TECHNISCHE UNIVERSITÄT DARMSTADT

Mastering the Legal Challenges (of RFID)

Prof. Dr. Viola Schmid, LL.M. (Harvard)[1]

published in: RFID and Beyond: Growing Your Business Through Real World Awareness / Claus E. Heinrich (ed.), published by Wiley Publishing, Inc., 2005, ISBN: 978-0-7645-8335-3[2]

Radio Frequency Identification provides the opportunity to improve products and services, make them safer and cheaper, and even protect people and animals from themselves and others.[3] The use-oriented chapters of this book express the hope that "RFID will revolutionize . . . the way we do business, and deliver unimaginable benefits."[4] Two main legal arguments can be made against making use of these numerous opportunities:

- The right to *data privacy,* which is the right to privacy with respect to the collection, processing, and storage of personal data by automatic means.[5]
- The right to *data security,* or *IT security,*[6] which is the existence of reasonable security safeguards protecting personal data from such risks as loss or unauthorized access, destruction, use, modification, or disclosure.[7]

SOME RFID SCENARIOS

These rights, which are concepts of European and public international law, are now on the verge of becoming new legal issues in the American legal system. Paradoxically, an inverse relationship exists between these rights and the benefits of RFID:"In order to have the most value to both individuals and society, the infrastructure (to read tags) needs to be widespread. . . And yet it is just the widespread infrastructure that raises the most questions."[8] Many of the RFID applications that promise the greatest technological, medical, and economic benefits also create the greatest legal challenges. This chapter examines three of the many possible scenarios.

EPC SCENARIOS

Electronic product codes (EPCs)[9] are a strategy for the real-time enterprise (RTE)[10] and contain, for example, the following type of information:" The cola can was produced at the New York plant on September 9, 2004." This is EPC scenario 1; it doesn't involve personal data and therefore has no relation to existing privacy provisions of the United States Constitution and the United States Code. EPC scenario 1 can then theoretically be combined with two other data records, to create two more scenarios. EPC scenario 2 includes details about the sale: "The cola can

was sold for U.S. $1 on October 6." EPC scenario 3 involves the customer: "bought by credit card holder X." The combination of EPC scenarios 1, 2, and 3 triggers privacy protection under U.S. and European law because "personal data"[11] are involved. [12]The reasons for employing EPCs are at least twofold: The cola example is part of an asset management strategy, whereas the federal Food and Drug Administration recommends RFID tagging for drugs as a means of combating counterfeit drugs: "In recent years, however, the FDA has seen growing evidence of efforts by increasingly wellorganized counterfeiters backed by increasingly sophisticated technologies and criminal operations to profit from drug counterfeiting at the expense of American patients."[13] The impact of counterfeit drugs on the health, liberty, or happiness of humans can be devastating. RFID may offer a welcome remedy to minimize these risks.

RTAMP SCENARIOS

RTAMP, or the real-time authentication and monitoring of persons, occurs when access authorizations need to be checked wirelessly or when RFID tags distributed around the home are used to determine whether elderly people requiring care have, for example, taken their medication, brushed their teeth, or eaten (Activities of Daily Living-Monitoring, a visionary project of Intel that was presented at a workshop of the Federal Trade Commission).[14]Another scenario is the attachment of RFID to students' school bags or nameplates while tag readers are installed at the school gates and at locations the students' parents and teachers think could be dangerous.[15] In 2004 the implementation of RFID strategies at a primary school in Osaka, Japan, is the reaction to a 15-minute rampage of a mentally disabled person who stabbed eight children and seriously wounded 13 others in 2001.[16] Reportedly similar strategies are employed at a Buffalo school in a "gritty neighborhood."[17]

RTAMA SCENARIOS

An example of real-time authentication and monitoring of animals (RTAMA) is the planned legislation in Idaho in response to the challenges of bovine spongiform encephalopathy (BSE, or mad cow disease). The aim of the legislation is to make the import of cattle dependent on RFID identification.[18] From a technological perspective, EPC applications are real scenarios and RTAMP and RTAMA are partly future areas of use. The newness of RFID in everyday use and the diversity of areas of use prevent a final legal assessment at the moment. Yet this newness and diversity require the first steps toward a legal assessment to be made. And these steps are required by not only American or European law and legal theory, but by laws everywhere: A global technology such as RFID will require global RFID law—at least a global discussion of whether any RFID law is needed.The economy thrives to globalize, the products and services will be marketed globally (via the Internet), and the RFIDs attached to products and included in services would be a chill and a hindrance for these market chances if certain national legal systems would object to RFID applications and ban them. But even in this hypothetical scenario, it is evident that information about RFID and deliberation is needed. Even a hypothetical State S with the highest data privacy standards imaginable that banned RFID would be in the greatest danger that its hypothetical anti-RFID laws would be circumvented or without force because RFID will be so widespread. If steps on a legal stepladder

have to be considered, why not consider as the first step in State S the German law? German law was not only a pioneer of data privacy and data security,[19] but it is now also very important for those for and against RFID. RFID is being piloted and rejected on both sides of the Atlantic, as the paradigmatic scenarios in Rheinberg, Germany, demonstrate. On June 23, 2004, the Washington Post reported: "A store in Rheinberg, Germany, took RFID tags out of its loyalty cards after protests. Many large firms working with RFID now have extensive disclosure statements on their Web sites."[20] The article reported on a workshop, Radio Frequency Identification: Applications and Implications for Consumers,[21] on June 21, 2004, organized by the Federal Trade Commission (FTC). At the workshop, Katherine Albrecht, who founded the consumer rights movement CASPIAN,[22] boasted that ". . . CASPIAN uncovered the scandal and rocked Germany."[23] What had happened? Two scenarios can be distinguished: the METRO scenario and the CASPIAN scenario.

METRO Group Scenario

The real-time enterprise METRO, of Germany, has a "future store,"[24] the purpose of which is to test Real World Awareness (RWA) strategies and familiarize customers with such strategies. The METRO loyalty card contained an RFID tag and was designed to ensure, among other things, youth protection in the multimedia department.This department gives customers the opportunity to try out movies before they buy them. They hold their loyalty cards in front of a reader and can then watch selected sequences from the movies—as long as they are at least 16 years old, as required by the German Youth Protection Act. METRO handed out loyalty cards only to people who were at least 16.The reader installed in the multimedia department needed only the customer number: The presence of a loyalty card automatically meant compliance with the Youth Protection Act. As the subsequent events in the CASPIAN scenario showed, this one-way, read-only transfer of data without reference to personal details (apart from the customer number)—totally unspectacular from the point of view of data privacy law—might not have offered adequate data security.

CASPIAN Scenario

On January 31, 2004, Ms. Albrecht received a METRO loyalty card after she and some other activists had been on a visit there.Without METRO involvement, the activists purported to read the tag's memory during a public presentation of Ms. Albrecht's the following day using a RFID
reader from the company Megaset. They added the sentence "Thank you, Katherine" to the memory.[25] The CASPIAN scenario is thus a data security law scenario provoked by activists. It was not METRO that illegally read personal or other data but, rather, the activists who accessed the tag's memory.Whatever the legal significance of the activists' reading or writing strategy,[26] there is no dispute that the METRO tag is unprotected against RFID readers and writers. This could be a breach of German data security law,[27] which requires that the storage of personal data by automatic means must be protected against unauthorized access, destruction, use, modification, or disclosure.Why should a separate law apply if an individual's nonpublic personal information is stored in an RFID tag rather than on a handheld or personal computer? Under German law, data privacy requires data security.

RFID QUESTIONS

Should consumers be notified if companies use RFID? Should RFID be covered under data security law? And, will RFID invade consumer privacy? This section looks at each of these questions in turn.

QUESTION 1: DO CONSUMERS NEED TO BE NOTIFIED OF RFID USE?

Here is the clear answer to this question in areas under U.S. jurisdiction: In July 2004, there was not yet any legislation requiring notification.[28] However, some differences already exist in the legal developments between federal and state law, as described in the two following sections.

Federal Level: The Duty of Information
The activist Ms.Albrecht is demanding a duty of information at the federal level with the proposed legislation CASPIAN—RFID Right to Know Act of 2003.[29] The CASPIAN initiative wants the duty of information to also cover RFID that acts purely as a bar code, as described by EPC scenario 1, earlier in this chapter—that is, no personal data is involved, unlike the EPC combination scenarios 1, 2, and 3.[30] All uses of RFID technology should be clearly labeled and indicate at least the following information: ". . . at a minimum, that the consumer commodity
. . . bears an RFID tag and that tag can transmit unique identification information to an independent reader before and after the purchase."[31] The proposed legislation is not far removed from the selfregulation policies of some RTEs in the electronic product code industry. They propagate comparable guidelines, "which are based . . . on industry responsibility, providing accurate information to consumers and ensuring consumer choice."[32]

State Level: RTAMA and Duty to Information
The states differ in that one state uses RFID in its legislation as a control instrument while others are occupied with the right-to-know issue. An example of a state using RFID as a control instrument is in the RTAMA scenario in Idaho. The data privacy interests of the breeders show that RTAMA can change economic reality and the market:"The tags contain medical history, lineage, and price, which livestock owners are wary about releasing. . .We think it's very important to protect that data, and we will not go to a mandatory system until we find a way to protect that data."[33] The proposed legislation in Utah, Missouri, and California provides examples of the right-to-know issue. In Utah, the first attempt failed in March 2004 because of resistance from retailers who felt too restricted in their RFID plans. The politician introducing the legislation then announced a further breach.[34] The legislative bodies in California and Missouri are still deliberating.[35] To summarize, the United States does not (yet) have any legal requirement to label goods that have RFID tags. Even nonlegal guidelines for industry responsibility, however, should advise the industry to inform the public. Consequently, the following sentence will not need to be uttered in the future: "RFID industry is in a crisis, but it's not a crisis of functionality—it's a crisis of confidence." The area in which RFID is being used should determine whether the information is provided in the form of labels, notices in stores, or information on a Web site. This chapter thus distances itself from the CASPIAN initiative, which demands labels (with tags attached under the labels) and recommends that the issue of whether the duty of information to the general public is necessary in all RFID scenarios needs to be

discussed. There is no apparent legal requirement, for example, that a car thief be warned about the use of an antitheft device. Should an unauthorized person be informed of efficient RFID security applications[36] or a child or an elderly person requiring care be informed of RFID tags (designed to protect her) if the tags then cease to be effective? The RTAMP scenarios let us foresee interesting legal and philosophical discussions about RFID and self-determination, freedom, privacy, and security.[37] In addition to the proposed detailed and use-oriented legal examination, in some instances it would be a good idea from a technical point of view to indicate RFID strategies by using labels. For example, if the channel for transferring data is short and the product to be read is large, a label indicating "RFID inside" helps locate the tag and thus speeds up the read process.[38] To conclude our discussion of the theoretical German state, State S, the German chief privacy officer demands RFID legislation, but, so far, the German government sees no necessity for initiating the legislative process.[39]

QUESTION 2:WHAT REQUIREMENTS ON THE USE OF RFID ARE NEEDED UNDER DATA SECURITY LAW?

The protection goals that are familiar from IT security law—such as identity, authenticity, integrity, obligation, and confidentiality[40]—also apply to RFID. U.S. IT security law requires examination, particularly in the area of technological standardization,[41] which needs to be further developed for specific areas of RFID use. The METRO and CASPIAN scenarios prove the great significance of data security for the deployment of RFID. The Idaho RTAMA scenario also shows you that access rights must be effectively secured, for example, if the food agency should not be granted access to all information that is important to the life of the cattle. The general rule needs to be that the more personal or economically relevant the data processed in the memory, sensor, and logic device, the more specific the rules must be that determine which read devices can (exclusively) access it and using which authentication. This statement is particularly true for RTAMP scenarios and even more so for complex cases within these scenarios, such as improving the care of seniors or students through monitoring. Monitoring can take place only with exclusive access rights—otherwise, there is a risk that people's privacy will be invaded. The EPC applications occupy a special position: In contrast to the comparatively complex RTAMP and RTAMA applications, electronic product code applications need to be read by as many readers as necessary (or possible). Here, the rule is that RFID can work only without authentication and identification.[42] This "lack of IT security" is justifiable if only EPC scenario 1 is used. Combinations involving EPC scenarios 2 and 3 involve personal data and are thus subject to higher security requirements. Practitioners point out that the demand for RFID that is secure under
data privacy and data security law (the "smart" RFID tag approach) conflicts with the need for cost effectiveness:"With a budget of five cents, there is very little to spend on additional logic gates."[43] The response is that cost effectiveness has always presented a challenge in the quest to make IT secure and sustainable and to improve its functional quality. Beyond the unilateral, specific security requirements, which depend on the type of application and the complexity of the tag (for example, storage capacity, type of logic device, direction of data transfer—read only or read/write, for example—or distance of data transfer[44]), future RFID law will face another challenge: the assessment of tools that privacy activists use in bilateral and multilateral scenarios to protect their own data. Such "DataPrivatizers" can range from RFID detectors to active jamming approaches that stop the wireless interfaces from

working.[45] Depending on how well the tools function and how much they are used, the main deciding factor will be whether, first, society and, second, the legislators, authorities, and courts find the right balance between RFID manufacturers and users on the one hand and consumers – who either accept or reject RFID—on the other. This process will entail considerable effort, particularly for EPC RFID applications, as the planned legislation in California, Utah, and Missouri illustrates. The social and legal issue will be the extent to which EPC RFID tags can and should be read ubiquitously and pervasively after the business transaction has taken place. In summary, because there is still no legislation shaping the requirements for RFID use, the detailed legal security criteria are fuzzy and they are difficult to determine—even for informed, motivated early adopters. However, what should become clear is that the total disregard for security arguments, such as in the METRO scenario, predictably leads to a lack of acceptance. Technology needs to be accepted if it is to be successfully marketed and thus have a chance to contribute to the good of the public.

QUESTION 3: IS THERE A DANGER THAT RTES WITH RWA STRATEGIES (IN PARTICULAR, RFID) DIGITALIZE PEOPLE AND THEIR BIOGRAPHIES AND MISAPPROPRIATE DATA?

The answer to this question is clearly Yes. However, there are always risks in life. All technologies come with opportunities and risks, and it is society and the law's task to recognize and analyze these opportunities and risks and, if necessary, develop strategies to align the opportunities and risks optimally with each other. The proposed CASPIAN legislation would add the provisions in the following sidebar to the Privacy subsections of the United States Code.[46] The background to this demand to create consumer privacy RFID legislation and the responsibility of the Federal Trade Commission for monitoring and issuing data privacy and data security standards is the fear that RFID will further increase the danger that data will be collected and sold in a quantity and quality unimaginable until now. There are many instances of the illegal sale of data without the consent of those affected, as Ms.Albrecht has found in her research:"There are also a number of disquieting cases where Internet companies reneged their privacy policies during hard times by attempting to sell customer purchase data to the highest bidder."[47] The risk of breaking the law is equally high for all technologies—but the consequences are more dangerous with technologies that can digitalize even more data, and thus generate more products (EPC combination scenarios 1, 2, and 3), and sell them at lower transaction costs.

§ 6831 PRIVACY PROTECTION FOR CONSUMERS
(a)
(1) A business shall not combine or link an individual's nonpublic information with RFID tag identification information beyond what is required to manage inventory.
(2) A business shall not, directly or through an affiliate, disclose to a nonaffiliated third party an individual's nonpublic personal information in association with RFID tag identification information to identify an individual.
(b) The Federal Trade Commission shall establish appropriate standards for the businesses described in subsection (a) of this section:

(1) To insure the integrity and confidentiality of an individual's records and information;
(2) To insure that RFID tag records do not identify individuals;
(3) To protect against anticipated threats or hazards to the security of an individual's records and information; and
(4) To protect an individual against substantial harm or inconvenience, which may result from unauthorized access to or use of an individual's records and information

Economists would like to answer the question of whether the incentives to misappropriate data are greater or less with more data (because the costs lessen if more data is available). In cyberspace, the following statement applies: There is no way of making good the misappropriation of data. After databases have been outlined and passed to an unauthorized party, there is no guarantee that their content has been deleted.[48] A wrong cannot be made right again. In addition to evaluating the risks of RFID, its opportunities need to be explored. Therefore, everyone involved in the market (manufacturers, users, consumers, and the public) must be open to discussion and be informed as quickly as possible about the opportunities that RWA offers in order to develop a culture for dealing with its use and its risks. Legislation also needs to be discussed even if it does not concentrate on the same issues as CASPIAN.[49] The necessity of legal regulations must be decided separately for each scenario. See the section "RTAMP Scenarios," earlier in this chapter, for examples of how labeling can reduce the effectiveness of RFID in protecting people from themselves, and see "EPC Scenarios" to see where labeling is a prerequisite for reading tags quickly if the channel for transferring data is short. Rather than a call for a moratorium, this is a global appeal to lawyers to look into RFID. Maybe RFID needs global legislation—as the fight against cybercrime[50] and spam[51] does. A far less satisfactory outcome would be the future intimated by The Economist: "Scaremongering by some privacy advocates, who fear that details of everything they buy will be held on a database and potentially used for nefarious purposes, has made some firms quite defensive about their RFID ambitions."[52] In summary: All parties concerned should work on the safety, security, and privacy of RFID and—for lack of a strict legal framework— ask the time-honored question: How do I want my data and that of my children to be handled?

[1] The author would like to thank Ms. Ruth Schadel and Mr.Andreas John for helping with her research.
[2] This is a document of 2004. Some of the links (e.g. 9, 24, 42) might no longer function. This article is not a "living document".
[3] Floerkemeier, C.; Schneider, R.; Langheinrich, M. "Scanning with a Purpose—Supporting the Fair Information Principles in RFID Protocols" (July 27, 2004), http://www.inf.ethz.ch/~langhein/articles/ , p. 5. Shows 15 different kinds of purpose declarations for RFID reader queries: access control, anticounterfeiting, antitheft, asset management, contact, current, development, emergency services, inventory, legal, payment, profiling, repairs, returns, and other.
[4] Langfort, S.Wal-Mart's global director of RFID, as cited in Washington Post: Krim, J. "Embedding Their Hopes in RFID," June 23, 2004.
[5] European Union law: Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 1.
[6] IT security and data security are synonymous in this context. In a future legal perspective, there will be in Germany a fundamental right to data security (Article 2 Section 1 and Article 1 Section 1 of the German Constitution) and a so-called "institutional guaranty" of IT security.
[7] Public international law: OECD guidelines on the protection of privacy and transborder flows of personal data (September 23, 1980), Part Two, No. 11, "security safeguards principle"). European Union law: Regulation (EC) No. 460/2004 of the European Parliament and of the Council of March 10, 2004, establishing the European Network and Information Security Agency.Article 4 (c) "network and information security" means the ability of a network or an information system to resist ". . . accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted data. . . ."
[8] Elliot Maxwell, chairman of the International Policy Advisory Council of EPCglobal, as cited in Washington Post: Krim, J."Embedding Their Hopes in RFID," June 23, 2004.
[9] www.epcglobalinc.org/about/faqs.html (July 27, 2004).The Electronic Product Code (EPC) is a unique number that identifies a specific item in the supply chain. The EPC is stored on a radio frequency identification (RFID) tag, which combines a silicon chip and an antenna. After the EPC is retrieved from the tag, it can be associated with dynamic data, such as where an item originated or the date of its production. Much like a Global Trade Item Number (GTIN) or Vehicle Identification Number (VIN), the EPC is the key that unlocks the power of the information systems that are part of the EPCglobal network.
[10] Raskino,M."Driving Out of the Downturn—The Real Time Enterprise," Conn. L.Trib., Vol. 28, No. 47 (December 2002); Kuhlin, B.; Tielmann, H. The Practical Real Time Enterprise. Berlin: Springer, 2005.
[11] European Union law: "Personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); 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 [Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article 2 (a)] U.S. law: "Personal information" means individually identifiable information about an individual collected online, including (A) a first and last name (B) a home or other physical address, including street name and name of a city or town (C) an e-mail address (D) a telephone number (E) a Social Security number (F) any other identifier that the Commission determines to be the physical or online contacting of a specific individual or (G) information concerning the child or the parents of that child that the Web site collects online from the child and combines with an identifier described in this paragraph (Children's Online Privacy Protection Act of 1998).
[12] Schmid,V. RFID and Privacy, Germany, to be published in 2005.
[13]Combating Counterfeit Drugs: A Report of the Food and Drug Administration, Feb. 2004, http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html (July 14, 2004).
[14] Fishkin, K. Intel Research, Seattle:"RFID for Healthcare: Some Current and Anticipated Uses," a lecture given at the FTC Workshop, June 21, 2004; http://www.ftc.gov/bcp/workshops/rfid/ (July 27, 2004): "Better Eldercare: Activities of Daily Living– Monitoring: If RFID tags are scattered about a house (either from purchase or manually) and RFID readers can detect when you come near those objects, then we can do a good job of inferring ADLs including medication taking."
[15] Japan Today, July 8, 2004, "School to put electronic tags on students to monitor safety" http://www.japantoday.com/e/?content=news&cat=4&id=304748 (July 27, 2004).
[16] Pagano,A."Massacre of Japanese schoolchildren provokes questioning of society,"August 3, 2001,World Socialist Web site, http://www.wsws.org (July 27, 2004).
[17] Scheeres, J. "Three Rs: Reading, Writing, RFID," Wired News, http://www.wired.com/news/print/0,1294,60898,00.htm (July 27, 2004).
[18] There is no federal animal-identification system. Hawks, B."Review of National Animal Identification Plan," hearings of the Agriculture, Nutrition and Forestry Committee—U.S.Senate, http://agriculture.senate.gov/Hearings/testimony.cfm?id=1070&wit_id=3034 (July 27, 2004). 2004 Idaho Bill No. 816, Idaho 57th Legislature—second regular session.
[19] The world's first data privacy law was enacted on September 30, 1970, in the state of Hessen in Germany.
[20] Krim, J."Embedding Their Hopes in RFID," Washington Post, June 23, 2004.
[21] www.ftc.gov/bcp/workshops/rfid (July 27, 2004).
[22] CASPIAN stands for Consumers Against Supermarket Privacy Invasion and Numbering. Compare the CASPIAN Web site: www.nocards.org (July 27, 2004).

[23] www.spychips.com/metro/scandal-payback.html (July 27, 2004).
[24] METRO Group:"METRO Group startet die unternehmensweite Einführung von RFID": www.future-store.org/servlet/PB/-s/15k9c5za28j5wasfwsu1dpi2yl2125xy/menu/1002256_pprint_l1/1088551037081.htm?part=null (July 27, 2004).
[25] Heise online news: www.heise.de/newsticker/meldung/print/44237 (July 27, 2004).
[26] Under German law, this may be in breach of telecommunications secrecy (Jürgen Müller, Ist das Auslesen von RFID-Tags zulässig? DuD 2004, 215, 217), but is justified by Ms. Albrecht's right to information under data protection and data security law.
[27] For example, the annex to the German Data Protection Act, Section 9, if the METRO tag holds "personal data."
[28] The author is working on a paper for German law that would consider a duty of information in the German Data Protection Act.
[29] CASPIAN, RFID Right to Know Act of 2003: www.nocards.org/rfid/rfidbill.shtml (July 27, 2004).
[30] ."There should . . . be a general presumption that Americans can know when their personal information is collected, and to see, check, and correct any errors," Vermont's U.S. Senator Patrick Leahy, at a conference on "Video Surveillance: Legal and Technological Challenges," Georgetown University Law Center www.leahy.senate.gov/press/200403/032304.html (July 27, 2004).
[31] Amendments to the Fair Packaging and Labeling Program (Title 15 U.S.C. Ch. 39 Sec.1453 paragraph (9) and Title 15 U.S.C. Ch. 39 Sec. 1453;Title 21 U.S.C. Ch. 9 Subch. II Sec. 321;Title 21 U.S.C. Ch. 9 Subch. IV Sec. 343;Title 21 U.S.C. Ch. 9 Subch.V Part A Sec. 352; Title 21 U.S.C. Ch. 9 Subch.VI Sec. 362; Title 27 U.S.C. Ch. 8 Subch. II Sec. 215;Title 15 U.S.C. Ch. 36 Sec. 1333).
[32] (1.) Consumer Notice—Consumers will be given clear notice of the presence of EPC on products or their packaging.This notice will be given through the use of an EPC logo or identifier on the products or packaging.
(2.) Consumer Choice—Consumers will be informed of the choice that they have to discard, disable, or remove EPC tags from the products they acquire. It is anticipated that for most products, the EPC tags would be part of disposable packaging or would be otherwise discardable. EPCglobal, among other supporters of this technology, is committed to finding additional cost-effective and reliable alternatives to further enable consumer choice.
(3.) Consumer Education—Consumers will have the opportunity to easily obtain accurate information about EPC and its applications in addition to information about advances in technology. Companies using EPC tags at the consumer level will cooperate in appropriate ways to familiarize consumers with the EPC logo and to help them understand the technology and its benefits. EPCglobal would also act as a forum for both companies and consumers to learn of and address any uses of EPC technology in a manner inconsistent with these guidelines.
(4.) Record Use, Retention, and Security—As with conventional bar code technology, companies will use, maintain, and protect records generated through EPC in compliance with all applicable laws. Companies will publish, on their Web sites or otherwise, information on their polices regarding the retention, use, and protection of any consumer-specific data generated through their operations, either generally or specifically with respect to EPC use.
[33] Wilson, M."USDA Steps Up Efforts to Track Livestock," CNN.com, May 24, 2004.
[34] Swedberg, C. "States Seek RFID Laws: State Legislators in Utah and Missouri Have Sponsored Bills That Would Require Retailers to Alert Customers When Goods Contain RFID Tags, RFID Journal, March 16, 2004, http://www.rfidjournal.com/article/articleprint/833/-1/1/ (July 27, 2004).
[35] . Missouri: S.B. No 867, RFID Right to Know Act of 2004 last action: March 9, 2004, Hearing Cancelled E-Commerce and the Environment. California: S.B. No 1834 last action: June 22, 2004, set first hearing.
[36] Another issue is information for authorized parties, which, according to the opinion in this chapter, is required.
[37] For example, because the medication or toothpaste is touched but not used or the children avoid RFID readers at dangerous locations.
[38] Association for Automatic Identification ad Mobility, Standards, March 2004, http://www.aimglobal.org/technologies/rfid/ (July 27, 2004).
[39] German law:"Bundesdatenschutzbeauftragter fordert RFID-Gesetz," Heise online news, May 17, 2004, http://www.heise.de/newsticker/meldung/print/47414; and question of the member of the House of Representatives Gisela Piltz and others (House of Representatives materials 15/3025). Comparable to U.S. law: chief privacy officer, Department of Homeland Security,Washington, DC 20528.
[40] U.S. law:The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide
(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information
(C) availability, which means ensuring timely and reliable access to and use of information. (E-Government Act of 2002; § 3542); German sources: Eckert, C. IT—Sicherheit. Konzepte,Verfahren, Protokolle, 2.Auflage 2003, S. 6ff.
[41] "ISO/IEC 15408-1:1999 under 4.1.1: Security is concerned with the protection of assets from threats, where threats are categorized as the potential for abuse of protected assets." According to available research, this does not include any provisions on RFID (July 2004).To protect assets: For example, California S.B. 1389, see California Civil Code § 1798.82, which requires a state agency or a person or business to disclose any breach of the security of data.
[42] METRO, positioning paper from February 28, 2004: www.future-store.org/servlet/PB/-s/1w8t0r213ahtv1tbkk5ipvv5iz10gnvqu/menu/1002376_l1/index .html (July 27, 2004).

[43] Juels,A.;Rivest, R. L.; Szydlo,M."The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," http://www.rsasecurity.com/rsalabs/node.asp?id=2060 (July 27, 2004).
[44] For cloning tags when the data transfer channel is not secure. Kelter, H.;Wittmann, S. "Radio Frequency Identification—RFID," DuD 2004, 331, 333.
[45] Juels,A.;Rivest, R. L.; Szydlo,M."The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," http://www.rsasecurity.com/rsalabs/node.asp?id=2060 (July 27, 2004). Heise online news:"WOS3: Prototyp des DataPrivatizer zur Kontrolle von RFID-Tags," www.heise.de/newsticker/meldung/48190 (July 27, 2004). Christian Floerkemeier/Roland Schneider/Marc Langheinrich, "Scanning with a Purpose—Supporting the Fair Information Principles in RFID Protocols," http://www.inf.ethz.ch/~langhein/articles/ (July 27, 2004).
[46] Amendment to Title 15 U.S.C. Ch. 94 Privacy. Both existing subchapters (Sec. 6801 ff) contain provisions for the privacy protection of customer information held by financial institutions.
[47] From Katherine Albrecht in 2002, "Supermarket Cards: The Tip of the Retail Surveillance Iceberg," 79, Denv.U.L. Rev. 534, 538 with other proof. See also United States District Court, E.D.New York, Re: JetBlue Privacy Litigation, Master File No. 03-CV-4847), a class action complaint for giving a government contractor five million passenger itineraries in 2002 to test an experimental Department of Defense data mining project.
[48] Because it cannot be guaranteed that the data is deleted from all end devices and that the unauthorized party has no way of copying it.
[49] The German Federal Data Protection Commissioner and a politician from the liberal party are calling for an RFID law in Germany, www.heise.de/newsticker/meldung/47743 (July 27, 2004).
[50] Public International Law: Council of Europe: Convention on Cybercrime (October 23, 2001), which the United States has signed.
[51] Public International Politics: World Summit on the Information Society, Geneva, July 7-9, 2004; http://www.un-ngls.org/wsis-spam-report.htm (July 29, 2004) reports initiatives of the International Telecommunications Union, OECD-Workshops, and of some United Nations Member States.
[52] The Economist, June 26, 2004, "The Future Is Still Smart; Technology, Shopping and Beyond."