CyLaw-Report XXIV - Conference Speeches to the „Internet of Things“ in 2008 (Version 2.0)

ISSN 1867-1969

TECHNISCHE UNIVERSITÄT DARMSTADT

In 2008 Cylaw (Öffentliches Recht) at the University of Technology, Darmstadt, Germany, rendered two speeches at international conferences in Zürich, Switzerland and Nizza, France.

(I) The first speech was given at the "First International Conference, Internet of Things 2008" in Zurich, Switzerland in March 2008.[1] The conference was organized by MIT, University of St. Gallen and ETH Zurich. The Proceedings are published in Springer Lecture Notes on Computer Science (LNCS) 4952[2].

(II) The second speech was given at the "Internet of Things – Internet of the Future" in Nizza, France in October 2008. The conference was organized by the French Presidency of the European Union (French Ministry of Higher Education and Research, the Ministry of Economy, Industry and Employment, and the Secretary of State for the Development of the Digital Economy, in cooperation with the Directorate General Information Society and Media of the European Commission.)

(I) Zürich: Radio Frequency Identification Law Beyond 2007 - Answers to 6 Questions

"Ladies and Gentlemen,

The agenda for the next twenty minutes is "RFID Law beyond 2007" and I want to follow up on it with two concurring perspectives:

- the "RFID" law perspective of it's World Pioneer State – the United States of America – and
- the data protection law perspective of it's World Pioneer Regions – the European Community and the Federal Republic of Germany.

This twofold approach and the answers to six questions are the red thread running through my presentation. Be informed that I am aware of your criticism: Too much for twenty minutes! Nevertheless, please join me in a jurisprudential par force ride and a courageous endeavor. Hopefully, I can provide you with an overview of the legal challenges and a structure for further deliberation, lobbyism and criticism.

(1) What is Law?

The first question that arises is: What is Law? Law is the product of legislature, of judiciary and of administration. In 2007, we could state that "RFID" Law is in the

[1] For more information about the conference see www.iot2008.org (04/14/08).

[2] Floerkemeier, C./ Langheinrich, M./ Fleisch, E./ Mattern, F./ Sarma, S.E. (Eds.), "The Internet of Things", Springer LNCS 4952, 2008.

status of pending legislation – from a privacy point of view we have no court or administrative decisions, yet. The World Pioneer of "RFID" Law is the USA and in September 2007 – when I submitted my article – 18 states discussed Senate-, House- or Assembly Bills.[3] For these American states, "RFID" already poses questions at the legislative bodies, whereas in the European Community and in Germany – the data protection legal pioneers – the law makers still deliberate whether new law for "RFID" is necessary.[4] When we think about new or traditional[5] law for "RFID", we should define "RFID" (second question).

(2) What is "RFID"

Someone suggested that "RFID is not RFID – there exists no common definition and one may realize that mainly the "air" protocol ties together all the different technologies". From a legal perspective this is true as can be demonstrated by reading section 52.7. h (1) of the Californian Civil Code:

"Identification device: means any item, application, or product that is passively or actively capable of transmitting personal information including, but not limited to devices using radio frequency technology."[6]

So we deal with a technology – you may call it "RFID" (Radio Frequency Identification)[7], "SRD" (Short Range Devices)[8] or "NFC" (Near Field Communication)[9]

---

[3] See the overview table in Schmid, V. "Radio Frequency Identification Law beyond 2007", in: Floerkemeier, C./ Langheinrich, M./ Fleisch, E./ Mattern, F./ Sarma, S.E. (Eds.), „The Internet of Things", Springer LNCS 4952, 2008, p. 202.

[4] The European Commission is preparing a recommendation (Art. 249 Sec. 5 EC) on RFID law. It has opened an online consultation until April 2008 http://ec.europa.eu/information_society/policy/rfid/index_en.htm (04/14/08). Such a recommendation would not be legally binding but might be a tool for the interpretation of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281, 23/11/1995 P. 0031 – 0050) and for national data protection law, compare C-322/88, judgment of the court of justice of 12/13/89, Grimaldi vs. Fonds des maladies professionnelles, S. I-4407 (4419 ff.). The German government is well informed about the challenges for RFID law but does not want to take action in 2008, see BTDrucks 16/7891, http://dip21.bundestag.de/dip21/btd/16/078/1607891.pdf (04/14/08).

[5] Cyberlaw is the law dividing rights and obligations, chances and risks in Cyberspace. From a Cyberlaw perspective, traditional law is existing law governed by legal traditions that might not similarly apply to Cyberspace.

[6] See the official website for Californian state law http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=civ&codebody=&hits=20 (07/06/08).

[7] See Gillert, F./Hansen, W.-R., "RFID for the Optimization of Business Processes", pp. 102—109.

[8] see Ronzani, D., "Why Marketing Short Range Devices as Active Radio Frequency Identifiers Might Backfire", in: Floerkemeier, C./ Langheinrich, M./ Fleisch, E./ Mattern, F./ Sarma, S.E. (Eds.), „The Internet of Things", Springer LNCS 4952, 2008, p. 216 f., citing Kern, C., "Anwendungen von RFID-Systemen", 2008, Finkenzeller, K., "RFID Handbuch", 2006 and Glover, B./ Bhatt, H., "RFID essentials", 2006.

[9] See Gillert, F./Hansen, W.-R., "RFID for the Optimization of Business Processes", pp. 176—178.

etc. – a technology that is passively or actively capable of contactlessly transmitting information. Hence let us put "RFID" in quotation marks. Example given in section 219 of the New York Assembly Bill 222 (2007):

"Radio Frequency Identification means any technology that uses radio waves or other wireless means to transmit identifying information between a tag, badge or other device and a reader without physical contact."[10]

(3) Transmission of non-personal information – The Bag Paradigm?

From a legal perspective the third question is whether this technology transmits personal information (personal data) or non-personal information. An example for non-personal information is the Apenheul Bag Scenario:

> "The Apenheul (…) is a zoo specialized in all kinds of apes and monkeys. An outstanding feature of the park is the opportunity for some kinds of monkeys to move freely through the crowd of visitors. Curious as they are, the monkeys often try to open visitors' bags in hope of a free lunch. The park therefore introduced the "Monkey bag", a green bag with an extra clip lock which monkeys cannot open. The bag is obligatory, which is enforced by the receptionists providing the bag at the entrance of the park […] Aside from this security reason for implementing the bag, the department of marketing added a marketing feature to the bag: scanning visitors movements through the park through an active RFID sewn into the bag […] The Monkey Bag RFID has a marketing function: how do visitors move through the park and how can the flow of people be optimized. […]"[11]

Clearly the "Bag Scenario" complies with traditional information privacy law in the USA, Europe and Germany, because no personally identifiable information is involved.

"The visitors remain unanimous, are not traced real time and do not suffer any consequences as a result of the data they provide."[12] Moreover, it is evident that such tracing should not be legally prohibited. Nevertheless – in my opinion – future "RFID law" should incorporate a *principle of transparency* for non-personally identifiable information retrieved by RFID (the "Bag Paradigm" developed here). Consequently the marketing department of the zoo would be forced to inform the visitors about the active RFID *(duty to information)*. It is then a matter of provider choice

[10] Section 219 (1 E.) General Business Law as in New York 2007, Assembly Bill 222 ("RFID Right to Know Act").
[11] European Technology Assessment Group, "RFID and Identity Management in Everyday Life", 2006, http://www.itas.fzk.de/eng/etag/document/hoco06a.pdf (04/14/08), p.21.
[12] Ibid., p. 22.

- whether the marketing department also offers bags without RFID for those not wanting active RFIDs monitoring their movements

and it is a matter of consumer choice

- whether they visit the zoo if the marketing department doesn't offer this choice.

Be assured, my academic ivory tower existence doesn't ignore the criticism arising in the audience right now. "RFID" law will be a matter of controversy in the years to come and I am aware of a very valid criticism: some of you will ask how I can prove that there is at least one other person caring about RFID monitoring her movements anonymously. In the age of "facebook" and the publication of personal diaries as weblogs – why should anyone care if the provider of a service – here the zoo – tries to improve his product by monitoring demand streams anonymously? Even more so there is a potential benefit for consumers: the provider tries to improve the service. And I have to concede: in 2008 I have no statistics or opinion polls of people supporting the commandment of a duty to information for the Bag Scenario. Nevertheless I challenge you in my article with the postulation of new law for the Bag Scenario, at least for Germany. The simple reason being, that I regard my consumer behavior and criticism as an object of value. If the zoo owner is interested in my behavior and my criticism he should ask. He should give me the information enabling me to decide

- whether I take the bag supporting such marketing strategies , or
- whether I don't take the bag, wanting to be a kind of visitor sphinx in my spare time.

The Bag Paradigm is a result of my scientific research and not a legislative scenario of the present.

(4) Transmission of personal information – the Electronic Product Code Scenario (EPC)?

The fourth question is: Apart from the bag scenario, how many "RFID" scenarios involving (personal) information do we have? In 2005, I have laid groundwork for four other scenarios differing whether "RFID" is used to

- *monitor products* (Electronic Product Code scenario = EPC),
- *monitor animals* (Real-time authentication and monitoring of animals scenario = RTAMA)
- *monitor persons* (Real-time authentication and monitoring of persons scenario = RTAMP)[13] or
- *collect data for profiling purposes* (Aggregation scenario = AGG)[14].

[13] Schmid, V., "Mastering the Legal Challenges", in: Heinrich, C. "RFID and Beyond, Growing Your Business Through Real World Awareness", Wiley Publishing Inc., Indianapolis, USA (2005), pp. 193—207.

From a privacy point of view the critical issue is, whether these scenarios contain personal information. Traditionally privacy law concentrates on the protection of personal data[15] and wherever personal data is involved in the "RFID" communication and information process, existing law regulates the use of "RFID". This is at least true for the data protection pioneers – the European Community and Germany[16] – and therefore the RTAMP-Scenarios, e.g. the monitoring of school children, students, ill and disabled persons, and the AGG-Scenarios, e.g. the EPC scenarios combined with credit card information, would be covered there by existing law.

In summary: in the European Community and in Germany we do not need new law for "RFID" scenarios involving personal data (personal information). Only one caution is to be added for data protection law specialists in the audience: this denial of the necessity of new law depends on the conviction that you are satisfied with the efficiency and enforcement of the existing data protection law.[17]

The thesis that traditional law is sufficient to meet the challenges of "RFID" personal data scenarios is not equally true for the USA who has a different privacy (law) culture to Europe and Germany. However the RTAMP-Scenario – prohibition of subcutaneous implanting an identification device – is a legal reality in three States of the USA: the aforementioned Californian Civil Code of 2007 and laws in North Dakota and Wisconsin. Section 52.7. (a) Californian Civil Code reads as follows:

"Except as provided in subdivision (g) a person shall not require, coerce, or compel any other individual to undergo the subcutaneous implanting of an identification device."[18]

---

[14] Schmid, V. "Radio Frequency Identification Law beyond 2007", in: Floerkemeier, C./ Langheinrich, M./ Fleisch, E./ Mattern, F./ Sarma, S.E. (Eds.), "The Internet of Things", Springer LNCS 4952, 2008, p. 206.

[15] See Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, of June 20th 2007, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf (04/14/08)

[16] See Holznagel, B./Bonnekoh, M., "Rechtliche Dimensionen der Radio Frequency Identification", in: Bullinger, H.-J./ten Hompel, M., "Internet der Dinge", 2007, pp. 365—420; Hansen, W.-R./Gillert, F., "RFID for the Optimization of Business Processes", pp. 197—207; Schmitz, P./ Eckhardt, J., "Einsatz von RFID nach dem BDSG – Bedarf es einer speziellen Regulierung von RFID-Tags?", CR 2007, pp. 171—177.

[17] EU Commission, "Flash Eurobarometer survey on Data Protection – Citizens' perceptions", January/February 2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf (07/07/2008); EU Commission, "Flash Eurobarometer survey on data protection – Data controllers' perceptions", January/February 2008, http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf (07/07/2008); wik-Consult/RAND Europe, CLIP/CRID/GLOCOM, "Comparison of Privacy and Trust Policies in the Area of Electronic Communications", 2007, http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/final_report_20_07_07_pdf.pdf (07/07/2008).

[18] See the official website for Californian state law http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=civ&codebody=&hits=20 (07/06/08).

Perhaps it would be interesting to pursue the RTAMP-Legislation further. The title of the conference “Internet of Things” however forces me to hurry on to the EPC-Scenario. The question whether the Electronic Product Code Scenario involves personal information is a matter of controversy in Germany.[19] It depends on how we define “personal information” (personal data). It depends on whether we determine that the reading of wearable passive RFID tags containing a unique identifier for products such as clothes or groceries is “personal information” (personal data) about the person wearing these clothes or carrying these groceries. If you meet me on the street and don’t know Viola Schmid: Is it “personal information” (personal data) that I wear a suit from … and underwear from …. and carry a bag with groceries from …?[20] Undoubtedly, this is a topic for further papers but instead of presenting my own opinion I want to continue with an overview of the pending “RFID” legislation in the United States in 2007. The reason is that one of the five categories of this “law in motion”– the so called “Right to Know” legislation[21] – tries to find the answer for the duty to information and deactivation of “RFID” with leaving the retail store. This “Right to Know” legislation is only one of five kinds of “RFID” legislation.

(5) Five Kinds of RFID Legislation

These five kinds of legislation can be differentiated:[22]

Right-to-Know-legislation,
Prohibition-legislation,
IT-Security-legislation,
Utilization-legislation and
Task-Force-legislation.

[19] Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27.10.2006, http://www.bfdi.bund.de/cln_007/nn_1207020/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DSBundLaender/72DSK-RFID,templateId=raw,property=publicationFile.pdf/72DSK-RFID.pdf (04/14/08).

[20] Hansen, W.-R./Gillert, F., “RFID for the Optimization of Business Processes”, p. 103: “Electronic Product Code differs from European Article Number by having a serial number in addition to the manufacturer and product (class) numbers. The serial number allows individual objects to be identified uniquely”.

[21] Section 219 General Business Law as in New York 2007 Assembly Bill 222 (“RFID Right to Know Act”).

[22] See Schmid, V. “Radio Frequency Identification Law beyond 2007”, in: Floerkemeier, C./ Langheinrich, M./ Fleisch, E./ Mattern, F./ Sarma, S.E. (Eds.), “The Internet of Things”, Springer LNCS 4952, 2008, p. 202, 207 ff.

The following table shows legal “RFID” activity in 18 states in the USA in 2007 (SB = Senate Bill; AB = Assembly Bill; HB = House Bill):

State	Right-To-Know-Legislation	Prohibition-Legislation	IT-Security-Legislation	Utilization-Legislation	Task-Force-Legislation
Arkansas	-	SB 195	-	SB 183	SB 846
California	SB 388	SB 29 SB 31	SB 30	-	-
Georgia	-	HB 276	-	-	-
Massachusetts	HB 261 SB 159	-	-	-	-
Michigan	-	HB 4133 HB 5061 HB 5091	-	HR 51	-
Missouri	SB 210 SB 13	-	-	-	-
New Hampshire	HB 686		-	HB 269	-
New Jersey	AB 3996	SB 1866	AB 3015	AB 4061	-
New York	AB 222 AB 261				AB 225 SB 165
North Dakota	-	SB 2415	-	-	-
Oregon	HB 3277	-	-	-	-
Pennsylvania	HB 993	-	-	-	-
Rhode Island	-	SB 474	-	-	-
Tennessee	HB 2190	-	-	-	-
Texas	-	HB 1925	SB 2027	SB 574 HB 1308 HB 2990	-
Virginia	HB 2086	-	-	-	-
Washington	HB 1031 SB 6020			HB 1133 SB 5366	-
Wisconsin	-	AB 141 AB 488	-	-	-

On my parforce ride I only choose the hurdles of (a) “Right-to-Know” Legislation and (b) “Prohibition” Legislation.

(a) “Right-to-Know” legislation denotes initiatives – mainly in Electronic Product Code scenarios – demanding that the customer be informed. Furthermore, the customers shall be able to deactivate or remove the tags after purchase, so that after leaving the retail shop reading attacks are unsuccessful.[23] As the table shows you, this “Right to Know” legislation is an idea that in 2007 is widespread in the legislature of the American states. Furthermore it is a postulate of the European Article 29 Data Protection Working Party[24] and in 2008 rejected by the German government[25]. If “Right-to-Know” legislation will be enacted in 2008 – e.g. in New York – the answer to the EPC scenario will be: at least in New York with leaving the retail store consumers are protected against reading attacks of Electronic Products Codes of products they are wearing or carrying. Consequently – where “Right to Know” legislation is enacted – we don’t need to answer the question whether personal data is involved.

(b) The already mentioned RFID laws in North Dakota, Wisconsin and California are examples for “Prohibition” legislation in “Real-time authentication and monitoring of persons” scenarios (the so called RTAMP scenarios). Hence – in these states – no one may induce the subcutaneous implanting of identification devices. I want to emphasize that this prohibition legislation is law in existence and not only a legal initiative as the four other categories.

For the legally experienced, I concede that it is perhaps a matter for discussion which importance state law has in the USA. However the online “Right-to-Know-Recommendation” consultation of the European Commission[26] demonstrates the transatlantic parallelism of “RFID” legislative ideas. In summary it can be said that the table proves the validity of my categorization. And the question that follows is evident:

(6) What are the arguments in these legislative proceedings in 2007 and 2008?

Mainly three lines of argumentation can be discerned:

We do not need law. “Self regulatory practices” of the economy – such as the Electronic Product Code Guidelines[27] – are sufficient.

[23] Schmid, V., “Radio Frequency Law in a Global Perspective”, in: Hansen, W.-R./Gillert, F., “RFID for the Optimization of Business Processes”, pp. 215—218.

[24] Article-29-Group: Working document on data protection issues related to RFID technology (10107/05/EN WP 105) (2005), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf (04/14/08).

[25] BTDrucks 16/7891, http://dip21.bundestag.de/dip21/btd/16/078/1607891.pdf (04/14/08).

[26] http://ec.europa.eu/information_society/policy/rfid/index_en.htm (04/14/08).

[27] See the official website of EPCglobal http://www.epcglobalinc.org/public/ppsc_guide/ (04/07/08).

Firstly: As a jurisprudent, I am biased. I think that the questions,

- whether an employer can request of his employees the implantation of "RFID" (RTAMP Scenario) or
- whether "RFID" tags attached to products have to be deactivated or removed upon leaving the retail shop (EPC Scenario)

merit a legal answer. I think that legislation – and not judiciaries – should find an answer to the question whether employers may coerce their employees to be implanted with a "RFID". You may be surprised: today I am not a wholehearted supporter of the Californian Legislation. Perhaps we decide in High Security Environments such as nuclear power plants or prisons on the implantation of "RFID".

Law should be general and not refer to one specific technology. Therefore no law for one technology (LOT) – no RFID Law – is advisable.

Secondly: In my opinion it is true that law should not relate to one technique. The Californian way of encompassing every subcutaneous identification device – including RFID but not focusing on it – is the right way. We have to deal with contactless technologies capable of actively or passively transmitting information – whatever their name might be.

Law should not be premature and should not stymie technological and economical progress.

Thirdly: Law should not stymie but support progress. I think that the legislative debates serve to inform the public and to further the social acceptance of RFID technology. There should be no fear mongering of privacy advocates but the qualified discourse how we evaluate the opportunities and risks of these technologies. The law with its majoritarian and representative character may legitimize usages that are now under fierce discussion of activists.

These questions lead to my last point: Your Critique is Input for me and perhaps you will tell me how many hurdles went down on my parforce ride to future "RFID" law in the following minutes.

(7) Add-On: What Can a Radar Chart with the Axes Globality, Verticality, Ubiquity and Technicity Contribute to the Legal Discourse?

In my opinion "RFID" law has to satisfy the ideal of being technology and market compatible and technology has to satisfy the ideal of being market and legally tolerable. One should not postulate new legislation without offering a strategy – hence I developed a radar chart with the four axes "globality, verticality, ubiquity and

technicity"[28], revolving around two scenarios – an EPC scenario (tagging an item) and a RTAMP scenario (subcutaneous implants with medical information).

The four axes of the radar chart are defined as follows:

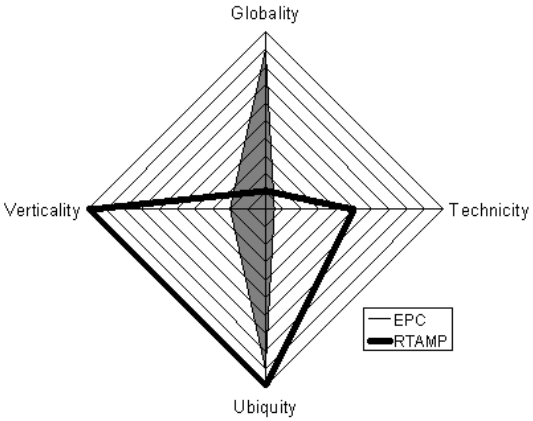
(a) *Globality*: In how many countries should RFIDs be freely produced and marketed?

(b) *Verticality*: How long is the lifespan and/or the length of use of the tag/chip, reader and background device?

(c) *Ubiquity*: To what extent are RFIDs part of our inner (subcutaneous use) or outer (ambient intelligence) present? To what extent are we surrounded by RFIDs – or not?

(d) *Technicity*: Which technical qualities does the system show with respect to the processing of data, as well as the protection against unauthorized access?[29]

I will not go into the details – kindly look into my article if you are interested – but stress the result of this chart for "RFID" legal lobbyism and criticism.



Firstly the EPC scenario: Electronic product codes shall be affixed to products nearly everywhere (high globality), in 2007 they are confined to the supply chain (low lifespan, low verticality), theoretically EPC could be used ubiquitously, the entire surroundings of a person (things, plants, animals) could be tagged (therefore high ubiquity) and the technique is comparatively simple (low technicity). To further global marketeering EPC legal lobbyism should also be global and take into account that the criticism against "RFIDs" will spread globally equally. This is the experience made for example by a RFID protagonist (Metro) who was faced with transatlantic "RFID"

[28] See Schmid, V. "Radio Frequency Identification Law beyond 2007", in: Floerkemeier, C./ Langheinrich, M./ Fleisch, E./ Mattern, F./ Sarma, S.E. (Eds.), "The Internet of Things", Springer LNCS 4952, 2008, p. 203 ff..

[29] Schmid, V. "Radio Frequency Identification Law beyond 2007", in: Floerkemeier, C./ Langheinrich, M./ Fleisch, E./ Mattern, F./ Sarma, S.E. (Eds.), "The Internet of Things", Springer LNCS 4952, 2008, p. 203.

criticism.[30] So if you don't opt for a law side stepping strategy and resort to EPC self regulatory practices – EPC Guidelines – you should design and be prepared for RFID law in a global perspective.

Secondly the juxtaposition for this Global Perspective shall be presented: In the hypothetical RTAMP scenario I have chosen a chip which is implanted into a person. This chip contains medical information (blood type, allergies or special diseases e.g. diabetes or epilepsy). In emergencies the chip enables doctors to immediately access life saving information fulfilling the old postulation: "Don't give me privacy, but give me back my vitality." This Real-time Authentication of Persons (RTAMP) Scenario has a much lower globality value (10 %). Considering the comparatively high costs for the product and the ethical doubts, it is expected that only a little number of states will choose such a technology that – literally – "goes under one's skin". Clearly the RTAMP scenario reaches the highest verticality value (100 %). Theoretically the tag accompanies the chipped person their whole life (with implantation as an infant). The life span of the wearer then is identical to the duration of the tag. RFIDs that "go under one's skin" accompany the wearer everywhere and therefore have the full ubiquity value (100 %). The RTAMP scenario with the implanted chip gets a middle value for technicity (50 %). Such a tag contains sensitive data (§ 3 Section 9 German Data Protection Act) and therefore needs a stringent IT-security policy that protects it from unauthorized reading or rewriting. In summary it can be said that this is a single country endeavor and I already foresee some of the criticism in the audience: Do we have to store these sensitive data on the tag and not in the backhand device? Is it really feasible to implant a RFID for a lifetime? Think about new attacks and new techniques to overpower today's IT security strategies. These questions will be dealt with by RFID law beyond 2007.

Slides see: "RFID Law beyond 2007"

[30] Schmid, V., "Mastering the Legal Challenges", in: Heinrich, C. "RFID and Beyond, Growing Your Business Through Real World Awareness", Wiley Publishing Inc., Indianapolis, USA (2005). pp. 193, 196 ff.; Metro was the first international acting retailer who started to tag their products throughout the "Metro Future Store", a pioneer project in Rheinberg, Germany to evaluate the benefits of RFID in the supply chain. Activists from Germany (FoeBuD) and the USA (CASPIAN) started massive protests against this use of RFID. See Stern article of 11/03/04 http://www.stern.de/computer-technik/technik/index.html?id=521435&nv=ma_ct (04/07/08).

(II) Nizza: A Seven Minute Agenda for the Transformation of the “Mobile Internet” to the “Internet of Things” to the “Internet of Persons”

Slides see: “Internet of the Future”