# Privacy Protection against Ubiquitous RFID Spying: Challenges, Countermeasures and Business Models

## Diplomarbeit

zur Erlangung des Grades eines Diplom-Ökonomen der

Wirtschaftswissenschaftlichen Fakultät der Universität Hannover

vorgelegt von


Name: Heese [redacted] Vorname: Marcel [redacted]


Erstprüfer: Prof. Dr. Michael H. Breitner

Hannover,
den 10. Dezember 2004

# Table of Contents

## Figures:



## Tables:

## Abbreviations:

| | |
|---|---|
| 4P | Permanent Privacy Protection Process |
| BDSG | Bundesdatenschutzgesetz |
| CPO | Chief Privacy Officer |
| CRM | Customer Relationship Management |
| EEPROM | Electronically Erasable Programmable Read Only Memory |
| EPC | Electronic Product Code |
| EU | European Union |
| FRAM | Ferromagnetic Random Access Memory |
| ICAO | International Civil Aviation Organization |
| ID | Identification |
| MIT | Massachusetts Institute of Technology |
| PEC | Privacy Enhancing Content |
| PES | Privacy Enhancing Service |
| PET | Privacy Enhancing Technology |
| RAW | Read And Write |
| RFID | Radio Frequency Identification |
| ROM | Read Only Memory |
| SBT | Selective Blocker Tag |
| SRAM | Static Random Access Memory |
| TKG | Telekommunikationsgesetz |
| UPC | Universal Product Code |
| US | United States |
| USA | United States of America |
| WORM | Write Once Read Many |

# 1 Introduction

## 1.1 Problem and Motivation

Headlines as „Bugging operation on cereals" or „Your products are watching you" are descriptive statements of many international consumer and privacy protection organizations. The 20th century was characterized by various 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 [Wei96] and stands for the actual trends of information processing and wireless computing technologies. In 1991 Michael 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 [Wei91, pp. 66-75]. The business world adopted the expression "pervasive computing" as a more pragmatic approach for the penetration of all branches with the omnipresent information processing and object-to-object communication already today, by using today's technology of mobile computing [LM03]. 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 on 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 [BCV+03, p. 3].

Radio Frequency Identification (RFID) is the technology to realize many ubiquitous computing applications already today. RFID allows the contact-less reading and writing of data stored on tiny tags. It will be used in various applications like item tracking in whole product lifecycles, but will also be realized in passports, banknotes, tickets and other objects of the daily life. 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.

On the one hand it allows companies or governmental organizations to optimize processes. One the other hand the new possibilities of data mining and the availability of data in global networks rise doubts that these developments lead to the end of the individual's privacy and are a big step in the direction of an "Orwell State". [1] In this case Moore's[2] law is on the side of governments and corporations that want to invade personal privacy. The speed of technological innovations continuously provides cheaper and stronger infrastructures to collect, transport, store and analyze personal data [Hsu03, pp. 9-13]. This necessitates comprehensive consideration to realize both: The protection of individual's privacy and the benefits of the new technology.

### 1.2 Goal and Approach

The goal of this paper is the presentation of ideas and considerations for a protection against "RFID spying". Essential for a successful protection of privacy is a comprehensive concept that includes an overall societal discourse. The discourse includes various instruments and institutions. Technical, legal and market driven instruments are executed by individuals as well as companies and governments. Furthermore, considerations are presented on how to implement these countermeasures and bring them to use for the individual. The rising demand for privacy protection opens new opportunities for business. The „RFID Privacy Space", as market for privacy protection, can develop strong growth in the future.

Chapter 2 depicts the characteristics and applications of RFID as ubiquitous computing technology and the resulting privacy threats. RFID's abilities of ubiquitous data collections allow imagining various privacy offenses, violations and intrusions. International consumer and privacy protection organizations raise an alarm and proclaim RFID's eroding impact on personal privacy. Without consideration of data and information security RFID offers a perfect surveillance infrastructure. Approaching are, e. g. the scenarios of the "transparent consumer" in retail trade [MS04, pp. 122-129] or the "Orwell State". The latter may be provoked by the evident

[1] George Orwell describes in his novel "1984" a totalitarian state, which has installed an all-embracing surveillance network to control the activities of his citizens [Orw49].

[2] Moore's law is the result of an empirical study from 1965, stating that the technological advances in the semiconductor industry, the complexity of integrated circuits doubles every 18 months [Moo65].

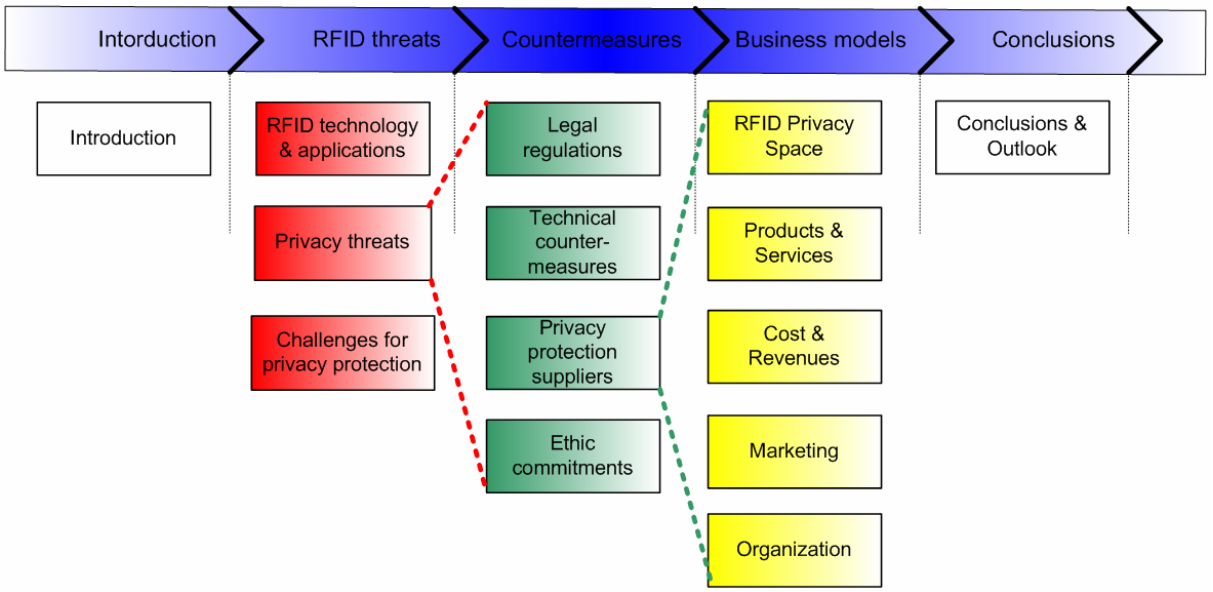


Figure 1: Approach; Source: Own illustration

threats of today's global terrorism, including massive assaults with ABC-weapons. Therefore the influence of RFID on the dimensions of privacy is analyzed.

Chapter 3 describes a comprehensive approach to encounter RFID's privacy threats: The permanent privacy protection process named "4P" or also "Fo(u)r P(rivacy)". 4P includes a holistic societal discourse including various instruments and institutions. Especially the legislation is supposed to protect privacy by regulations adapting technological developments. Minimum standards for privacy protection must be established, penalizing violations. The individual's awareness of privacy threats increases. Necessary is a self-dependent review of the individual's privacy status and level, then privacy enhancing technologies will enable everybody to do a "do it yourself" privacy protection. Beyond that, as a consequence of the RFID widespread, specialized privacy protection suppliers will gain in importance. Finally companies using RFID are forced to establish ethic commitments, demanded by market forces and the privacy awareness of their customers. The goal of 4P is ensuring privacy and enabling a beneficial use of RFID.

Chapter 4 concretizes business models for privacy protection suppliers. Entrepreneurs realize that the protection of privacy and new technologies are not strictly a contradiction. Privacy enhancing technologies (PETs), privacy enhancing services (PESs) and privacy enhancing contents (PECs) are the fields where specialized suppliers actively can support the individual's fight against privacy threats. The RFID Privacy Space, as a market for privacy protection products and

services, develops strong growth. Exemplary activity models executed by companies within the RFID Privacy Space are introduced. They are based on deconstruction of the RFID Privacy Space's value chain. Depending on the Privacy Space's characteristics, adapted approaches for the organization, marketing, costs and revenues are necessary for these companies.

# 2 Basic principles of ubiquitous RFID applications and privacy

## 2.1 Ubiquitous computing

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" [Wei91].

In 1991 Michael Weiser had the vision of an invisible technology, embedded in everyday objects, removing annoyances from the daily routine and allowing the human to concentrate on the essential basics of his action. Following his ideas, personnel computers and laptops based on silicon-technology are only an intermediate step on the way to achieving the real potential of information technology. So far, personal computers were in a world of their own, requiring complicated user interfaces and code languages that have nothing to do with the tasks they should fulfill.

Weiser sees the disappearance of computers not as a consequence of technological developments, but of the human psychology. Whenever humans learn something very well, they stop being aware of it. E.g., when seeing a street sign, its information is being absorbed, without being aware of the process "reading" itself. As soon as many small computers are placed in daily objects, able to communicate with each other, the disappearance will happen. The opposite of ubiquitous computing is the idea of virtual reality. Here the users enter the world of the computer with the help of special goggles, gloves or even body suits that sense their motions and project an artificial scene in front of their eyes. In ubiquitous computing instead the computer enters the world of the human and integrates itself invisibly.

The industry has already 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

protection organizations, which may impede the development of an RFID privacy protection supplier.

## 5 Conclusions and outlook

**Recapitulatory**, the previous discussion shows that the spread of ubiquitous computing applications exceeds today's possibilities of every-day-life surveillance and data mining. But the "information war" can be controlled by a comprehensive societal discourse supported by privacy protection processes and specialized business models.

A permanent evaluation of upcoming privacy threats and the timely execution of countermeasures minimize the impacts caused by a surveillance-scenario of wide spread RFID applications. Various societal institutions like governments, businesses and individuals are involved. With various countermeasures split in different fields, a broad set of instruments against the penetration of everybody's privacy is available. Besides acts and laws privacy enhancing technologies, services and contents as well as ethic commitments are part of a permanent privacy protection process, e. g. 4P presented here.

The individual's demand for privacy protection opens a new business sector, the RFID Privacy-Space. RFID privacy protection suppliers fulfill various activities based on the RFID privacy value chain. From a **critical** point of view, the internet has shown that a commercial support of privacy protection is associated with some difficulties, but can be successful. Similar basic conditions apply to RFID privacy protection suppliers. The RFID Privacy-Space is characterized by uncertainties regarding the market growth, heterogeneous structures of competitors, or the low willingness to pay for privacy protection. It is necessary to achieve a change in everybody's behavior towards privacy.

Characteristic for **future** challenges of privacy protection is an increasing speed of development in data processing and communication networks. More and more integrated into the daily life, accompanying everybody's actions invisibly and without the individual's awareness, these technologies follow Weiser's vision of ubiquitous computing. The borders between the real and the virtual world become more and

indistinguishable, caused through the reduction of media breaks. The representation and manipulation of the real world out of the virtual world becomes more precise and easy. The outcome of this is the demand for advanced privacy protection.

Therefore, it will become more and more important that governments follow technical developments carefully and adapt legal regulations at an early stage. The inclusion of societal imperatives in technical innovations is necessary as well. E.g., Langenheinrich suggests the integration of the Fair Information Practices in technical protocols [Lan04, p. 30]. Similarly, individuals have to raise their awareness of privacy threats continuously. Thereby, the individuals need external support from governments, privacy protection organizations as well as commercial privacy protection suppliers. As has happened to other technological innovations in the past, the free market forces will solve some privacy threats of RFID. Beyond individual's countermeasures, the pressure of public relations and reputation will force RFID misusing companies to abandon these activities. Challenges for privacy protection especially arise when the free market forces are disabled, e.g. when totalitarian regimes use RFID for the surveillance of their citizens. In that case, discreet privacy protection tools for individuals become more and more necessary. After securing RFID's privacy implications, a usage of RFID comes along with benefits for both: companies and governments as well as consumers and citizens. Therefore, it is necessary to achieve the cooperation between a social discourse, technical innovations and legal regulations. Achieving this, for the time being, the "Orwell State" and the "Vitreous Consumer" will remain fiction.