Webpages using a Software Agent*, 32 p., # 4, May 20, 2003.

Michael H. Breitner and Oliver Kubertin, *WARRANT-PRO-2: A GUI-Software for Easy Evaluation, Design and Visualization of European Double-Barrier Options*, 35 p., #5, September 12, 2003.

Dorothée Bott, Gabriela Hoppe and Michael H. Breitner, *Nutzenanalyse im Rahmen der Evaluation von E-Learning Szenarien*, 14 p., #6, October 21, 2003.

Gabriela Hoppe and Michael H. Breitner, *Sustainable Business Models for E-Learning*, 20 p., #7, January 5, 2004.

Heiko Genath, Tobias Brüggemann and Michael H. Breitner, *Preisvergleichsdienste im internationalen Vergleich*, 40 p., #8, June 21, 2004.

Dennis Bode and Michael H. Breitner, *Neues digitales BOS-Netz für Deutschland: Analyse der Probleme und mögliche Betriebskonzepte*, 21 p., #9, July 5, 2004.

Caroline Neufert and Michael H. Breitner, *Mit Zertifizierungen in eine sicherere Informationsgesellschaft*, 19 p., #10, July 5, 2004.

Marcel Heese, Günter Wohlers and Michael H. Breitner, *Privacy Protection against RFID Spying: Challenges and Countermeasures*, 21 p., #11, July 5, 2004.