



IST-2-004252-SSA

LEGAL-IST

LEGAL Issues for the Advancement of Information Society Technologies

Legal issues of RFID technology

Doc. No.:	D15	Responsible:	CIEEL
Rev. No.:		WP Reference:	
Issue Date:		Availability:	PU
Nr. pages:			

Status:	Final
---------	-------

KEYWORDS:	RFIDs, legal implications, data protection, data security
-----------	---

ABSTRACT

This report is conducted within the LEGAL-IST project and presents the technical functions and applications of RFID technology and discusses the legal implications with emphasis to data protection.



IST-2-004252-SSA

15
Report on Legal Issues of RFID
Technology

Rev. 0

Issue Date.: 16/05/2006


Page 2 of 30

QUESTIONS

For purposes of evaluation of the content of this study we kindly ask you to provide us with some feedback. Your answers will give the opportunity to contribute to the application of existing regulations on this emerging topic and shape the future policy making.

1. Is the study well aware of the technical features and the application potential of RFID technology?
2. Does the study capture the relevant legal issues relating to RFID technology?
3. How would you assess the issue of “personal data” that RFID tags may reveal? Do you agree / disagree with the opinion that RFID tags may be related to personal data in all 3 categories of the taxonomy (section 2.2 & 4.1. Please give the grounds for your statement)
4. Do you think that the data controller is the person who brings the tags on the product or also any other party that installs (in an unauthorised manner) a card reader and captures the information related to the RFID tag?
5. Do you think that the data controller shall have the obligations to inform the individuals about the use and removal / deactivation of the RFID tags as presented in section 4.3.3 (please give the grounds for your statement)
6. Please evaluate the technical and organisational measures as presented in section 4.3.4
7. Do you think that the current legislation is sufficient to deal with the RFID technology or new legislation is required (and for which exact issues)?
8. Please make any other additional comment to the study (i.e. are there any other relevant legal issues)
9. Please give your personal details in order to be able to facilitate effectively your feedback
Name, Organisation, Position, email, telephone

Please send your answers to Mr Torben Behrens (University of Goettingen) at: Legal-IST@jura.uni-goettingen.de

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 3 of 30</p>
---	---	--

COPYRIGHT


This document may not be copied, reproduced, or modified in whole or in part for any purpose without written permission from the LEGAL-IST Consortium*. In addition, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced.

All rights reserved.

This document may change without notice.

* The LEGAL-IST Consortium:

- European Society of Concurrent Engineering, (I)
- Loughborough University, Civil and Building Engineering Department, (U.K.)
- Centre of International and European Economic Law, (Gr)
- ALMA MATER STUDIORUM - UNIVERSITA DI BOLOGNA, (I)
- FIDAL, (F)
- J & A GARRIGUES, S.L., (E)
- KUNZ, SCHIMA, WALLENTIN & PARTNER RECHTSANWAELTE. (A)
- MASONS, (U.K.)
- UNIVERSITETET I OSLO, (N)
- GEORG-AUGUST-UNIVERSITAET GOETTINGEN STIFTUNG OEFFENLICHEN RECHTS, (D)
- CESPIM - CENTRO STUDI PER L'INNOVAZIONE D'IMPRESA S.R.L., (I)
- VALTION TEKNILLINEN TUTKIMUSKESKUS, (Fi)
- CETIM - CENTER FOR TECHNOLOGY AND INNOVATION MANAGEMENT GMBH, (D)
- INTERNATIONAL BUSINESS MACHINES BELGIUM, (B)
- Platte Consult, (D)

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 4 of 30</p>
---	---	--

CONTRIBUTORS

Name	Organisation
Dr Zoe Kardasiadou	Centre for International and European Economic Law (CIEEL) zoikard@the.forthnet.gr
Dr Zoi Talidou	Centre for International and European Economic Law (CIEEL)



 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 5 of 30</p>
---	---	--

TABLE OF CONTENTS

1	INTRODUCTION	6
1.1	PURPOSE, INTENDED AUDIENCE AND SCOPE	6
1.2	APPLICABLE DOCUMENTS	6
1.2.1	<i>Legal-IST project documents</i>	6
2	WHAT RFID IS ALL ABOUT.....	8
2.1	USE OF RFID TECHNOLOGY - SECTOR APPLICATIONS	9
2.1.1	<i>Retail / Consumer Goods Sector</i>	9
2.1.2	<i>Manufacturing Sector</i>	10
2.1.3	<i>Transportation/Logistics Sector</i>	10
2.1.4	<i>Recycling & waste management</i>	10
2.1.5	<i>Tracking of animals</i>	11
2.1.6	<i>Libraries</i>	11
2.1.7	<i>Health Care / Pharmaceutical Sector</i>	12
2.1.8	<i>Tracking of people (schools, prisons, VIP clubs)</i>	13
2.1.9	<i>Passports, IDs and Banknotes</i>	13
2.2	TAXONOMY OF RFID TAGS.....	15
3	LEGAL IMPLICATIONS	16
3.1	INFRINGEMENT OF THE RIGHT TO PRIVACY AND DATA PROTECTION	16
3.1.1	<i>Identification and profiling of a person</i>	16
3.1.2	<i>Unnoticed remote reading without line-of-sight</i>	16
3.1.3	<i>Use of RFID technology for law enforcement purposes</i>	17
3.2	INFRINGEMENT OF THE RIGHT TO PERSONALITY	17
3.3	INFRINGEMENT OF THE RIGHT TO HUMAN DIGNITY	17
3.4	UNFAIR COMPETITION.....	18
3.5	LABOUR LAW	18
4	RFID TECHNOLOGY AND DATA PROTECTION.....	19
4.1	DO RFID TAGS REVEAL PERSONAL DATA?	19
4.2	IS ARTICLE 9 OF DIRECTIVE 2002/58/EC APPLICABLE?.....	20
4.3	OBLIGATIONS OF THE DATA CONTROLLER	21
4.3.1	<i>Legal grounds for data processing enabled by RFIDs</i>	22
4.3.2	<i>Data minimisation and purpose limitation principle</i>	23
4.3.3	<i>Information requirements and data subject's rights</i>	24
4.3.4	<i>Technical and organisational measures for data security and exercise data subject's rights</i>	25
4.4	LEGISLATIVE MEASURES.....	27
5	CONCLUSIONS / RECOMMENDATIONS	28
6	REFERENCES	29

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 6 of 30</p>
---	---	--

1 Introduction

1.1 Purpose, Intended Audience and Scope

In the early 1970s fears about loss of privacy and worries concerning data protection - that made its appearance at this time – were focused on large, centrally held data-bases containing files about named or numbered individuals processed by huge computers situated in big rooms. People conceptualised the threat in terms of information in a file and the protection in terms of access security. As the Web, its attendant search engines and the inter-link ability of many databases in various networks have developed, the concept of “files” became trivial. Now the contribution of RFID technology to the realisation of the ambitious concept of an Ambient Intelligence Environment, where intelligent objects communicate to each other and exchange information (also personal data) and take decisions, brings us to the next step of the “Internet of the things”. Technology innovation and the impact of its usage stress a rethinking and re-examining of the existing legal framework.

From aforementioned perspective this deliverable is aiming at presenting the legal issues relating to RFID technology. The examination is not academic as far as this technology is currently being applied in some sectors, such as in the supply, logistics, consumer chain, for patients’ management or even on the new EU passports. In authors’ opinion, the most prominent current legal issue is the one related with the protection of privacy and data protection. The deliverable does not provide for an in-depth analysis of the related issues. Its aim is a first step analysis of the related issues which shall raise awareness and be used as a basis of further research and consultations in this sector.

To this purpose, the deliverable first analyses the technical aspects of the RFID technology, then it presents in detail various sectoral applications with implicit comments on relevant legal issues and at the end discusses in legal terms these issues.


This report has been prepared by the Centre for International and European Economic Law. Intended recipients of this Deliverable are all interested parties, such as RFID technology deployers (manufacturers and users), possible affected parties, such as employees, the European Commission as well as legal experts.

1.2 Applicable Documents


This report references the following reports:

1.2.1 Legal-IST project documents

1. State of the art research on legal issues related to the Information Society Technologies, April 2004.
2. Sixth Framework Programme Priority 2 Information Society Technologies Specific Support Action, Annex 1 – Description of Work, May 2004.

 <p>IST-2-004252-SSA</p>	<p>15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 7 of 30</p>
---	---	--

3. D 10a LEGAL-IST Roadmap

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 8 of 30</p>
---	---	--

2 What RFID is all about

Radio Frequency Identification (RFID) Technology uses radio waves to automatically identify wirelessly, contact less and without visibility¹ objects which, or people who have an RFID tag attached. It is grouped under the broad category of automatic identification technologies². One could say that it is no new technology: it was first used during the Second World War to identify airplanes as friend or foe³.

It consists of two parts: a tag that contains an identification number and a reader who works as a scanner that triggers the tag to broadcast its identification number. This number usually acts as an input to further data processing⁴. RFID is designed to enable readers to capture data on tags and transmit it to computer system without needing a person to be involved.

A typical RFID tag consists of a small integrated circuit attached to a radio antenna, capable of transmitting a unique serial number at a distance of several meters to a reading device in response to a query. The size of these microchips is about 1/3 of a millimetre (smart dust). It can easily be embedded onto or into (textile-) products, onto their packages, in items that humans carry with them all of the time or even direct implanted beneath their skin.

RFID tags can be active, semi-active or passive. **Passive Tags** do not have a power source; they simply reflect back energy coming from the reader antenna⁵. **Active RFID** tags on the other hand, have their own internal power source which is used to power any integrated circuits and generate the outgoing signal. They may have longer range and larger memories than passive tags, as well as the ability to store additional information sent by the transceiver. Active tags can also be distinguished between transponders and beacons. *Active transponders* are woken up when they receive a signal from a reader: they conserve battery life by having the tag broadcast its signal only when it is within the range of a reader. *Beacons* emit a signal with their unique identifier at pre-set intervals and are used in most real-time locating systems.

To retrieve a data stored on a RFID tag a reader is needed. A typical reader is a device that has one or more antennas that emit radio waves and receive signals back from the tag. This RFID reader is simultaneously a data-collection instrument, promiscuously gathering information from each RFID that responds to its broadcast, and a transmitter or broadcaster of information, as it sends its data through a network to a point where data is being further processed. The databases connected to these networks hold and keep the gathered information.

The unique serial number from RFID tags makes it easy for database and archiving companies to store and associate data by linking to this ID. The main use is to be seen in the tracking of


¹ Radio Frequency Identification, Wikipedia, available at: <http://en.wikipedia.org/wiki/Rfid>

² What is RFID?, RFID Journal, available at: <http://www.rfidjournal.com/article/articleprint/1339/-1/129/>

³ See <http://en.wikipedia.org/wiki/Rfid>

⁴ Hennig, Ladkin, Sieker, Privacy Enhancing Technology Concepts for RFID Technology Scrutinised, p.1.

⁵ The basic of RFID Technology, RFID Journal, available at: <http://www.rfidjournal.com/article/articleprint/1337/-1/129/>

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 9 of 30</p>
---	---	--

products in the retail procedure, in the shops or even after that, and in the spotting of human beings in prisons, schools and elsewhere.

RFID tags are increasingly being used as a more advanced form and possible replacement of bar codes. They provide for unique identification of each tagged unit whereas bar codes are identical for every unit of the same product⁶: RFID tags contain not only the product category such as "shampoo from company X" but clearly identify each individual item, e.g. additionally "bottle number 12345", which is a new quality.

Most of them operate as passive transponders. Active RFID tags are being used for more complicated procedures than identifying in a unique manner items. Such uses can be monitoring and storing information of the parameters of the environment in which these tagged items move like temperature and humidity. This could help recalling transportation steps to find out the precise moment of damage of sensitive goods, in order to change the conditions and avoid further damages.

Since prices of RFID are dropping it is to be expected that their widespread deployment will become increasingly economically viable⁷. Many postulate that they will be the essential drivers of ubiquitous computing and will introduce the so called "Internet of the things".

2.1 Use of RFID technology - Sector Applications

2.1.1 Retail / Consumer Goods Sector


Companies across the retail and consumer packaged goods supply chains have been among the early adopters of RFID and Electronic Product Code (EPC) technologies: by RFID means they reduce spoilage, they are improving promotional sales using EPC data, and they reduce out-of-stocks.

Electronic Product Code (EPC) is a set of standards for the automatic identification of consumer products replacing the current bar-code system. EPC consists of a header number that identifies the version of EPC, a manager number that identifies the company associated with the product, an object class number that identifies the product type and a unique serial number⁸. EPC global Network is a set of RFID technologies enabling immediate automatic identification and sharing of information on items in the supply chain. The numbers that EPC contains disclose their content only to the subscribers of the EPC global Network and give them access to the EPC Discovery Service, an Object Naming Service. Everyone with access to EPC Discovery can monitor or track the movement of a particular RFID-tagged item.

⁶ See *International Conference of Data Protection & Privacy Commissioners*, Resolution on Radio-Frequency Identification, (Nov. 20, 2003) p. 2, available at: <http://www.privacyconference2003.org/resolutions/res5.DOC>

⁷ According to Gerd Wolfram, manager of the German company Metro, the deployment of RFIDs to each product unit will start when the price per unit will reach the 1 cent or less. Currently the price is about 14-15 cents per unit, so that RFIDs are used only in supply chain on whole pallets of goods, *Frankfurter Allgemeine Zeitung*, 14/01/2006, p. 18

⁸ See EPCglobal „Electronic Product Code“ available at: www.epcglobalus.org/Network/Electronic%20Product%20Code.html

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 10 of 30</p>
---	---	---

The retail industry is using passive tags that implement no protection against unauthorised access to EPC tag. Hence the EPC can be read out directly by any RFID-reader from a six to eight meters distance⁹. This range is big enough for attackers to scan objects reliably at entry posts to public buildings and places.

2.1.2 Manufacturing Sector

Whether or not they face mandates from customers, many manufacturers are finding that RFID has the potential to bring major benefits, both in their supply chains and in their factory operations. This new technology can increase productivity and reduce costs by enabling to track inventory, reusable containers, work in process and finished products: they can manage parts inventory with active RFID, improve the tracking of work in process, reduce parts defects, and increase factory productivity by using active RFID tags. In some cases, RFIDs aim in such seemingly simple tasks as ensuring that the right label goes on a product or that a box contains everything it should. In other cases, RFID is put through more complex uses as tracking an item through every workstation and recording every tool that performed an operation on it. This information can be used to quickly identify potential problems and correct them before they show up in the product. RFID can furthermore save companies a great amount of money spent on replacing lost tools, that can be easily traced through the tags.

Companies that supply the U.S. Department of Defence and airplane makers Boeing and Airbus will be required to put RFID tags on shipments to these major companies. The aim is to track high-value parts and products internally, to tag and track metal parts, to use RFID to reduce counterfeiting of parts, to improve safety by using RFID to track hazardous materials and to track work in process. This deployment of RFID technology addresses mainly to the Department of Defence and concerns the military supply chain and the aerospace applications.


2.1.3 Transportation/Logistics Sector

Transportation and logistics companies will play a key roll in ensuring end-to-end visibility in the supply chain. Some are already tagging product for their customers. Others are examining how they can benefit internally, by improving the utilization of containers with RFID tracking: they can boost container yard throughput with RFID tracking, improve cargo tracking with RFID, logistics hubs can benefit from a real-time locating system, and they can improve the visibility of cargo in transit and cargo security with electronic seals.

2.1.4 Recycling & waste management

The Electronic Product Code (EPC) tags may be used to automatically sort recyclable material and will also identify manufacturer, type and weight of disposable material (the manufacturer of

⁹ Auto-ID Centre (2003): Technical report 860MHz-930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1., MIT, USA, available at: http://interval.hu-berlin.de/downloads/rfid/chipklassen/4_candidate_recommendation_1_0_1.pdf

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 11 of 30</p>
---	---	---

a product that will eventually constitute hazardous waste may ultimately have to pay for its safe disposal).

2.1.5 Tracking of animals

Low-frequency RFID tags are commonly used for animal identification. Pets can be implanted with small chips so that they may be returned to their owners if lost. They can also be used to satisfy the need to track herds and to be able to recognize when an animal is missing and, if the animal has died, locate its body¹⁰.

Recent repeated outbreaks of animal epidemics, such as Bovine Spongiform Encephalopathy (BSE), Foot and Mouth disease have considerably changed consumers' attitudes towards meat products. They want guarantees that the food they eat is of the highest quality, and has been handled safely throughout the supply chain from 'farm-to-fork'. As a result, electronic animal tracking is rapidly becoming a significant area for RFID solutions. Following successful animal tracking trials¹¹, the European Council of Ministers (ECM) has adopted a law¹² throughout Europe requiring the individual electronic tagging of sheep and goats using RFID technology. After an initial transitional period, chip tagging in compliance with ISO standard 11784/85 will be compulsory from 1 January 2008 for Member States with a sheep and goat population exceeding six hundred thousand animals. It will remain optional for Member States with populations smaller than this, except for animals intended for trade within the EU.

Besides, RFID tags are used for to identify big pets, such as dogs over 20 kilograms. There are already several laws in the European level that makes the wear of such a tag compulsory. On the tag are to be found at least following data: unique number for the chip, data of the pet and data of the owner of the pet. The privacy concerns that rise here is besides the threat of unauthorised acquisition of the data, who has the right to access these data and for what reasons (law enforcement, competent authority to grant the pet placket)¹³.

2.1.6 Libraries


Libraries began using RFID systems to replace their electro-magnetic and bar code systems in the late 1990s. RFID technology in libraries promises to relieve repetitive strain injury, speed patron self-checkout, make possible comprehensive inventory and automated sorting, retrieve hidden items and support security. Many libraries (more than 130 in North America and the

¹⁰ See http://www.rfidgazette.org/asset_tracking/

¹¹ See *Balch, Feldman, Wilson*, Assessment of a RFID System for Animal Tracking, The BORG Lab, Georgia Institute of Technology, Atlanta, Oct. 1 2004, available at: <http://www.cc.gatech.edu/~storm/Feldman2004TR.pdf>

¹² See Regulation 1760/2000/EC of the European Parliament and of the Council establishing a system for the identification and registration of bovine animals and regarding the labelling of beef and beef products and repealing Council Regulation 820/97/EC, 2000, OJ L 204, p.1, and Council Regulation 644/2005/EC of 27 April 2005 authorising a special identification system for bovine animals kept for cultural and historical purposes on approved premises as provided for in Regulation 1760/2000/EC of the European Parliament and the Council, 2005, OJ 107, p. 18

¹³ See the 2004 Annual Report of the Berliner DPA, available at: http://www.datenschutz-berlin.de/jahresbe/04/teil4_4.htm

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 12 of 30</p>
---	---	---

Stadtbibliothek of the city of Vienna¹⁴) are starting to tag every item in their collections with RFID tags. The tag contains some amount of static data (bar code number, manufacturer ID number) that is permanently affixed to the library item (i.e. book, CD, DVD). This information is transmitted from the reader to the library's security, circulation and inventory applications¹⁵.

Current library RFID tags do not prevent unauthorised reading of tag data¹⁶. Here we are handling with an item-level tagging regime that might raise privacy concerns: the ability to track tags introduces the possibility of surveillance of library patrons and their reading habits in case title and author information is stored on the tag¹⁷. Therefore best practices of Berkeley Library include limiting the data and the use of this tag as a bar code only¹⁸. The activist group Electronic Frontier Foundation proposes to the San Francisco Public Library to use RFID tags with kill technology and to protect so patrons from inventorying and tracking risks¹⁹.

2.1.7 Health Care / Pharmaceutical Sector

Hospitals plan to deploy RFID to identify patients, call up records, reduce medical errors and improve overall productivity. For instance, a pilot project has started in July 2005 in clinical centre of Saarbrücken in cooperation with the companies Intel, Siemens Business Services and Fujitsu-Siemens. Thousand of patients receive on admission a bracelet with an RFID tag on which the patient identifier is stored. Physicians and nurses may access the patient identifier and then the data stored on a database through a wireless network. The project is based on a solution already deployed in Jacobi Medical Centre, New York²⁰. An additional use of RFIDs carried by hospital personnel is that it can also get easily located from a central system in case of emergency²¹.

The U.S. Food and Drug Administration has endorsed the use of RFID technology as a way to reduce the counterfeiting of drugs²². This will help preventing the introduction of counterfeit drugs and biologics into the drug distribution chain, facilitating the identification of counterfeit drugs, minimising the risk and exposure of consumers to these and avoiding unnecessary costs to the prescription drug distribution system (implementing the Prescription Drug Marketing Act PDMA²³).

¹⁴ <http://www.ekz.de/2110.html>

¹⁵ See Lori Bowen Ayre, Wireless tracking in the library: benefits, threats, and responsibilities, p. 233, in: *Simson Garfinkel, Beth, Rosenberg*, RFID applications, security and privacy, 2006

¹⁶ See *Molnar, Wagner*, p. 218

¹⁷ *Molnar, Wagner*, Privacy and Security in Library RFID issues, practices and architectures, CCS'04, October 25-29 2004, Washington, DC, USA, p. 210, available at: <http://www.cs.berkeley.edu/molnar/library.pdf>

¹⁸ Available at: <http://berkeleypubliclibrary.org/BESTPRAC.pdf>.


¹⁹ http://www.eff.org/Privacy/Surveillance/RFID/20031002_sfpl_comments.php.

²⁰ Computer mir Augen und Ohren, at: Frankfurter Allgemeine Zeitung, 14.01.2006, p. 18.

²¹ *Article 29 Working Party*, WP 105, Working document on data protection issues related to RFID technology, January 19, 2005, available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

²² See U.S. Food and Drug Administration, Combating counterfeit Drugs, A Report of the Food and Drug Administration, February 2004, available at: www.fda.gov/oc/initiatives/counterfeit/report02_04.html

²³ Available at: www.fda.gov/cber/pdma.html.

 IST-2-004252-SSA	15 Report on Legal Issues of RFID Technology	Rev. 0 Issue Date.: 16/05/2006 Page 13 of 30
---	---	--

2.1.8 Tracking of people (schools, prisons, VIP clubs)

A group of children in Yokohama City in Japan wears active tags to keep them safe on their way to and from school²⁴. Each child participating to the programme wears a bracelet with a RFID tag. The tags can be set to send a signal, every second or every minute to existing Wi-Fi access points used by the city for wireless Internet access. Those Wi-Fi points function as RFID readers. They transmit the data to the school information system which is holding its pupil's identification. The system can also be set up to notify parents or guardians automatically via e-mail on a cell phone or PC if a child passes a specific Wi-Fi access point on the way to or from the school. This system has been tried out to increase public confidence in children's safety and to combat crimes against children while in transit to school.

The VIP Baja Beach Club of the Catalan city of Barcelona offers its VIP clients the opportunity to have a syringe-injected RFID microchip implanted in their upper arms that not only gives them special access to VIP lounges, but also acts as a debit account from which they can pay for drinks²⁵.

A new tracking system has been developed, which provides real-time identification and tracking of inmates and officers within prisons facilities, both indoors and out²⁶. The system can accurately locate and identify any person wearing a small wireless "tag" device, and this information is integrated into prison monitors. It handles common prison complexities such as a multi-floor, mixed indoor/outdoor environment, as well as the need for cell-level accuracy. The tag immediately detects any attempt to remove or tamper with it. The Los Angeles County jail system has reportedly engaged in a pilot project to use RFID technology to track inmates at the Pitchess Detention Centre in Castaic²⁷.

2.1.9 Passports, IDs and Banknotes

In May 2004 the International Civil Aviation Organisation (ICAO) adopted specifications for machine readable travel documents (MRTD) which demands for digital storage of the passport's holder name, date of birth, passport number and of the pass photo²⁸. Optional data items include such data as nationality, profession, and place of birth. In the future they intend to launch other biometrics too, as the fingerprints and the iris. The ICAO specification relies on the ISO 14443. Tags in this standard are passive and for security reasons the intended read range is about 10 centimetres. The ICAO guidelines specify also an array of cryptographic measures, to ensure the authenticity and privacy of the personal data held in the chip.

In compliance with the recommendations of the ICAO the Council of the European Union adopted on 13/12/2004 a regulation²⁹ mandating the inclusion of both facial image and

²⁴ <http://www.rfidjournal.com/article/articleprint/2050/-1/1/>


²⁵ See <http://news.bbc.co.uk/2/hi/technology/3697940.stm>; <http://www.heise.de/newsticker/meldung/53789>

²⁶ See <http://www.technologynewsdaily.com/node/1900>

²⁷ See <http://www.socaltech.com/fullstory/0001952.html>

²⁸ Available at: http://www.icao.int/cgi/goto_m.pl?icao/en/strategic_objectives.htm

²⁹ Council Regulation 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385, available at: http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00010006.pdf

 IST-2-004252-SSA	15 Report on Legal Issues of RFID Technology	Rev. 0 Issue Date.: 16/05/2006 Page 14 of 30
---	---	--

fingerprints in future passports and travel documents issued by EU Member States. The new regulation aims at better protecting EU passports against forgery, at enabling better identification of passport holders and at harmonising security standard features used in the production of passports and travel documents issued by Member States³⁰.

Since November 2005 Germany introduced the first e-passport³¹, equipped with biometric data stored on a RFID tag. According to the relevant provision of the German Passport Law³², new law – which still does not exist – should settle down the type of biometric data in use, details about the way of their encryption and storage, and the purpose limitation. In Italy the Foreign Affairs Ministry issued on 17th January 2006 a decree concerning the introduction of a new electronic passport that will include biometric data contained in RFID chips³³.

RFID technology is fierce controversial³⁴. It still shows high error probability³⁵ and bring up serious data protection concerns. *Intended read range* of a reader means the range achievable with vendor-standard readers. However the information on the tag may be obtained by readers who may achieve longer read ranges³⁶. It is also possible to eavesdrop on a conversation between a legitimate reader and an RFID tag over a greater distance (10 meter). The risk of eavesdropped or unauthorised obtained data from an unauthorised reader is extra high and the consequences to the private sphere are tremendous, e.g. identity theft and alteration. Therefore is of significant importance for Passports and other governmental-issued documents that the identification contained in their tags cannot be altered. Though specialist still argue that the technology (Passive Authentication, Basic Access Control and Active Authentication) used is not effective enough for reducing the opportunity for unauthorized reading of the passports and the consequential threats of identity theft, tracking and hotlisting³⁷.

The European Central Bank was moving forward with plans to embed RFID tags as thin as a human hair into the fibres of Euro bank notes by 2005³⁸. A spokesman for the ECB in Frankfurt confirmed on July 4, 2003 that the bank intends to add further protection to the Euro. Hitachi Ltd. has developed a RFID chip that requires no external antenna and makes possible the embedding of tracking and identification chips in bank notes, tickets and other paper products³⁹.

³⁰ See e-government of the European Union news available at: <http://europa.eu.int/idabc/en/document/3669/330>

³¹ <http://www.epass.de/>

³² Paragraph 4 Abs. 4 Satz 1 PassG

³³ See www.statewatch.org/news/2006/feb/08italy-biometric-passports.htm

³⁴ See *Borchers*, Kritik am Reisepass, c't 21/2005, available at: <http://www.heise.de/ct/05/21/060/>


³⁵ So *Schulzki-Haddouti*, Neue Reisepässe: Mit Sicherheit teuer, available at: <http://www.sicherheit-heute.de/index.php?ccpage=Verkehr>

³⁶ See *Juels, Molnar, Wagner*, Security and Privacy Issues in E-Passports, IEE SecureComm 2005, available at: www.cs.berkeley.edu/~dmolnar/papers/papers.html

³⁷ See essay above. Also *Rieback, Crispo, Tanenbaum*, Is your cat infected with a computer virus?, 2006, available at: www.rfidvirus.org/papers/percom.06.pdf

³⁸ See *Yoshida*, Euro Bank Notes to Embed RFID Chips by 2005, EETimes, 19.12.2001, available at: <http://www.eetimes.com/story/OEG20011219S0016>

³⁹ See <http://www.computerworld.com/mobiletopics/mobile/story/0,10801,84543,00.html>

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 15 of 30</p>
---	---	---

But now it is still uncertain whether they will force this plan or not because, according to new statements, RFID technology is not safe enough to combat monetary counterfeit⁴⁰.

2.2 Taxonomy of RFID tags


RFID technology is part of the broader technology of automated identification of items or of people. As shown above (sec. 2.1) the use of RFID technology at the moment and the applications, that we can foresee in the near future being put in practice, let us build three broad categories of RFID tags according to the information they may reveal about a person and the way this information is revealed (authorised or not):

a) We have the tags that contain only an item number (i.e. in retail / consumer goods sector). These tags are passive and are at the moment the most frequent and widespread application of RFID technology. Their use is in giving information for the identification of an item. Through the linking of the RFID tag number with a products database one can find out what kind of item this is. Supposing the item information is linked to the purchaser during the payment procedure and further stored to a customers' database one may create customers' purchase profiles. Supposing the item information can be associated to a person either because this person is currently visible or this person is identifiable by other means, for instance with its RFID identification card (i.e. passport) or employee's card, this all may lead to a person's identification for various purposes (customers' profiling, surveillance of workers at workplace).

b) The second category concerns tags that contain an identification number which reveals the identity of a person after the matching of the information contained on the tag with a backend data-base, which holds the information concerning the identity of the person (see sec. 2.1.8). In comparison with the first category here we have a more direct relation to the information of the RFID tag and the person carrying it because one needs only the link to the back-end database which provides for the information of a person.

c) However the stronger relation to a person is to be found in the RFID tags of the third category. On these tags personal data are directly stored. They are normally active tags and contain information like name, age, nationality and so on (see sec. 2.1.9).

⁴⁰ See <http://www.zeit.de/zeit-wissen/2006/01/Falschgeld.xml>

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 16 of 30</p>
---	---	---

3 Legal Implications

On the basis of the aforementioned taxonomy of RFID tags and the current or envisaged or even possible applications of RFID technology, as described above, following legal implications may arise.

3.1 Infringement of the right to privacy and data protection


RFIDs tag may be related to personal information. Data protection and the information self-determination is a precious fundamental right that should be protected from the technical development, if this proceeds without taking into account the conformity to main constitutional values and rights. It should be assured that the right to privacy and to data protection will not turn into a caprice of the individual but will still remain an obligation of the democratic society.

3.1.1 Identification and profiling of a person

RFID tags consist of a unique identification number. The use of the tag is to enable identifying and tracking every single item. Everyone who carries at least one so-tagged item is possible to get allocated and tracked. RFID tags function as a unique identifier and the growing interoperability of the system makes allocating and tracking possible worldwide. Beyond that, the link-ability of RFID technology to other databases and their supersets-archives can facilitate the identification process. RFID information can be used independent from information of other sources. But the facileness of the combination of both turns it into a main threat to privacy. As we saw in the application of RFID technology in the retail sector, once tagged objects are owned by persons, it is possible to be related to them. The ability of tracking objects might become an ability to track individuals. Using RFID technology retailers might track customers within their shops in order to create profiles of movement which can be used to improve marketing strategies. One should mention that this is possible only by connecting the information obtained by the tagged object that individuals carry with them and their customer or credit cards that they submit at the purchase point. Only in that matter the data stored on the EPC tag relates to the person carrying it. In shopping malls several shops might interlink tracks and analyse the popularity of different parts of the centres by analysing the favourite shopping routes of customers that have already been identified by one of the shops in the mall. The advantage of it is a better management and promotion policy to increase consumption.

3.1.2 Unnoticed remote reading without line-of-sight

RFID tags can be read without line-of-sight and without overt evidence that they are being read. In addition their small size and the lack of need of energy supply make them appropriate to be installed hidden. The problem is that radio waves allow data to be processed over a given distance without any need for a direct line-of-sight link with the chip and without the data subject having to take an active part in the process. In other words, data processing can take place without the knowledge of the data subject. Any data on RFID transponders that have not been destroyed or deleted can be read by visible or even invisible readers. The unnoticed remote reading may indeed be used for various purposes without the knowledge of the person in

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 17 of 30</p>
---	---	---

question, for instance for unnoticed surveillance of workers, unnoticed profiling of one's consuming preferences etc.

3.1.3 Use of RFID technology for law enforcement purposes

The state might have an interest on making use of personal data obtained through RFID applications for law enforcement purposes. Here all the applications mentioned above can be used by the Law Enforcement Authorities, under the conditions that every national legislation allow this, for the purposes of prevention, investigation and prosecution of criminal offences. We could imagine the interest of these authorities for the exact identification of the owner of a consumer good related to a criminal offence, or the lists of the movement of cars passing through the toll-controls, the tracking of people carrying RFID enabled IDs or passports, or even RFID implanted tags. Even the use of RFID tags in banknotes can be highly problematic in this perspective. Through RFID it will be possible to determine which banknotes were withdrawn by whom from which automatic teller machine, or where those banknotes were then used to buy certain products or services.

3.2 Infringement of the right to personality

RFID technology will contribute to the realisation of the Ubiquitous Computing: in a world of ubiquitous services the interaction of humans with computers should step behind and help us enter a digital world without realising it. The citizens must be fully aware of the innovation and of the data-processing procedures that enable this phenomenon but at the same time concerns them instantaneous⁴¹. Within a densely populated world of smart and intelligent but invisible communication and computation devices, no single part of our lives will per default be able to seclude itself from digitalisation⁴². Nevertheless one should always be able to retrace the data-processing procedures and have the right to switch onto an "of-line" world. If there is no possibility to do so, this will affect the free expression of the personality of a human being.


3.3 Infringement of the right to human dignity

RFID systems introduce for the first time a new dimension of availability of trustworthy data about objects and about the movement of these objects in real time. They improve the congruence between real and virtual life⁴³. Consequently one could say that we enter a new era where the co-existence of two cognitive dimensions takes place while there is no assurance that the new technological aspects that lead us over are faultless. Beside the sociological aspect of this observation, there is a legal impact too: complete reliance on technical systems and on-going dependency on them can turn into discrimination of individuals and breach of their constitutional rights. Here one could think of an obligation to carry RFID because there is no other way of

⁴¹ See *Langheinrich*, Die Privatsphäre im Ubiquitous Computing - Datenschutzaspekte der RFID-Technologie, available at: <http://www.vs.inf.ethz.ch/publ/papers/langhein2004rfid.pdf>

⁴² *Langheinrich*, Privacy by Design-Principles of Privacy-Aware Ubiquitous Computing, p. 7 available at: <http://www.vs.inf.ethz.ch/publ/papers/privacy-principles.pdf>

⁴³ See *German Federal Authority for Information Systems Security* (Bundesamt für Sicherheit in der Informationstechnik), Security Aspects and Prospective Applications of RFID Systems, 2005, p. 85, available at: http://www.bsi.bund.de/fachthem/rfid/RIKCHA_englisch.pdf

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 18 of 30</p>
---	---	---

acting in a future society. For instance we could imagine of future toll-controll systems using only RFID technology, where the right of travelling anonymous simply does not exist. The nature of RFID technology, identifying by sending information will first affect the right to privacy and to data protection of the individuals. However, the range of use of the new technology and the intensity of its application could contribute to the establishment of an environment, which does not respect basic values of a democratic society and fundamental constitutional rights. In this regard, the Japanese program for the children (see sec. 3.1.8) might breach children's right to privacy and dignity by treating them like cattle or a piece of inventory and by familiarizing them with an environment and a world of absolute surveillance.

3.4 Unfair competition


The interoperability of RFID systems is from a business perspective in positive: for a sustainable model, a retailer should avoid having to implement several different tag readers in order to scan tags produced by various manufacturers. Inexpensive tags simply do not have the memory to store lists of readers that can authenticate themselves to the tag, in order to avoid unwanted reading of tags; and they don't have the power to call out to an enterprise server to get this information from a database⁴⁴. So they are exposed to unauthorised reading by competitors, for instance if a rival enters the shop of a competitor and “scans” by a mobile reader its inventory. In this respect concerns appear regarding unfair competition practices.

3.5 Labour law

The deployment of RFID technology for the improvement of manufacturing, the supply and the logistics chain or for the end-customer service in the retail sector may raise implications for the employees. Besides, the use of the same RFID tags for other purposes, such as the surveillance of employees which is already mentioned above, this technology may affect the health of employees in terms of possible radiation emitted during the data communication between tag and reader. It might also lead to cutting personnel as a result of rationalisation through the use of the technology. Such issues shall be treated as any other similar technology which is introduced at the workplace. For instance, according to national legislation in question prior approval by the workers' council might be necessary for the deployment of RFID technology⁴⁵. Moreover, as for any other technology deployed within the workplace, the employer has a duty to monitor any negative effects to employees' health and take the appropriate counter-measures.

⁴⁴ For more details concerning authentication in the RFID technology see *Marlena Erdos*, RFID and authenticity of goods, p. 137, in: *Simson Garfinke /, Beth, Rosenberg*, RFID Applications, Security and Privacy, 2006

⁴⁵ The German Kaufhof AG has prior agreed with the employee's Council the exact purposes of RFID tags within its stores and its obligations regarding employees' health safety and a temporary prohibition of personnel reduction as a result of the use of RFID technology: RFID in Pilotphase – Gesamtvereinbarung bei der Kaufhof Warenhaus AG, in: RDV 2005, pp. 185

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 19 of 30</p>
---	---	---

4 RFID Technology and Data Protection

As shown in previous section the prominent legal implications are closely linked to privacy and data protection. Depending on how intensive the use of RFIDs is, possible breaches to the right to privacy may be qualified also as breaches of the rights to the free expression of personality and to human dignity. Therefore, in this section the legal issues related to data protection shall be discussed in more detail. To this end, the legal basis is the EU Directives on data protection, notably the general Directive 95/46/EC on the protection of personal data and, where necessary, the Directive 2002/58/EC on the protection of personal data in the electronic communications sector. In this regard, special attention should be also paid to the work done already by the Article 29 Data Protection Working Party⁴⁶.


4.1 Do RFID tags reveal personal data?

The notion of personal data is defined in the Directive 95/46/EC. According to article 2 (a) of the Directive “*personal data shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*”. Recital (26) of the Directive states that “*in order to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person*”.

At a first glance, RFID tags look to be anonymous. Whether or not RFID tags contain or relate to personal data is a crucial point for the applicability of the Directive on the protection of personal data. As shown above, in the taxonomy of RFID tags (sec. 3.2), such tags are not always anonymous. According to the third category, tags, such as those used for ID cards or passports contain personal data. Here, therefore, there is no doubt about Directive’s applicability. The second and first category of the taxonomy deals with cases where a person is identifiable only. The second category is referring to cases where one to identify a person needs to link the number contained on the RFID tag to the backend database. This category may very well fall within the scope of the Directive, since the number of the tag is an identification number that reasonably may be linked by means of the data controller, such as the back-end database, to a person⁴⁷. The first category addresses the most vague cases of identifiable persons since one need to correlate information from at least two back-end databases, such as the one containing the product information and the one containing the customers’ information. It also addresses cases where the item information can be associated to a person either because this person is currently visible or by other means such as an RFID ID card or employee’s card.

⁴⁶ Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, WP 105, January 19, 2005, available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

⁴⁷ See Keuleers, Ewout, Reconciling RFID technology with data protection principles, Droit Nouvelles Technologies, April 2005, p. 2

	<p>15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 20 of 30</p>
---	---	---

Important criterion is the available extra information as well as the operating expenses to identify and to personalise someone⁴⁸. Article 29 Data Protection Working Party opines that the Directive is applicable to cases, where a person can be identified at an associative level due to the large mass of information surrounding her/him or stored about her/him⁴⁹. It also opines that the relation to a person may be established even where a store is using by scanning a RFID tagged product a customer carries everyday, in order to profile this person's shopping habits. It also sees a risk to personal data if someone scans by unauthorised readers products that a person carries which at current state may be valuable, such as banknotes etc. There are, however, opposing opinions to such a definition, as expressed in the public consultation carried out by Article 29 Data Protection Working Party. Apparently, regard shall be paid to whether such operations will be reasonably deployed, in terms of economic and other factors, in order to identify a person⁵⁰.

As a result, the perception of personal data has to be re-analysed in regard to specific characteristics of the RFID technology. Directive 95/46 is certainly applicable in the vast majority of the aforementioned cases; the interpretation of the notion "personal data" regarding the new emerging needs has to be at least at European level consistent.

4.2 Is article 9 of Directive 2002/58/EC applicable?

According to article 9 of the aforementioned Directive location data other than traffic data of subscribers or users of public communications networks or publicly available electronic communications services may be processed for the provision of a value added service only if they made anonymous or with the prior informed consent of the subscribers or users. The electronic communications service provider has thus the obligation to inform and obtain the consent of the data subjects.


As shown in section 2, RFID technology may reveal or be primarily used for the localisation of persons. In this regard, it is to examine whether article 9 of Directive 2002/58/EC is applicable. The wording of this article and the scope of the Directive does not however provide for a direct applicability. Article 9 requires that a processing of personal location data is taking place within the context of a public communications network or a publicly available electronic communications service and, as a result addresses the obligations of the respective providers. RFID technology enables, on the other hand, a communication without the need of a publicly available network and the provision of such services nor involves respective providers⁵¹.

⁴⁸ See *Saeltzer*, Sind diese Daten personenbezogen oder nicht?, DuD 2004, p. 218

⁴⁹ *Article 29 Data Protection Working Party*, Working document on data protection issues related to RFID technology, WP 105, 19 January, 2005, available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf, sections 3, 4.1

⁵⁰ *Article 29 Data Protection Working Party*, Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology, WP 111, 28 September, 2005, available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf

⁵¹ So *Mueller, Juergen*, Ist das Auslesen von RFID-Tags zullaessig?, in: DuD 2004, pp. 215 ((216)

	<p>15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 21 of 30</p>
---	--	---

Article 9 may be applicable only where the RFID technology is an additional feature of the terminal equipment of the subscriber or user which enables the provision of a value added service. For instance, an RFID tagged mobile phone may communicate subscriber's or user's data to third parties for the purpose of advertising when the owner of the RFID tagged mobile phone passes a certain point. To the extent the electronic communications service provider is transferring personal data to the third party, i.e. the name and number of the RFID tagged mobile phone owner, consent of the owner shall be prior obtained.

Since RFID technology enables the location of persons, especially in an unnoticed and possibly very intrusive manner, it shall be further examined whether there is a need for a specific provision or whether, at least a uniform application of existing provisions may be achieved at EU level.

4.3 Obligations of the data controller

According to article 2 (c) Directive 95/46/EC the controller *“shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data”* Normally, thus, the data controller will be the tag deployer who determines the purpose of the tag use in conjunction with the whole processing taking place through the transmission of the tag information to the reader and from the reader to any other means, such as a back-end database. In this sense, the tag deployer, as data controller, shall comply with the principles and obligations as set out in the EC Data Protection Directives.

The Directive lays down the following principles with regard to data processing:


Purpose limitation: Personal data shall be collected and further processed for explicit and specified purposes (art 6)

Proportionality: Personal data shall be relevant and not excessive for the specified purposes

Data quality: Personal data must be accurate, kept up to date and where necessary erased or rectified

Lawfulness: Personal data shall be processed fairly and lawfully (art 6), i.e. only for legitimate grounds as laid down in article 7 of the Directive. Such grounds are a) the unambiguous, specific and freely given informed consent of the data subject, b) the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, c) a legal obligation to which the controller is subject, d) legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, e) for the protection of vital interests of the data subject and f) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.

There are also other legal grounds laid down in article 8 of the Directive as far as the personal data are sensitive. In the context of RFIDs, as shown above (sec. 2.1.7., such data may be related to health, if for instance RFID tags are used for the patient management. Accordingly, sensitive data may be processed either by data subject's explicit consent, or for the protection of data subject's vital interest where this is physically or legally incapable of giving his / her consent, or

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 22 of 30</p>
---	---	---

for purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a person subject to professional or equivalent secrecy.


Data subject's rights: Data subject has a) the right to be informed (art 10, art 11 Directive 95/46/EC) about data controller's identity and his representative, if any; the purpose(s) of the processing for which the data are intended; the recipients of the data; whether replies to questions are obligatory or voluntary and the possible consequences of failure to reply including the existence of the data subject's right of access to and the right to rectify the data concerning him; b) the right of access (art 12 (a) Directive 95/46/EC) as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed; c) the right of rectification (art 12 (b) Directive 95/46/EC) concerning incomplete or inaccurate data or, in general, data which processing does not comply with the provisions of the Directive.

Data security: According to art 17 of the Directive the controller is required to take all appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, disclosure or access, in particular where the processing involves the transmission of data over a network. The controller is thus free to choose these measures that may effectively avoid the aforementioned risks. Moreover the measures are the result of the assessment of four variables: the risk represented by the processing, the nature of the data to be protected and the state of the art and the cost of the implementation of the measures.

4.3.1 Legal grounds for data processing enabled by RFIDs

In applying aforementioned principles to processing by RFIDs the vast majority of such processing shall be based on data subject's prior consent. In the private sector it is hard to think on cases where the use of RFIDs is necessary for the conclusion of a contract. Customer cards, VIP cards etc. are normally used for value-added services and therefore they do not serve the prime purpose of the contract, i.e. the purchase of an item or service. In some other cases the RFID technology might be used for the purchase of a specific service, for instance within a VIP club or with regard to product information in a smart-home environment etc. Also here this service is a contractual service for which the data subject has consented as part of the conclusion of a contract.

When location data are processed by using of RFID technology and for the provision of value added services and this processing is enabled within the context of a public communications network or publicly available communications services, the provider of the value added services shall according to article 9 of Directive 2002/58/EC ask for the prior informed consent of the data subject. For instance, an RFID tagged mobile phone may communicate subscriber's or user's data to third parties for the purpose of advertising when the owner of the RFID tagged mobile phone passes a certain point. To the extent the electronic communications service provider is transferring personal data to the third party, i.e. the name and number of the RFID tagged mobile phone owner, consent of the owner shall be prior obtained. As Article 29 Data Protection Working Party points out, an obligation to take effective privacy enhancing measures,

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 23 of 30</p>
---	---	---

i.e. privacy identity management measures, may be imposed to the electronic communications service provider⁵².

In some other cases, however, it is possible that RFID technology is used without consent, for instance for the patients' management and treatment within a hospital or for the monitoring of prisoners. Especially, in the latter case as well as in all cases of obligatory use of RFID tags imposed by law for the public interest (i.e. EU passports) it should be examined whether each specific RFID application is necessary, proportional and does not violate human's dignity.


Finally, consent may not legitimate a processing where this is not deemed to be given free or where the processing is deemed to be unfair. For instance, in the employment context consent specific safeguards shall be taken prior to the use of RFIDs technology which might lead to the surveillance of the workers. Besides this, a permanent surveillance is not deemed to be fair as this might occur with RFIDs which can provide location / movement data of the employees at a permanent basis. As Article 29 Data Protection Working Party points out, the processing of employees' location data can be justified where this is necessary for the security of the transport of people or objects or the better allocation of resources in scattered locations but not for the mere monitoring of employer's⁵³.

4.3.2 Data minimisation and purpose limitation principle

The data minimisation and purpose limitation principle within the context of RFID systems (tag & reader) means the data controller shall configure the systems so that only the necessary data are collected and further processed for the purpose of the processing. If for instance, tags are deployed within manufacturing or the logistics chain, these tags shall not process personal data unless necessary for the security of the production or the transportation of the goods. Should personal data be processed these shall be limited to the absolute necessary and not, for instance, allow for a permanent surveillance of the employers. Furthermore, within the purpose limitation principle it shall be ensured that the data are not further processed for other purposes than those for which the data are collected. For instance, data collected for the improvement of manufacturing, logistics processes or for the customer service shall not be used for the monitoring of the behaviour and location of the employees. For law enforcement purposes data shall be processed only within the limits and requirements as laid down by the national jurisdictions (see also article 13 Directive 95/46/EC).

⁵² Article 29 Working Party, Opinion on the use of location data with a view to providing value-added services, 25/11/2005, WP 115, p. 6 available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf

⁵³ Article 29 Working Party, Opinion on the use of location data with a view to providing value-added services, 25/11/2005, WP 115, p. 10 available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 24 of 30</p>
---	---	---

4.3.3 Information requirements and data subject's rights

As far as processing by RFID technology is based on data subject's informed consent and also within the context of data subject's right to be informed –even where the processing is not based on informed consent- specific measures are discussed as to the proper information.

Collection of data under informed consent means covert capture of information should not be permitted. Informed consent is recognised as the primary tool available to individuals to protect their privacy from technological invasion. In a world of ubiquitous data-processing, here per radio frequency transmitted, where the data subject does not even notice that his/her personal data are in process and consequently cannot follow the different stages of the procedure, informed consent becomes a crucial point. The same thoughts apply also to the data subject's right to be informed.


There are several papers dealing with the proper manner to comply with the information requirements⁵⁴. Accordingly, the data controller shall inform the data subject of the identity of data controller, whether a product contain a RFID tag, whether this tag may be read by which readers, incl. publicly available readers, of the possibility that this information is captured without data subject's active involvement, which information is read and further processed, for what purposes, whether this information is further transferred to third parties and about data subject's rights to access and rectify its personal data. To this end, technical and organisational measures shall be taken, as for instance adequate pictograms when entering a RFID tagged place, written information on the processing capabilities and activation stage of the tags, the presence of the readers etc. Depending on whether the processing is based on data subject's informed consent it is also required that the data controller shall inform the data subject about the technical possibilities to deactivate the tags. It is, finally, required that the data subject, notably where the processing is based on the consent, shall be granted the right not to be discriminated by deny of use of this technology. For instance, the data subject shall have the option to return a product from which the RFID tag was removed or to travel without using the RFID automated toll-system collection⁵⁵.

In this respect the data subject's rights, i.e. the access and the rectification or even deletion of the data, if such data are incorrect or where the processing is based on consent, shall be enabled by technical means. For instance, retailers shall provide for adequate means where consumer may follow the processing of its data and be able to deactivate the tags. To this end, it is also required that the data controller shall offer the technical means to deactivate or remove securely the tags or even that the tags shall offer the technical possibility to switch them off or on⁵⁶. There are,

⁵⁴ *Article 29 Working Party*, WP 105, Working document on data protection issues related to RFID technology, January 19, 2005, sec. 4.2, 5.2, available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf ; Committee established by standards New Zealand on behalf of GS1 NZ, EPC/RFID Consumer Protection Code of Practice; Italian Data Protection Authority, Smart (RFID) Tags: Safeguards applying to their use, March 2005, available at: <http://www.garanteprivacy.it/garante/doc.jsp?ID=1121107> ;

⁵⁵ *German Association for the promotion of the public and not-public data traffic*, (Verein zur Foerderung des oeffentlichen und nicht oeffentlichen Datenverkehrs e.V.) (FOEBUD), available at: <http://www.foebud.org/rfid/positionspapier.pdf>

⁵⁶ See footnote 53 & 54.

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 25 of 30</p>
---	---	---

however, authors opining the data controller is not obliged and responsible for the removal of passive tags which do not contain themselves personal data – from the moment the customer leaves the store. Should the tag be read by an unauthorised person – under the condition that the tag data are deemed to be personal data-, this shall be sanctioned only on the basis of the unauthorised access to and / or collection of personal data⁵⁷. Though, this opinion does not put this obligation in the light of the data controller’s data security obligation.

It is thus worth mentioning that RFID technology poses very urgent the technical features which shall serve the transparency of the processing and exercise of data subjects’ rights. It also poses very urgent issues related to ubiquitous computing for which current data protection legislation might not fully address these issues. As a result, these issues shall be further examined in at EU level consistent manner, notably the exact application of data controller’s obligations to the RFID technology, the need to specify the obligations in sector applications and if necessary the need for more detailed provisions addressing the specific characteristics of the technology.


4.3.4 Technical and organisational measures for data security and exercise data subject’s rights

As aforementioned, technical and organisational measures are proposed for the proper exercise of the right to information, the right to access, rectify and delete the data. The same measures may apply also within the data controller’s obligation to safeguard the data security. Data security encompasses the aspects of data integrity and accuracy, data confidentiality and data availability. For instance, the possibility to check and modify or erase some data may serve both the principle of the data accuracy as laid down in the Directive 95/46/EC, the exercise of the respective data subject’s rights and also data controller’s data security obligation as laid down in article 17 of Directive 95/46/EC. Similarly, technologies deployed for the confidentiality of the data may also serve the need for data integrity. For instance, encryption may not be only used as counter-measure to protect the confidentiality but may also prohibit the unauthorised data alteration if so configured.

In the following we present some of the major technical measures envisaged in the context of RFID technology and data protection. However, some of them, such as the encryption for the purposes of confidentiality and integrity, may also serve the protection of other goods. For instance, where a patient ID is stored on the tag, on the basis of which the hospital personnel may access patient’s medical record, it is of utmost importance that the patient ID may not be altered and lead to wrongful information and, consequently, may affect patient’s health.

Kill-Order Solution: The most common solution to the RFID privacy problem is to disable the tag at the point of sale by sending a "kill" command, the so called kill solution. For example a supermarket might use RFID tags to facilitate inventory management and monitoring of shelf stocks. To protect consumer privacy, checkout employees would "kill" the tags of purchased goods; no purchased goods would active RFID tags. Even though deactivated tags cannot be read anymore, this solution has several technical and economic drawbacks: This cannot be

⁵⁷ *Westerholt von Graefin, M. / Doering, W., Datenschutzrechtliche Aspekte der Radio Frequency Identification, in: CR 2004, pp. 710 (715).*

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 26 of 30</p>
---	---	---

implemented to all tag functions, for instance to library book tags or toll collection systems. Moreover one has to consider the customers inability to control the success of deactivation. Nevertheless deactivation of the tag at the point of sale ensures the privacy of the consumer (if the tag is properly killed) but it prevents post-purchase services such as warranty, access to product support, advanced recycling and waste management, advanced home applications, and all the other applications in the two last phases of the RFID-tag life cycle.

The physical shielding of a tag: Tags may be shielded with an aluminium sheet in order to protect unauthorised reading where the tag is made mandatory, as for instance in the EU passports. However, this technology is not suited for clothes and other objects being worn. It is also opined, the physical shielding does not provide for protection should the tagged item be open, as for instance this may happen with a passport in data subject's bag.

The blocker tag: While an ordinary tag is a simple, cheap passive device intended as an "electronic bar-code" for use in supply-chain management, a blocker tag is a cheap passive RFID device that can simulate many ordinary RFID tags simultaneously. When carried by a consumer, a blocker tag thus blocks RFID readers. It can do so universally by simulating all possible RFID tags. Or a blocker tag can block selectively by simulating only selected subsets of ID codes, such as those by a particular manufacturer, or those in a designated "privacy zone"⁵⁸.

Encryption Solution: Encryption of the data being transmitted is one method of protecting against anyone eavesdropping on communication via the air interface. It is a way of insuring that information namely personal data carried in an RFID tag will not be read by an unauthorised reader⁵⁹. One should certainly take into account that not all of the tags support strong cryptographic procedures which exclude them from being strong protected from unauthorised retrieving of data. At the moment even specialists⁶⁰ insist on storing content data in a backend database and just a unique number on the tag that will be associated to the database as the most effective way of avoiding eavesdropping.

User-model solution: This solution implies that users exert full control over RFID tags by means of appropriate authentication mechanisms. Objects do not a priori respond to network requests⁶¹. Instead the user self-initiates the use of intelligent services if they are available and useful in the respective context. The context decision when and how the use of tags is appropriate is thus taken by the object owner. This model can induce a high level of control with users since the intelligent infrastructure cannot act autonomously. RFIDs shall not generally be destroyed but designed to be reactivated later e.g. for handling warranty cases. To ensure privacy the RFID tags shall be sent to a dormant mode at the point of sale. The tags could then be re-awakened by a codeword. This codeword shall be automatically generated by the store⁶².

Privacy Bit (proposal by RSA security): It represents a simple and cost-effective way of mitigating the problems of RFID privacy while preserving the consumer benefits of RFID. A privacy bit is a single logical bit resident in the memory of an RFID tag. It indicates the privacy


⁵⁸ See *Juels, Rivest, Szydlo*, The Blocker Tag: Selective blocking of RFID tags for consumer privacy, p. 1.

⁵⁹ See *Jonathan Collins*, Tag Encryption for Libraries, available at: <http://www.rfidjournal.com/article/articleprint/1027/-/1/1>.

⁶⁰ See Security aspects and prospective applications of RFID systems, BSI, p. 46, available at: http://www.bsi.de/fachthem/rfid/RIKCHA_englisch_Layout.pdf.

⁶¹ *Spiekermann, Sarah*, Perceived Control: Scales for Privacy in Ubiquitous Computing, p. 4, download in: <http://www.wiwi.hu-berlin.de/iwi/internetoeconomie/content/de/publikationen/index.php>.

⁶² See *Berthold, Oliver*, Datenschutzgerechte RFID-Technologie, p 2, under: <http://coltrane.wiwi.hu-berlin.de/interval/publications/dateien/1113385510-sicherheit2005.pdf>

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 27 of 30</p>
---	---	---

properties of the tag. A tag's privacy bit might be *off*, indicating that the tag is freely subject to scanning, or it may be *on*, indicating that the tag's information cannot be scanned. The operation of changing the privacy bit should naturally require authorization via an RFID-tag-specific PIN. The RFID readers will be able to scan the tags either private or public: if the privacy-bit is on, only private scanning will be permitted.

As a result, the security measures shall be further considered and evaluated under the scope of the particular threats raised by each application, the nature of goods to be protected (personal data, personal data related to health etc) taking also into account the related costs⁶³. Another important point is the design of RFID technology in a privacy and security friendly manner. Therefore, the implementation of privacy and security features in respective ISO standards and RFID protocols is currently broadly discussed.

4.4 Legislative measures


Up to now there are no legislative measures taken in view of RFID technology. National Data Protection Authorities and the Article 29 Data Protection Working Party are working mainly on appropriate interpretation of existing legal framework whilst the legal scholarship examines whether specific legal provisions may apply. For instance, it is pointed out that the article 6c of the German Federal Data Protection Law (BDSG) is partly applicable to RFID tags, notably where the tag does not directly process or store personal data, as for instance passive tags containing only the product ID⁶⁴.

In the US there are initiatives on passing specific legislation regulating the use of RFID technology in businesses, schools, governments and other applications. This initial response varies widely from state to state: Utah recently reviewed its laws on unauthorised access to networks and added wireless networks as it previously only addressed wire line networks: it clarifies that computer crimes laws apply to wireless networks. Virginia's law authorises research relating to methods of electronic toll collection. Also provides that data generated by automated electronic toll-collection systems on use of toll facilities can only be disclosed when so required by order of a court. Wyoming authorises tele-pharmacies to use automated inventory control including radio frequency tags. In many other states there exist draft legislation on RFID technology, which sometimes just seek to require only labelling and notice that RFID is in use, while in other cases like the California's approach would most tightly regulate the technology itself, including prohibitions of certain applications and technology-specific security requirements⁶⁵.

⁶³ See *German Federal Authority for Information Systems Security* (Bundesamt für Sicherheit in der Informationstechnik), *Security Aspects and Prospective Applications of RFID Systems*, 2005, section 7.8, available at: http://www.bsi.bund.de/fachthem/rfid/RIKCHA_englisch.pdf

⁶⁴ *Westerholt von Graefin, M. / Doering, W.*, *Datenschutzrechtliche Aspekte der Radio Frequency Identification*, in: CR 2004, pp. 710 (714); *Lahner, Claus Mauricio*, *Anwendung des par. 6c BDSG auf RFID*, in: DuD 2004, p. 723

⁶⁵ US privacy legislation related to RFID available at: <http://www.ncsl.org/programs/lis/privacy/rfid05.htm>

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 28 of 30</p>
---	---	---

5 Conclusions / Recommendations

First conceived in 1948, Radio Frequency Identification has taken many years for the technology to mature to the point where it is sufficient affordable and reliable for widespread use⁶⁶. The use of RFID technology for different purposes in increasingly more sectors and in various applications of everyday life may benefit business, individuals and public services. With increasing use comes increasing concern on the protection of privacy and possible of the right to personality and human dignity. RFID applications pose a series of legal issues concerning the privacy protection and data protection:

In what extent and from which moment RFID tags contain personal data?


What are the exact obligations of the data controller?

What are the security measures to be taken by the data controller? Is the data controller obliged to provide for technical means to deactivate or remove the tags?

Is the data controller responsible for any unauthorised access to the information contained in the tags even if this information is merely indirectly related to the data subject?


Clearly there is considerable work to be undertaken before RFID becomes as pervasive as bar codes. In authors opinion, the emerging technology shall be further followed in order to find out its real potential and consequently the respective risks. Further research and consultation at EU level shall be encouraged in order a) to work-out adequate practices for each sector of application, b) promote the implementation of privacy enhancing technologies at the design level, c) find out possible gaps and the need for complementary legislative measures.

⁶⁶ See *C.M. Roberts*, Radio Frequency Identification (RFID), *Computer & Security*, 2006, p. 18

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 29 of 30</p>
---	---	---

6 References

- Annual Report of the Berliner DPA, 2004, available at: http://www.datenschutz-berlin.de/jahresbe/04/teil4_4.htm
- Article 29 Data Protection Working Party*, Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology, WP 111, 28 September, 2005, available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf
- Article 29 Data Protection Working Party*, Working document on data protection issues related to RFID technology, WP 105, January 19, 2005, available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf
- Article 29 Working Party*, Opinion on the use of location data with a view to providing value-added services, 25/11/2005, WP 115, p. 6 available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf
- Auto-ID Centre (2003)*: Technical report 860MHz-930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1., MIT, USA, available at: http://interval.hu-berlin.de/downloads/rfid/chipklassen/4_candidate_recommendation_1_0_1.pdf
- Balch / Feldman / Wilson*, Assessment of a RFID System for Animal Tracking, The BORG Lab, Georgia Institute of Technology, Atlanta, Oct. 1 2004, available at: <http://www.cc.gatech.edu/~storm/Feldman2004TR.pdf>
- Berthold, Oliver*, Datenschutzgerechte RFID-Technologie, p 2, under: <http://coltrane.wiwi.hu-berlin.de/interval/publications/dateien/1113385510-sicherheit2005.pdf>
- Borchers*, Kritik am Reisepass, c't 21/2005, available at: <http://www.heise.de/ct/05/21/060/>
- Collins, Jonathan*, Tag Encryption for Libraries, available at: <http://www.rfidjournal.com/article/articleprint/1027/-1/1>
- Committee established by standards New Zealand on behalf of GS1 NZ*, EPC/RFID Consumer Protection Code of Practice
- Council Regulation 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385, available at: http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00010006.pdf
- Council Regulation 644/2005/EC of 27 April 2005 authorising a special identification system for bovine animals kept for cultural and historical purposes on approved premises as provided for in Regulation (EC) No 1760/2000 of the European Parliament and the Council, 2005, OJ 107, p. 18
- EPCglobal „Electronic Product Code“ available at: www.epcglobalus.org/Network/Electronic%20Product%20Code.html
- Erdos, Marlena*, RFID and authenticity of goods, p. 137, in: *Simson Garfinkel / Beth Rosenberg*, RFID Applications, Security and Privacy, 2006
- Garfinkel, Simson / Rosenberg, Beth*, RFID Applications, Security and Privacy, 2006, p. 533
- German Association for the promotion of the public and not-public data traffic*, (Verein zur Foerderung des oeffentlichen und nicht oeffentlichen Datenverkehrs e.V.) (FOEBUD), available at: <http://www.foebud.org/rfid/positionspapier.pdf>
- German Federal Authority for Information Systems Security* (Bundesamt für Sicherheit in der Informationstechnik), Security Aspects and Prospective Applications of RFID Systems, 2005, available at: http://www.bsi.bund.de/fachthem/rfid/RIKCHA_englisch.pdf
- Hennig / Ladkin / Sieker*, Privacy Enhancing Technology Concepts for RFID Technology Scrutinised, p.1
- International Conference of Data Protection & Privacy Commissioners*, Resolution on Radio-Frequency Identification, (Nov. 20, 2003) p. 2, available at: <http://www.privacyconference2003org/resolutions/res5.DOC>
- Italian Data Protection Authority, Smart (RFID) Tags: Safeguards applying to their use, March 2005, available at: <http://www.garanteprivacy.it/garante/doc.jsp?ID=1121107>
- Juels / Molnar / Wagner*, Security and Privacy Issues in E-Passports, IEE SecureComm 2005, available at: www.cs.berkeley.edu/~dmolnar/papers/papers.html
- Juels / Rivest / Szydlo*, The Blocker Tag: Selective blocking of RFID tags for consumer privacy, p. 1

 <p>IST-2-004252-SSA</p>	<p style="text-align: center;">15 Report on Legal Issues of RFID Technology</p>	<p>Rev. 0 Issue Date.: 16/05/2006 Page 30 of 30</p>
---	---	---

Keuleers, Ewout, Reconciling RFID technology with data protection principles, *Droit Nouvelles Technologies*, April 2005, p. 2

Lahner, Claus Mauricio, Anwendung des par. 6c BDSG auf RFID, in: *DuD* 2004, p. 723

Langheinrich, Die Privatsphäre im Ubiquitous Computing - Datenschutzaspekte der RFID-Technologie, available at: <http://www.vs.inf.ethz.ch/publ/papers/langhein2004rfid.pdf>

Langheinrich, Privacy by Design-Principles of Privacy-Aware Ubiquitous Computing, p. 7 available at: <http://www.vs.inf.ethz.ch/publ/papers/privacy-principles.pdf>

Molnar / Wagner, Privacy and Security in Library RFID issues, practices and architectures, CCS'04, October 25-29 2004, Washington, DC, USA, p. 210, available at: <http://www.cs.berkeley.edu/molnar/library.pdf>

Mueller, Juergen, Ist das Auslesen von RFID-Tags zullaessig?, in: *DuD* 2004, pp. 215

Rieback, Crispo, Tanenbaum, Is your cat infected with a computer virus?, 2006, available at: www.rfidvirus.org/papers/percom.06.pdf

Roberts, C.M., Radio Frequency Identification (RFID), *Computer & Security*, 2006, p. 18

Saeltzer, Sind diese Daten personenbezogen oder nicht?, *DuD* 2004, p. 218

Schulzki / Haddouti, Neue Reisepässe: Mit Sicherheit teuer, available at: <http://www.sicherheit-heute.de/index.php?cccpage=Verkehr>

Spiekermann, Sarah, Perceived Control: Scales for Privacy in Ubiquitous Computing, p. 4, download in: <http://www.wiwi.hu-berlin.de/iwi/internetoekonomie/content/de/publikationen/index.php>

U.S. Food and Drug Administration, Combating counterfeit Drugs, A Report of the Food and Drug Administration, February 2004, available at: www.fda.gov/oc/initiatives/counterfeit/report02_04.html

Westerholt von Graefin, M. / Doering, W., Datenschutzrechtliche Aspekte der Radio Frequency Identification, in: *CR* 2004, p. 710

Yoshida, Euro Bank Notes to Embed RFID Chips by 2005, *EETimes*, 19.12.2001, available at: <http://www.eetimes.com/story/OEG20011219S0016>