Managing Risk Perceptions of RFID

Frédéric Thiesse

Auto-ID Labs White Paper WP-BIZAPP-031

Frédéric Thiesse
M-Lab Project Leader
University of St. Gallen

Contact:

Auto-ID Lab St.Gallen / Zurich
University of St.Gallen
Dufourstr. 40a
9000 St.Gallen
Switzerland
Phone: +41-71-224-7243
Fax: +41-71-224-7301

E-Mail: frederic.thiesse@unisg.ch

Internet: www.autoidlabs.org

Business Processes & Applications

Abstract

Against the background of the first RFID-Rollouts by large retailers in North America and Europe, this paper concerns itself with the perception of RFID technology as a risk to privacy. The objective of our contribution is to identify, at a relatively early phase of the risk development, strategic options with which RFID suppliers and users can positively influence the public acceptance of the technology. We propose a strategic framework based on research findings on risk perception and technology acceptance as well as a set of options for coping with the public perception of RFID-related privacy risks.

Keywords: RFID, Privacy, Technology Acceptance, Risk Perception

1. Introduction

1.1. Practical Relevance

The technologies of Radio Frequency Identification (RFID) enjoy an enormous interest at the current time, not only from the standpoint of research but also from corporate practice. Enterprises from diverse branches are hoping for solutions to a wide range of management problems through RFID, from simple increases in processing efficiency for the receipt and despatch of goods in distribution centres through to improvements in goods availability on the shelves and on to the struggle against shrinkage and product counterfeiting. However, over the past few years, concerns about the possible risks of using RFID have increasingly been voiced.

The risks associated with RFID that are discussed in the public include both the direct impact of electromagnetic radiation on health, as well as indirect economic consequences such as the elimination of jobs through increasing automation (Duce, 2003). The most frequently voiced fear refers to the misuse of data generated by RFID, resulting in an undesirable intrusion into the privacy of individuals. The debate has become additionally heated through the actions and campaigns of pressure groups. For example, the well-publicised "Big Brother Award" given to the Metro Group, along with a demonstration in February 2004 in front of the Metro Future Store, caused the retailer to ultimately withdraw the RFID-based customer cards that were in circulation at the time (Albrecht and McIntyre, 2005). Further examples in Europe and the US, such as the call for a boycott of Gillette products because of tests with RFID transponders in razor blade packages, show that these are not isolated incidents. That this protest movement can bring about such sustainable effects, whilst working with the simplest of methods, permits conclusions regarding the significance that data protection and privacy have achieved in the populace as a whole.

1.2. Research question and structure

This contribution concerns itself with the question how companies should cope with negative press reactions and the campaigns of various social groups in order to positively influence the public perception of RFID and thus to pave the ground for future applications in retail, CPG, life sciences and other industries. For this reason, the primary aims of the article are: (a) to use theory and research on risk perception and technology acceptance to analyse the development of RFID as a risk issue and (b) to consider ways to minimise the effect of risk perceptions on implementations of the technology and consumer behaviour. To meet these aims the article is structured into five sections. It begins with a short overview of RFID

technology, its relevance to privacy, and technical countermeasures proposed in other works. The following section provides a review of the theoretical concepts of risk, trust, and technology acceptance as well as the interrelations between them. We continue with an analysis of media-reporting about RFID and reconstruct the history of the RFID risks debate over the past few years. In a next step we propose a theory-based framework for risk management and propose a set of strategic options. The contribution ends with a discussion of our approach and an outlook on future developments.

2. RFID and Privacy

2.1. RFID technology and applications

RFID is a technology for the automatic identification by radio of physical objects such as industrial containers, palettes, individual products and also people. The identification event takes place over transponders located in or on the respective objects, which can be addressed without physical contact, over the so-called "air interface", by the antenna on a scanner device. Typical areas of application for RFID lie, adjacent to classics such as animal identification or access control systems, above all in Supply Chain Management, where the technology makes possible simplified goods turnover, automatic stock control in the storeroom resp. on the sales floor, theft protection, product tracking etc. (Bose and Pal, 2005).

 The reason for the recent rapid and escalating use of RFID lies primarily in advanced miniaturisation, maturity as well as in the constant price decline which makes the use of RFID economically viable in ever more areas of application (Byfield, 1996; Sarma, 2001; Want, 2004). Another trigger has been especially the activities of the Auto-ID Center, a project founded in 1999 at the Massachusetts Institute of Technology (MIT), in cooperation with numerous industrial sponsors, for the development of RFID Standards. The main result of the Auto-ID Center was the "Electronic Product Code (EPC)" (Sarma, 2005), a worldwide unambiguous numbering scheme for the designation of arbitrary physical goods which should ensure the interoperability of the technology in supply chain wide applications. In the following years EPC became the technical foundation for the multiple RFID initiatives of large chain stores such as Wal-Mart and Metro, and also for industrial enterprises such as Novartis or the US Department of Defense.

2.2. Privacy aspects of RFID

The threat to privacy through the use of information technology has its origins in the ability to permanently save and link information about individuals (Culnan and Bies, 2003; Perrin,

2005; Spinello, 1998). With RFID and similar technologies, yet another dimension to data acquisition has developed through (a) the temporal and spatial extension of data collection activities, (b) the inability to recognise and reconstruct data collection, (c) the acquisition of new data types through real-time monitoring, (d) the ever decreasing transparency of reasons for acquiring data, and (e) the uncontrolled data access caused by extreme interconnectedness (Cas, 2004; Langheinrich, 2005). Thus, the use of ID tags, sensors and location systems leads to the disappearance of what Lessig (1999) calls "structural" or "architectural" barriers, i.e. economic factors that make privacy intrusions costly or unprofitable. In the case of RFID, the privacy-related problem arises particularly because of the globally unique identity of each good and the possible linkage with the owner. That facilitates, in principle, an automatic tracking of individual people (Juels, 2006; Sarma et al., 2002; Weinberg, 2005).

2.3. Privacy-enhancing technologies

The perpetual privacy debate has lead to a variety of technical proposals for securing RFID data and encompasses, apart from general IT security measures, a number of RFID-specific "Privacy-Enhancing Technologies (PETs)". These prevent the uncontrolled reading of transponders as well as the manipulation of information saved in them. The literature contains several different approaches (Cavoukian, 2004; Juels et al., 2003; Kumar, 2003; Weis et al., 2003). The simplest protection from access to transponders by third parties is physical separation, by means of a metal net or a foil sheet. Other options include the use of jammer transmitters or so-called "blocker tags", distance-based access control, and bug-safe anti-collision protocols. The most widespread PET mechanism is the kill command in transponders following the "EPC Class 1 Generation 2" standard.

3. Theoretical Underpinnings

3.1. Risk perception

A classic definition of risk is given by Harding (1998) who defines the term as "a combination of the probability, or frequency, of occurrence of a defined hazard and the magnitude of the consequences of the occurrence". This notion usually provides the basis for formal risk assessments and is the form in which risk is often conceptualised by technical experts. While this view considers risks most of all quantitatively and typically rejects other forms of risk perception as irrational, the layperson generally has a more intuitive, qualitative risk concept which is not limited to the probability of damages or the extent of damages (Renn and Levine, 1991). This finding has led many researchers to propose that risk is socially constructed rather than an objective state of nature.

Initial research into risk perception in the late 1970s and 1980s resulted in the development of a theory of risk perception known as the "Psychometric Paradigm" (Fischhoff et al., 1978; Slovic et al., 1981). This research posited that people judge "risk" in terms of psychological dimensions other than probability and harm, e.g. the familiarity of the risk, the willingness to take a risk in general, the catastrophic potential of the risk and its possible benefits (Slovic, 1992). These psychological factors were used to explain public responses to low probability technological risks.

Another perspective on risk perceptions is the "Cultural Theory of risk" (Douglas and Wildavsky, 1982) that focuses on culture, rather than individual psychology as an explanation for differences in risk judgments. Cultural Theory argues that views of risk are produced by social structures. Furthermore, it proposes that there are four basic "ways of life" that determine the way in which we see the world around us and thus the way in which we assess risk.

A significant conclusion for companies dealing with risk is that management of risk in this context should not revolve purely around the consequences of what is only a potential risk, but must also influence the process of risk development itself (Jones, 2001). If the subject of risk develops into a crisis, the enterprise in question may suffer serious consequences, (Watson et al., 2002) as a number of examples in the last few years have demonstrated (see e.g. Cantwell, 2002 for a collection of case studies).

3.2. Risk and Trust

A second concept that is received as a factor of great importance in understanding risk perception and reactions to risk is trust (Slovic et al., 1991). In simple terms, trust can be defined as the belief by one party about another party that the other party will behave in a predictable manner (Luhmann, 1979). Trust is closely related to risk since "the need for trust only arises in a risky situation" (Mayer et al., 1995), i.e. trust would not be needed if actions could be undertaken with complete certainty and no risk.

Although the importance of trust is widely recognized across many disciplines, there is widespread disagreement about its definition, characteristics, antecedents, and outcomes (Lewicki and Bunker, 1995; McKnight et al., 2002). In the IS research domain trust is mostly discussed in the context of e-commerce as an antecedent of a customer's willingness to transact with a web-based vendor (Belanger et al., 2002). The multi-dimensional nature of trust has led to several differentiations in current literature. Based on their analysis of trust concepts McKnight and Chervany (2001) identify the high level constructs of dispositional trust, institutional trust, and interpersonal trust. Trust can also be characterized by its stage of development. Jarvenpaa et al. (1999) differentiate between the initial development of trust and mature trust. Other IS researchers highlight the difference between trust in trading partners and technology trust, i.e. trust in the underlying technical infrastructure based on technical safeguards and protective measures (Knights et al., 2001; Ratnasingham and Pavlou, 2002).

Mayer et al. (1995) discuss the important difference between trust and trustworthiness. They indicate that the perceived trustworthiness of the trustee is an antecedent of trust. As Gefen et al. (2003a) note, trustworthiness is a characteristic of the trustee that depends on the perceptions of benevolence, ability and integrity. Trust on the other hand refers to the trustor's willingness to engage in a risky behaviour.

3.3. Risk and technology acceptance

Previous research in IS has investigated perceptions of privacy, trust, and risk using the Technology Acceptance Model (TAM). TAM is an adaptation of the theory of reasoned action and mainly designed for modelling user acceptance of information technology (Davis, 1989). TAM proposes that two particular beliefs, perceived ease of use (PEOU) and perceived usefulness (PU), determine the user acceptance of technology. Several studies have confirmed the explanatory power of TAM in relation to various types of IT (Davis, 1989; Mathieson 1991; Taylor and Todd 1995; Venkatesh, 2000). Even though considerable TAM research has examined IT acceptance in the context of work-related activity, the theory is applicable to diverse non-organisational settings (Gefen et al., 2003b).

The original TAM model has been enhanced by research on the antecedents of the two central belief constructs in the model, e.g. prior experiences with similar technology use (Taylor and Todd, 1995; Agarwal and Prasad, 1999), demographics such as age or education (Morris and Venkatesh, 2000; Agarwal and Prasad, 1999) and personal innovativeness (Agarwal and Prasad, 1998). Another approach to enhance the original TAM has been to extend the model with new constructs, e.g. intrinsic motivation (Davis et al., 1992; Venkatesh, 1999; Moon and Kim, 2001) and concepts of trust and risk.

Pavlou (2001), for instance, demonstrated that privacy perceptions influenced trust, which in turn influenced the perceptions of risk. Perceived risk had a direct – although negative – impact on intentions to use. Within TAM trust has a positive effect on PU because part of the guarantee that consumers will sense the expected usefulness is based on the sellers behind the system (Pavlou, 2003). On the other hand, PEOU is hypothesized to have positive influence on trust because PEOU can be argued to influence positively a person's favorable outcome expectation toward the acceptance of an innovative technology (Wu and Chen, 2005).

4. Empirical Evidence

In this section we reconstruct the debate on RFID and privacy following the "Social amplification of Risk Framework (SARF)". SARF was developed in the 1980s as a response to the disjunctures between the various strands of risk research (Kasperson, 1992; Pidgeon et al., 2003). SARF outlines an integrative framework describing the dynamic social processes underlying how people perceive and act in the face of risk. The authors list three

mechanisms that contribute to the social amplification (Kunreuther and Slovic, 2001). First, extensive media coverage of an event can contribute to heightened perceptions of risk, propagation of stigmatizing images, and amplified impacts. Second, a particular risk or risk event may enter into the agenda of social groups that dispute the credibility of factual information or inferences. A third mechanism is dramatisation, e.g. in the form of sensational headlines on the catastrophic potential of risks.

A special development of SARF is stigma theory (Kasperson et al., 2001). Stigma theory posits that certain properties of risk-related events predispose them for strong "ripple effects". Such ripple effects strengthen and expand the negative attitudes and heightened risk perceptions with regard to a given technology.

As we will show in the following, all three amplification mechanisms can be found in the RFID risk debate in recent years as well as attempts by consumer advocacy groups and privacy activists to stigmatise the technology as whole.

4.1. Amplification through media coverage

As the first retail company worldwide, the German Metro Group started their RFID-Rollout in November 2004, for elevating the efficiency of their logistic processes as well as for the avoidance of shrinkage in the supply chain and for an improvement of goods availability in their subsidiary branches (Metro, 2004). In the years before, the company had already carried out a series of RFID Pilot Projects with their suppliers, especially in the scope of the so-called "Future Store" in Rheinberg near Düsseldorf. Against this background, this section examines the media resonance of RFID with the example of the most popular German Internet portal for news on information and communication technologies.

As not only anti-RFID campaigns but also the reporting and public discussion take place to a great extent on the Internet, it seems appropriate to draw upon this medium as the starting point for further analysis. The following statements underlie an examination on the basis of the Website www.heise.de, operated by the publisher of the biggest German computer magazine. This selection appears suitable, whilst (a) the focus on IT permits expectation of a large number of RFID relevant reports and (b) the content is nonetheless directed towards a relatively wide audience.

For the first step, a full-text search for the key words "RFID" and "Transponder" located all relevant RFID news items in the Heise database over the last few years. From the total number of 465 search results 243 texts related to other topics, such as TV satellites, and texts that only contained summaries of other news or links to RFID-related news were removed from the list manually. Subsequently, from the remaining 222 entries all 97 news items were identified which deal with the impact of RFID on information privacy. We selected all texts that either (a) explicitly discussed the privacy risks of RFID, (b) reported on the actions of consumer advocacy groups, privacy activists, and public authorities (e.g. national data protection commissioners), or (c) reported on the reactions of RFID users thereto. The graphical depiction of the results is shown in Figure 1.
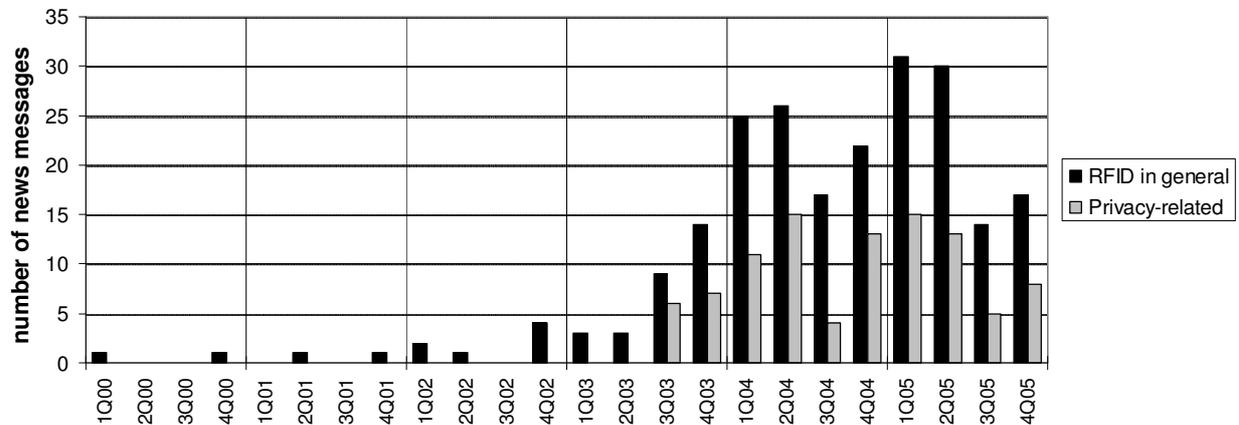
Figure 1: RFID-related entries in the Heise database

The term "RFID" appeared in the reporting list for the first time in the year 2001. It is quite evident from this data that, since mid-2003, privacy has suddenly become a controversial topic and, since then, has been associated directly with RFID and its potential risks. The start of this development was a report on July 8, 2003, through the organisation CASPIAN, regarding the publishing of 68 apparently confidential documents about the plans of the Auto-ID Center and its sponsors for introducing RFID. The article claimed that the motivation for using this technology was its ability to analyse the buying behaviour and financial situation of users without their knowledge. Furthermore, passive RFID transponders were described as being identifiable up to 30 metres away.

In the following months the subject area, in the beginning still vague, developed in the reporting to three substantive points. At the start the reporting was almost exclusively about the application of RFID in commerce, in 2004 the themes "FIFA World Championship" and "Biometric Passport" joined it. The backdrop for the first case was the decision by the Organisation Committee of the World Cup 2006 to equip World Cup tickets with personalised RFID chips. In the second case the reporting revolved around the storage of biometric information on future pass documents.

4.2. Amplification through the actions of pressure groups

In 2003 RFID as a risk issue was brought into the spotlight by groups such as the American Association "Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)" or the German "Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V (FoeBuD)" (Association for the Promotion of Public Mobile and Immobile Data Traffic). In the following years other NGOs (e.g. Electronic Frontier Foundation, Electronic Privacy Information Center, American Civil Liberties Union), but also some data protection authorities (e.g. the European Article 29 Working Group) joined the debate. If one

observes the behaviour over time of technology suppliers and their users in the context of such campaigns, a common pattern of action and reaction becomes evident. Enterprises are put on the defensive by pressure groups and react with a rapid withdrawal of individual application areas or projects. Some prominent examples are summarised in Table 1.

Table 1: Prominent examples for the influence of pressure groups on companies

Companies	Date	Events
Benetton / Philips	March 11, 2003	Action: Benetton announces that it plans to sew RFID tags into fabrics produced at Sisley. Two days later, in the internet, CASPIAN calls for a boycott of Benetton products.
	April 9, 2003	Reaction: Benetton announces in a press release that it will not use RFID in textiles.
Wal-Mart / Gillette	July 8, 2003	Action: CASPIAN publishes 68 "confidential" documents from the Auto-ID Center, which includes Wal-Mart and Gillette amongst its largest sponsors. On April 30, Wal-Mart had commenced an RFID pilot project for automated inventories in sales areas.
	July 9, 2003	Reaction: Wal-Mart terminates the pilot project and announces that it will use RFID only in internal logistics.
Tesco / Gillette	July 22, 2003	Action: the British retailing chain Tesco is accused of using RFID technology in order to capture data and photograph customers as they remove razor blades from a shelf.
	August 15, 2003	Reaction: Gillette denies all allegations, but Tesco admits to testing the "security-related advantages" of RFID technology. The pilot project is terminated at the end of July 2003.
Metro	February 1, 2004	Action: FoeBuD demonstrates in front of the Metro Future Store against the introduction of RFID-based customer cards.
	February 27, 2004	Reaction: Metro exchanges 10,000 customer cards for those without RFID tags.

4.3. Amplification through dramatisation

The before mentioned events and others came along with various attempts of pressure groups to dramatise events. A well-known case for this strategy was the disclosure of P&G's tests of RFID-based shelf inventory control with transponders on Max Factor Lipfinity lipsticks in spring 2003 at a Wal-Mart store in Broken Arrow, Oklahoma (see Hughes, 2005 for a description of the trial). In a press release, CASPIAN claimed that the companies had "experimented on shoppers with controversial spy chip technology and tried to cover it up"

(CASPIAN, 2003). The event got worldwide attention and coined the term of the "Broken Arrow Affair" (De Jager, 2005).

Another example of dramatisation was the case of the "RFID virus". In March 2006 Rieback et al. (2006) presented a conference paper that discussed the possibilities of using RFID transponders as a carrier for program code that could by-pass RFID middleware security mechanisms and thus manipulate a company's database. Though the paper had the character of a technical proof of concept with very limited relevance to real IS architectures, its content and the authors' press release – including the catastrophic scenario of RFID viruses infecting baggage databases at hundreds of airports within 24 hours – were discussed in several international newspapers and TV reports.

4.4. Stigmatisation

The reactive behaviour of RFID users allows pressure groups to "capture the issue", i.e. to seize the initiative and to succeed in raising the profile of an issue, to the point where others can no longer pretend it is unimportant and are required to respond (Leiss, 2003). One of the most potent devices for issue capture is to find a way to brand the risk source with a stigma (Flynn et al., 2001). In the case of RFID one strategy of stigmatisation has been to associate RFID with other technologies perceived as risky. For example, Katherine Albrecht, founder of CASPIAN and perhaps the world's most prominent anti-RFID activist, ranked the risks RFID poses to humanity as "on par with nuclear weapons" (cited by Downes, 2003). In another interview, she said that "this technology is like an electronic frisk or a form of X-ray vision." (cited by Murray, 2003).

Organisations such as CASPIAN employ the Internet strongly in their dialogue with customers, as for example the boycott appeals in Figure 2 show. One way of changing perceptions of the public is manipulation through language. Technology opponents, on their Websites and Publications, consistently allot RFID labels such as "spy chips", "big brother bar code", and "tracking devices", which blend the technology, potential application purpose and (negative) evaluation. This rhetoric is supported by graphical tools, e.g. drawings of RFID-equipped products that permanently emit radio waves and X-ray images of human beings which imply the idea of a technology that reveals an individual's most intimate details. Last but not least, contextual statements about the technology are combined with rumours about its application, and so the borderline between provable facts and speculation – willingly or not – becomes blurred. Examples are the greatly varying details given to size, range and reading rates of RFID transponders.
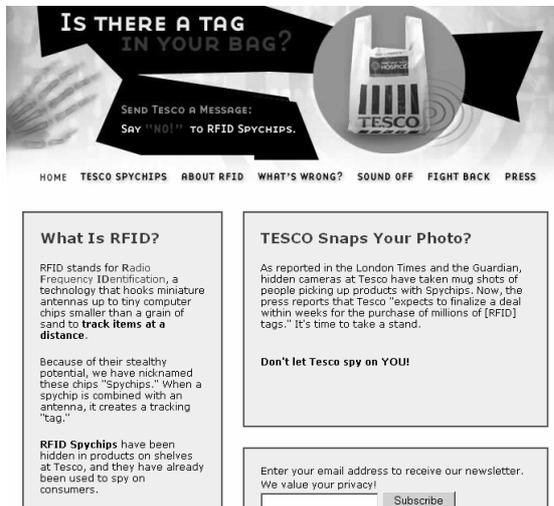
Figure 2: Examples of boycott appeals

The phenomenon that various RFID promoters have begun to adapt their official speak on RFID can also be regarded as an indicator of stigmatisation. British retailer Tesco, for example, never uses the term "RFID" in its communications but rather prefers the term "Radio Barcode". Nokia, again, decided to use the label "Near Field Communication" for its RFID-equipped mobile phones.

5. Managerial Implications

While IS research has led to significant findings on the determinants of technology acceptance, there remains the tricky issue of applying these insights to ensure that an emerging technology is likely to be accepted. This holds particularly true for the case of RFID as a base technology that has no use per se but rather serves as a foundation for a broad variety of technical artefacts. Against this background, this section discusses a set of strategic options that companies have at their disposal in order to influence RFID acceptance positively.

Our framework follows the findings of empirical works that have integrated trust and risk with TAM. The framework depicted in Figure 3 can be regarded as a simplification of these models, since we concentrate only on those factors that can be influenced by a company's actions. On the hand, we focus on the development of "institutional trust" and "interpersonal trust" as described by Gefen et al. (2003b). Furthermore, we add "technology trust" (Lui and Jamieson, 2003) to the model since the consumer's attitude toward RFID as a whole is at the centre of our framework. On the other hand, we consider the two main constructs of TAM, "usefulness" and "ease of use" (Davis, 1989). In contrast to that, other constructs that are

also relevant but can be regarded as virtually static, such as "personal innovativeness" (Lu et al., 2005) and "dispositional trust" (McKnight and Chervany, 2001), lie beyond this scope.
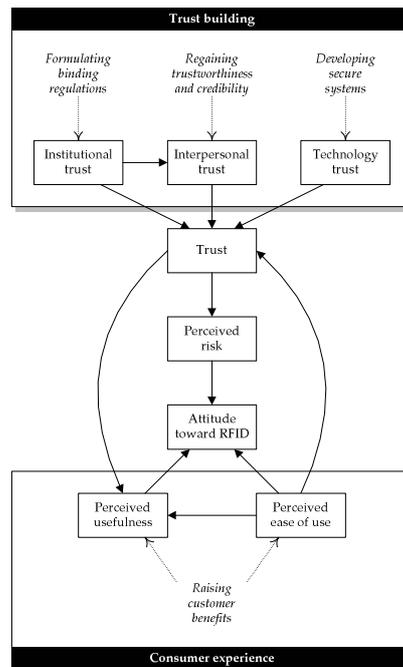

Figure 3: Trust and Risk framework

5.1. Institutional Trust

Institutional trust refers to the security one feels about a situation because of guarantees, regulations, safety nets or other structures (Shapiro, 1987; McKnight et al., 1998; Gefen et al., 2003b). One instrument for the development of institutional trust is the involvement in the official statutory process which requires some knowledge of the fundamentally different approaches to the protection of the private sphere that have established themselves in the USA and Europe (Langheinrich 2005): The European approach of favouring comprehensive, all-encompassing data protection legislation, and the sectoral approach popular in the US that favours voluntary industry regulations whenever possible, employing legal constraints only when absolutely necessary (Smith, 2001; Solove and Rotenberg, 2003). While the discussion about the regulation of RFID employment in Europe has up to now remained limited to the utilisation of already existing statutes, the numerous demands for RFID-specific legislation (e.g. the "RFID Bill of Rights" proposed by Garfinkel, 2002) led to a series of legislative initiatives in individual federal states, whose outcome at the current time is still open (Swedberg, 2004; Atkinson, 2004).

Aside from government regulation, another option for the implementation of privacy-related rules is self-regulation (Swire, 1997). For self-regulation effectively to address privacy concerns, organizations need voluntarily to adopt and implement a set of privacy policies and compliance procedures and enforcement mechanisms, so consumers will have the confidence that an organization is playing by the rules (Culnan and Bies, 2003). An example for this are EPCglobal's Guidelines on EPC for Consumer Products (EPCglobal, 2005). These commit EPCglobal member organisations, (a) to show clearly to the consumer the presence of an EPC-Tag in the product, (b) to inform him/her of the possibilities for removing the tag, (c) to make available further information on the functioning and application of EPC and (d) to guarantee that the EPC does not contain, collect or store any personally identifiable information.

5.2. Interpersonal Trust

The concept of interpersonal trust refers to the relation between the trustor and the trustee, i.e. the object of interpersonal trust is the specific other individual (or party) that one trusts (McKnight and Chervany, 2002). Pavlou and Gefen, 2004 note that interpersonal trust is not entirely independent from other dimensions of trust but is rather positively influenced by institutional trust. One option for the development of interpersonal trust is to formulate processes in such a way that customers gain the impression of "procedural fairness", that is, an appropriate handling of business activities (Culnan and Armstrong, 1999). In this respect, apart from knowledge about procedures, being able to control them through, for example, opt-in choices, constitutes an important factor (Culnan and Bies, 2003).

Furthermore, an open dialogue with customers, independent of individual transactions, plays an important role (Leiss, 2003; Renn, 1991; Seeger et al., 2001). Many of the following symptoms of rather ineffective risk communication manifest themselves in the current privacy debate: (a) denial and defensive information policy, (b) appeasement, (c) aggressive and confrontational interactions as well as polemics, (d) providing information too late, (e) reactive information policy, (f) lack of clarity and comprehensibility of information. As a result of hardening fronts and consensus problems, it is difficult to achieve and develop a constructive dialogue. Nonetheless, the willingness to give interviews, practical demonstrations, cooperate with interest groups, use experts appropriately and so on is over the longer term, successful measures and part of an open and proactive communication culture.

5.3. Technology Trust

Many of the Privacy-Enhancing Technologies proposed for RFID can immediately be regarded as impractical owing to extensive technical requirements, significant complexity for the user or for the fact that various RFID applications are rendered impossible in advance. Furthermore, most of the solutions pass on to the consumer the organisational effort for

privacy protection, similar to an opt-out procedure through the technology (Karjoth and Moskowitz, 2005). Moreover, the additional security acquired is not perceptible and, even worse, reliable verification is impossible (De Jager, 2005).

In contrast to other everyday technical safety mechanisms, for example the brakes of a car, which do not presuppose trust, but rather create it, the PETs mentioned do not provide the user with a direct "look & feel" experience (Juels, 2006). As Günther and Spiekermann (2005) found from an analysis of consumer perceptions, "regardless of privacy-enhancing technology employed, consumers feel helpless toward the RFID environment, viewing the network as ultimately more powerful than they can ever be". As a consequence, it is evident that technology vendors will have to put more emphasis on aspects of user control, simplicity and visual feedback mechanisms in the development of RFID components.

5.4. Usefulness and ease to use

RFID-based technical artefacts themselves bear the potential of increasing technology acceptance through additional services and benefits (Eckfeldt, 2005). An example for this is the usage of RFID in the branches of a retail chain in order to enhance the end-to-end shopping experience, aiming to win customer loyalty by inventing innovative ways of satisfying the new consumer needs (Roussos, 2004). In this context, examples for RFID-based applications that are both useful and easy to use are product information kiosks and self-checkout systems that address the needs of the "self-service consumer" (Bateson 1985, Dabholkar 1995), i.e. consumers who attach great importance to aspects of their shopping experience such as fun, enjoyment, control, and low waiting time, along with an interest in technology-based self-service options. Various surveys indicate a readiness by consumers to accept RFID in connection with improved product security, faster checkouts or easier returns (Gartner, 2003; CGEY, 2005). Metro's reports on the usage of self-checkouts and digital shopping assistants in the Extra Future Store also register an increasing customer acceptance of the new technologies (Metro, 2005).

6. Discussion

The objective of this contribution is to identify, at a relatively early phase of the risk development, strategic options with which RFID suppliers and users can positively influence the public acceptance of the technology. Owing to the fact that the number of consumers who have been confronted with RFID is still very limited, the data on public perceptions of the technology is limited as well. Hence, companies are faced with the dilemma of having to implement risk management strategies early despite neither positive nor negative impacts of the technology are yet fully understood. Regarding our approach, we see the following major issues that RFID adopters need to take into account in strategy development:

First, the use of SARF as a reference model for the analysis of future risk development might be generally inappropriate. Jackson et al. (2005) note that "it is unclear whether SARF can be used as a successful tool of prediction; perhaps it is too fuzzy a framework for this, its value being more as a way of explaining something after it has occurred." Critics of the framework refer to the theoretical value of the framework, the role of mass media, the individual vs. social processes comparison, the amplification metaphor and its strict linearity as an oversimplification of reality (Drevenšek, 2005). Murdock et al. (2003) point out that media can only amplify or attenuate risk if they capture or resonate with an existing public mood, and even then the media are not alone in this function. Furthermore, many consumers are not passive recipients of media messages but sophisticated and "media-savvy" users, i.e. they understand hype and sensationalism when they see it (Petts et al., 2001). The lack of observable attenuating effects in the case of RFID could be an indicator for the deficits of SARF's explanatory and predictive power. It is therefore imaginable that the current controversy and the media reporting on RFID will have no lasting effect on the broader public.

Second, in the same way as the public debate on RFID risks the focus of our analysis was set solely on the perception of privacy risks. It is possible that, for example, triggered by the increasing number of RFID readers on the sales floor, pressure groups change their line of attack and try to shift the focus of public attention to health risks of electromagnetic radiation or other issues. This eventuality does not affect the structure of our framework in itself but certain strategic implications that could be drawn from it. On the one hand, the visual marking of RFID readers and tags in stores, for instance, could be a reasonable option to demonstrate that retailers have nothing to hide. On the other hand, however, this act might also induce the feeling of constantly being exposed to potentially harmful radiation. Furthermore, the deactivation of tags at the point of sale by default could render impossible some RFID applications that are likely to be perceived as very useful, e.g. accelerated warranty claims processing and verification of authentic products and parts.

A third issue could be the underestimation of factors of risk perception that are not covered by our model, e.g. the consumer's social or cultural context. The differences between the valuation of privacy in Western and Asian cultures, for example, could play a much more important role than expected. Bailey and Caidi (2005) present the case of smart card adoption – a technology quite similar to RFID – in Hong Kong and Canada and come to the conclusion that differing cultural notions of privacy affect the acceptance of new information and communication technologies. Sareen (2005) gives the example of India whose citizens like confidential and secure access for their financial transactions first whereas personal privacy, although desirable, is usually of lower priority. Another indicator for the importance of cultural factors could be the fact that the US version of Albrecht and McIntyre's (2005) book on RFID was published under a different title ("The Spychips Threat: Why Christians Should Resist RFID and Electronic Surveillance") and with an additional chapter on the interpretation of RFID as the biblical "Mark of the Beast". In the extreme, these factors could either make any attempt to outweigh risk perceptions with useful RFID applications for the consumer either impossible or superfluous. The same holds for extensions of TAM, e.g. the influence of personal innovativeness.

Fourth, it is conceivable that the RFID issue divides into several sub-issues that further evolve independently with different perceptions of benefits and risks. A possible trigger could

be RFID-based technical artefacts such as Mastercard's PayPass system or Nokia's NFC phones, i.e. RFID technologies that are not perceived as RFID any more. On the one hand, this strategy might be helpful since it saves the particular artefact from general stigmatisation of RFID. On the other hand, it could also be regarded as myopic since it undermines the idea of utilising user-friendly applications in order to foster the acceptance of RFID as a whole.

7. Summary and Outlook

In the year 2001 Sanjay Sarma, Co-founder of the MIT Auto-ID Center, was quoted as saying, "Security concerns will be resolved long before we get to the consumer" (Schmidt, 2001). Today, as we know, this prediction has proved false. As the above analysis has demonstrated, the perception of RFID as a risk has, in the meantime, established itself and developed in a manner similar to other technological risk topics in the past. To what extent the perception of RFID as a risk will reach a crisis, or is likely to decline in significance, remains completely open and depends on the further development of the debate that is currently moving itself in the classical constellation of enterprises vs. NGOs. In this phase the stakeholders are still in a position to exert influence in how aspects come to fruition, as conflict intensifying or conflict extenuating. The demeanour of the RFID suppliers and users at present indicates, if anything, a conflict intensification.

Against this background, the aim of this contribution was to apply findings from the existing body of literature on risk perception and technology acceptance to RFID and to develop a set of strategic options for coping with the challenge of growing public rejection of the technology. The managerial implications that can be drawn from our research are twofold. On the one hand, theories on the development of risk indicate that risk perception is less a purely rational process based on quantifiable facts alone than the result of highly complex interactions on an individual as well as on a social level. It is therefore crucial that affected companies do not limit their view of RFID-related risks to technical problems that, in turn, are solved by additional technical mechanisms. On the other hand, we know from research on technology acceptance that intentions to use a particular technology are not only determined by risk perceptions but also by a range of factors that can actively be influenced, e.g. perceptions of trust and usefulness. Hence, companies implementing RFID in their logistical processes would be well advised to put more emphasis on consumer benefits of technical artefacts as well as risk communications than they do today. Both findings are still waiting to be translated into risk management strategies by RFID vendors and users.

Through the withdrawal from several critical areas of application and the decision not to apply RFID at the individual product level but only to pallets and cases, retailers and their suppliers as well as other RFID users have won some time. However, with the further development of the technology and, at the same time, falling prices, over time a number of applications are likely to become economically viable which entail activated transponders in individual products, which will remain activated beyond purchase. For these reasons, the introduced strategic framework should serve as a starting point for formulating risk management beyond the present predominantly technology-oriented perceptive.

References

Agarwal, R., Prasad, J. (1998) A conceptual and operational definition of personal innovativeness in the domain of information technology. Information Systems Research 9 (2) 204-216.

Agarwal, R., Prasad, J. (1999) Are individual differences germane to the acceptance of new information technologies? Decision Sciences 30 (2) 361-391.

Albrecht, K., McIntyre, L. (2005) Spychips: how major corporations and government plan to track your every move with RFID, Nelson Current, Nashville, TN.

Atkinson, W. (2004) Tagged: The Risks and Rewards of RFID Technology, Risk Management Journal 51 (7) 12–19.

Bailey, S.G.M., Caidi, N. (2005) How much is too little? Privacy and smart cards in Hong Kong and Ontario, Journal of Information Science, 31 (5) 2005, pp. 354–364.

Bateson, J. (1985) Self-Service Consumer: An Exploratory Study, Journal of Retailing 61 (3) 49–76.

Belanger, F., Hiller, J., Smith. W. (2002) Trustworthiness in electronic commerce: The role of privacy, security, and site attributes, Journal of Strategic Information Systems 11 (3/4) 245-270.

Bose, I., Pal, R. (2005) Auto-ID: Managing Anything, Anywhere, Anytime in the Supply Chain, Communications of the ACM 48 (8) 100–106.

Byfield, I. (1996) Developments in RFID, Sensor Review 16 (4) 4–5.

Cantwell, B. (2002) Why Technical Breakthroughs Fail: A History of Public Concern with Emerging Technologies, Working Report, Auto-ID Center, MIT, Cambridge (MA).

Cas, J. (2004) Privacy in Pervasive Computing Environments – A Contradiction in Terms?, IEEE Technology and Society Magazine 24 (1) 24–33.

CASPIAN (2003) Scandal: Wal-Mart, P&G Involved in Secret RFID Testing, Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN). (URL: http://www.spychips.com/press-releases/broken-arrow.html)

Cavoukian, A. (2004) Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology, Information and Privacy Commissioner Ontario, Toronto.

CGEY (2004) RFID and Consumers: Understanding Their Mindset, Cap Gemini Ernst & Young, New York (NY).

Culnan, M.J., Armstrong, P.K. (1999) Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, Organization Science 10 (1) 104–116.

Culnan, M.J., Bies, R.J. (2003) Consumer Privacy: Balancing Economic and Justice Considerations, Journal of Social Issues 59 (2) 323–342.

Dabholkar, P. (1996) Consumer evaluations of new technology-based self-service options: An investigation of alternative models of service quality, International Journal of Research in Marketing 13 (1) 29–51.

Davis, F. (1989) Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology, MIS Quarterly, 13 (3) 319-339.

Davis, F., Bagozzi, R., Warshaw, P. (1992) Extrinsic and Intrinsic Motivation to Use Computers in the Workplace, Journal of Applied Social Psychology 22 (14) 1111-1132.

De Jager, P. (2005) Experimenting on Humans Using Alien Technology, In: Garfinkel, S., Rosenberg, B. (eds.) (2005) RFID, Addison-Wesley, Upper Saddle River, NJ, pp. 439–449.

Douglas, M.T., Wildavsky, A.B. (1982) Risk and Culture: an Essay on the Selection of Technical and Environmental Dangers. University of California Press, Berkeley, CA.

Downes, L. (2003) Don't fear new bar codes. USA Today: 23A, September 25 (2003) (URL: http://www.usatoday.com/usatonline/20030925/5532478s.htm)

Drevenšek, M. (2005) Negotiation as the Driving Force of Environmental Citizenship, Environmental Politics 14 (2) 226-238.

Duce, H. (2003) Public Policy: Understanding Public Opinion, Executive Briefing, Auto-ID Center, MIT, Cambridge, MA.

Eckfeldt, B. (2005) What Does RFID Do for the Consumer?, Communications of the ACM 48 (9) 77-79.

EPCglobal Inc. (2005) Guidelines on EPC for Consumer Products, Lawrenceville, NJ.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., Combs, B. (1978) How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. Policy Sciences 9 (2) 127–152.

Flynn, J., Peters, E., Slovic, P., Mertz, C.K. (2001) Risk, media, and stigma at Rocky Flats, In: Flynn, J., Slovic, P., Kunreuther, H. (eds.), Risk, media, and stigma: Understanding public challenges to modern science and technology. Earthscan, London, pp. 309-327.

Garfinkel, S. (2002) An RFID Bill of Rights, Technology Review 105 (8) 35.

Gartner (2003) Retail Question & Answer: U.S., U.K. Consumers Will Accept RFID in Exchange for Benefits, Gartner Group International, Stamford, CT.

Gefen D., Rao, S., Tractinsky, N. (2003a) The Conceptualization of Trust, Risk and their Relationship in Electronic Commerce: The Need for Clarification, 36th Hawaii International Conference on System Sciences, Maui, HW.

Gefen, D., Karahanna, E., Straub, D.W. (2003b) Trust and TAM in Online Shopping: An Integrated Model, MIS Quarterly 27 (1) 51-90.

Günther, O., Spiekermann, S. (2005) RFID and the Perception of Control: The Consumer's View, Communications of the ACM 48 (9) 73–76.

Harding, R. (1998) Environmental Decision-making: the roles of scientists, engineers and the public, The Federation Press, Sydney.

Hughes, S. (2005) P&G: RFID and privacy in the supply chain, In: Garfinkel, S., Rosenberg, B. (eds.) (2005) RFID, Addison-Wesley, Upper Saddle River, NJ, pp. 397-412.

Jackson, J., Allum, N. and Gaskell, G. (2005) Perceptions of Risk in Cyber Space, In: R. Mansell, R., Collins, R. (eds.), Trust and Crime in Information Societies, Edward Elgar, London.

Jarvenpaa, S.L., Tractinsky, N., Vitale, M. (1999) Consumer Trust in an Internet Store, Information Technology and Management 1 (12) 45-71.

Jones, K.E. (2001) BSE, Risk and the Communication of Uncertainty: A Review of Lord Phillips' Report from the BSE Inquiry, Canadian Journal of Sociology 26 (4) 655–666.

Juels, A. (2006) RFID Privacy: A Technical Primer for the Non-Technical Reader, In Strandburg, K., Raicu, D.S. (eds.), Privacy and Technologies of Identity: A Cross-Disciplinary Conversation, Springer, New York, NY, pp. 57-73.

Juels, A., Rivest, R., Szydlo, M. (2003) The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, In: Proceedings of the ACM Conference on Computer and Communications Security, ACM Press, New York, NY, pp. 103–111.

Karjoth, G., Moskowitz, P. (2005) Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced, Research Report RC23710, IBM Research Division, Zurich / Yorktown Heights, NY.

Kasperson, R.E. (1992) The social amplification of risk - progress in developing an integrative framework, In: Krimsky, S., Golding, D. (eds.), Social Theories of Risk, Praeger, Westport, CT, pp. 153-178.

Kasperson, R.E., Jhaveri, N., Kasperson, J.X. (2001) Stigma and the social amplification of risk: Toward a framework for an analysis, In: Flynn, J., Slovic, P., Kunreuther, H. (eds.), Risk, media, and stigma: Understanding public challenges to modern science and technology, Earthscan, London, pp. 9-27.

Pidgeon, N., Kasperson, R.E., Slovic, P. (eds.) (2003) The Social Amplification of Risk, Cambridge University Press, Cambridge.

Knights, D., Nobel, F., Vurdubakis, T., Willmott, H. (2001) Chasing shadows: control, virtuality and the production of trust, Organization Studies 22 (2) 311–336.

Kumar, R. (2003) Interaction of RFID Technology and Public Policy. RFID Privacy Workshop @ MIT, Boston, MA.

Kunreuther, H., Slovic, P. (2001) Coping with Stigma, In: Flynn, J., Slovic, P., Kunreuther, H., Risk, Media and Stigma, Earthscan, London, pp. 331-352.

Langheinrich, M. (2005) Personal Privacy in Ubiquitous Computing – Tools and System Support, Ph.D. thesis No. 16100, ETH Zurich, Zurich.

Leiss, W. (2003) Searching for the public policy relevance of the risk amplification framework. In: Pidgeon, N., Kasperson, R.E., Slovic, P. (eds.): The Social Amplification of Risk. Cambridge University Press, Cambridge, pp. 355 – 373.

Lessig, L. (1999) Code and Other Laws of Cyberspace, Basic Books, New York, NY.

Lewicki, R.J., Bunker, B.B. (1995) Trust in relationships: A model of trust development and decline. In: B.B. Bunker and J.Z. Rubin (eds.), Conflict, Cooperation, and Justice. Jossey-Bass, San Francisco, CA, pp. 133-173.

Lu, J., Yaob, J.E., Yu, C.-S. (2005) Personal innovativeness, social influences and adoption of wireless Internet services via mobile technology, Journal of Strategic Information Systems 14 (2005) 245–268.

Luhmann, N. (1979) Trust and power. Wiley, Chichester.

Lui, H.K., Jamieson, R. (2003) Integrating trust and risk perceptions in business-to-consumer electronic commerce with the technology acceptance model, European Conference on Information Systems (ECIS 2003), Naples.

Mathieson, K. (1991) Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior, Information Systems Research 2 (3) 173-191.

Mayer, R.C., Davis, J.H., Schoorman, F.D. (1995) An integrative model of organizational trust, Academy of Management Review, 20 (3) 709-734.

McKnight, D.H., Chervany, N. (2001) Conceptualizing trust: a typology and ecommerce customer relationships model, 34th Hawaii International Conference on System Sciences, Maui, HW.

McKnight, D.H., Chervany, N.L. (2002) What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology, International Journal of Electronic Commerce and Business Media 6 (2) 35-59.

McKnight, D.H., Cummings, L.L., Chervany, N.L. (1998) Initial trust formation in new organizational relationships. Academy of Management Review 23 (3) 472–490.

McKnight, D.H.; Choudhury, V., Kacmar, C. (2002) Developing and Validating Trust Measures for e-Commerce: An Integrative Typology, Information Systems Research 13 (13) 334-359.

Metro (2004) RFID-Newsletter, No. 3/2004, Metro Group, Düsseldorf.
(URL: http://www.future-store.org/servlet/PB/s/15p26618bz5qr1uig2uo20f9m1ypmm rn/show/1004022/RFIDnet-Newsletter-03-dt_04-11-10.pdf)

Metro (2005) Customer satisfaction at the Future Store, Metro Group, Düsseldorf. (URL: http://www.future-store.org/servlet/PB/-s/t3khrl2kphfs1qfsv5w2elyaiypstgs/ show/1004489/off-Presse-Pressemat-2JahreFSI-engl_05-04-27.pdf)

Moon, J.-W., Kim, Y.-G. (2001) Extending the TAM for a World-Wide-Web context, Information & Management 38 (4) 217-230.

Morris, M.G., Venkatesh, V. (2000) Age differences in technology adoption decisions: Implications for a changing work force, Personnel Psychology 53 (2) 375-403.

Murdock, G., Petts, J., Horlick-Jones, T. (2003) After Amplification: Rethinking the Role of the Media in Risk Communication, In: Pidgeon, N., Kasperson, R.E., Slovic, P. (eds.): The Social Amplification of Risk, Cambridge University Press, Cambridge, pp. 159-174.

Murray, C.J. (2003) Privacy Concerns Mount Over Retail Use of RFID, EE Times, 1 Dec 2003. (URL: http://www.techweb.com/wire/26803432)

Pavlou, P.A. (2001) Integrating Trust in Electronic Commerce with the Technology Acceptance Model: Model Development and Validation, 7th Americas Conference in Information Systems, Boston, MA.

Pavlou, P.A. (2003) Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model, International Journal of Electronic Commerce 7 (3) 101-134.

Pavlou, P.A., Gefen, D. (2004) Building Effective Online Marketplaces with Institution-Based Trust, Information Systems Research 15 (1) 37-59.

Perrin, S. (2005) RFID and Global Privacy Policy, In: Garfinkel, S., Rosenberg, B. (eds.) (2005) RFID, Addison-Wesley, Upper Saddle River, NJ, pp. 15–36.

Petts, J., Horlick-Jones, T., Murdock, G. (2001) Social Amplification of Risk: The Media and the Public, Health and Safety Executive Contract Research Report 329/200, HSE Books, Sudbury.

Ratnasingham, P., Pavlou, P.A. (2002) Technology trust: the next value creator in B2B electronic commerce, IRMA International Conference, Seattle, WA.

Renn, O. (1991) Strategies of risk communication: Observations from two participatory experiments, In: Kasperson, R.E., Stallen, P.J.M. (eds.), Communicating Risks to the Public, Kluwer, Dordrecht, pp. 457–481.

Renn, O., Levine, D. (1991) Credibility and trust in risk communication, In: Kasperson, R.E., Stallen, P.J.M. (eds.), 1990. Communicating Risks to the Public, Kluwer, Dordrecht, pp. 175–218.

Rieback, M.R., Crispo, B., Tanenbaum, A.S. (2006) Is Your Cat Infected with a Computer Virus?, 4th IEEE Intl. Conf. on Pervasive Computing and Communications. (IEEE PerCom2006), Pisa.

Roussos, G. (2004) Building Consumer Trust in Pervasive Retail, International Workshop "Information Sharing and Privacy", Tokyo.

Sareen, B. (2005) Asia: Billions awaken to RFID, In: Garfinkel, S., Rosenberg, B. (eds.) (2005) RFID, Addison-Wesley, Upper Saddle River, NJ, pp. 451–466.

Sarma, S. (2001) Towards the 5¢ Tag, Working Report, Auto-ID Center, MIT, Cambridge, MA.

Sarma, S. (2005) A History of the EPC, In: Garfinkel, S., Rosenberg, B. (eds.) (2005) RFID, Addison-Wesley, Upper Saddle River, NJ, pp. 37–55.

Sarma, S., Weis, S., Engels, D. (2002) RFID Systems, Security & Privacy Implications, In: Lecture Notes In Computer Science, Vol. 2523, Springer, London, pp. 454–469.

Schmidt, C. (2001) Beyond the Bar Code, Technology Review 104 (2) 80–85.

Shapiro, S. (1987) The social control of impersonal trust. American Journal of Sociology 93 (3) 623-658.

Seeger, M.W., Sellnow, T.L., Ulmer, R.R. (2001) Public relations and crisis communication: Organizing and chaos, In Heath, R.L. (ed.), Public Relations Handbook, Sage, Thousand Oaks, CA, pp. 155-166.

Slovic P., Fischhoff, B., Lichtenstein, S. (1981) Facts and Fears: Societal Perception of Risk, Advances in Consumer Research 8 (1) 497–502.

Slovic, P. (1992) Perception of risk: Reflections on the psychometric paradigm. In: Krimsky, S., Golding, D. (eds.), 1992. Social theories of risk, Praeger, Westport, CT, pp. 117–152.

Slovic, P., Flynn, J. H., Layman, M. (1991) Perceived risk, trust, and the politics of nuclear waste. Science, 254 1603-1607.

Smith, H.J. (2001) Information Privacy and Marketing: What the U.S. should (and shouldn't) learn from Europe, California Management Review 43 (2) 8–33.

Solove, D.J., Rotenberg, M. (2003) Information Privacy Law, Aspen Publishers, New York, NY.

Spinello, R.A. (1998) Privacy Rights in the Information Economy, Business Ethics Quarterly 8 (4) 723–742.

Swedberg, C. (2004) States Move on RFID Privacy Issue, RFID Journal, April 30 (2004).

Swire, P.P. (1997) Markets, self-regulation, and government enforcement in the protection of personal information, In: U.S. Department of Commerce (ed.), Privacy and self-regulation in the information age, Washington, D.C., pp. 3–19.

Taylor, S., Todd, P.A. (1995) Assessing IT Usage: the Role of Prior Experience, MIS Quarterly 19 (4) 561-570.

Venkatesh, V. (1999) Creation of Favorable User Perceptions: Exploring the Role of Intrinsic Motivation, MIS Quarterly 23 (2) 239-260.

Venkatesh, V. (2000) Determinants of Perceived Ease of Use: Integrating Perceived Behavioral Control, Computer Anxiety and Enjoyment into the Technology Acceptance Model, Information Systems Research 11 (4) 342-365.

Want, R. (2004) The Magic of RFID, ACM Queue 2 (7) 41–48.

Watson, T., Osborne-Brown, S., Longhurst, M. (2002) Issues Negotiation – investing in stakeholders. Corporate Communications 7 (1) 54–61.

Weinberg, J. (2005) RFID, Privacy, and Regulation, In: Garfinkel, S., Rosenberg, B. (eds.) (2005) RFID, Addison-Wesley, Upper Saddle River, NJ, pp. 83–97.

Weis, S., Sarma, S., Rivest, R., Engels, D. (2003) Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: Lecture Notes in Computer Science, Vol. 2802, Springer, London, pp. 454–469.

Wu, I.-L., Chen, J.-L. (2005) An extension of trust and TAM model with TPB in the initial adoption of on-line tax: an empirical study, International Journal of Human-Computer Studies 62 (6) 784-808.