February 2005

Wahrnehmung und Management RFIDbezogener Risiken für die informationelle Selbstbestimmung

Frédéric Thiesse
Universität St. Gallen

Elgar Fleisch
Universität St. Gallen

In: Ferstl, Otto K, u.a. (Hg) 2005. *Wirtschaftsinformatik 2005: eEconomy, eGovernment, eSociety*; 7. Internationale Tagung Wirtschaftsinformatik 2005. Heidelberg: Physica-Verlag

ISBN: 3-7908-1574-8

Wahrnehmung und Management RFID-bezogener Risiken für die informationelle Selbstbestimmung

Frédéric Thiesse, Elgar Fleisch
Universität St. Gallen

Zusammenfassung: Der vorliegende Beitrag untersucht die Wahrnehmung von RFID-Technologie in der Öffentlichkeit als Risiko für die informationelle Selbstbestimmung, identifiziert Handlungsbedarfe für das Risikomanagement von Technologieanbietern/–anwendern und diskutiert mögliche Handlungsoptionen.

Schlüsselworte: RFID, Privacy, Datenschutz, Risikokommunikation

1 Einführung

Technologien und Anwendungen der Radiofrequenzidentifikation (RFID) erfahren in diesen Tagen ein enormes Interesse seitens der Forschung und betrieblichen Praxis, darüber hinaus aber auch in Medien und Gesellschaft. Während sich Unternehmen von RFID vor allem operative Effizienzgewinne in ihren internen Prozessen erhoffen und Kosten/Nutzen-Gesichtspunkte in den Vordergrund stellen, wurden in den vergangenen Monaten auch Stimmen laut, die auf die möglichen Risiken des RFID-Einsatzes verweisen und eine umfassende Technikfolgenabschätzung fordern. So zählt bspw. die Rückversicherung Swiss Re RFID bzw. Technologien des Pervasive Computing im Allgemeinen neben Nanotechnologie und der Creutzfeld-Jacob-Krankheit zu den derzeit drängendsten „emerging risks“ [Sch04].

Die mit RFID assoziierten Risiken umfassen sowohl direkte Auswirkungen der elektromagnetischen Strahlung auf die Gesundheit als auch indirekte ökonomische Konsequenzen wie den auf die zunehmende Automatisierung u. U. folgenden Personalabbau [Duc03]. Die mit Abstand am häufigsten geäußerte Befürchtung betrifft jedoch die Möglichkeiten des Missbrauchs der mittels RFID generierten Daten und unerwünschte Eingriffe in die Privatsphäre des Einzelnen. Hier reichen die Ängste der Bevölkerung von der Analyse und Auswertung des individuellen Verbraucherverhaltens bis hin zur allgegenwärtigen Überwachung durch die als „Schnüffel-Chips im Joghurtbecher“ [Zei04] titulierten RFID-Transponder.

Zusätzlich angeheizt wird die Diskussion durch Aktionen und Kampagnen von „Pressure Groups“ [Wha98] wie der US-amerikanischen Vereinigung „Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)“ oder des deutschen „Vereins zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. (FoeBuD)“. Bspw. führten die medienwirksame Verleihung des sog. „Big Brother Award“ an die Metro AG und eine Demonstration vor dem Metro Future Store in Rheinberg am 28.2.2004 letztlich zu einem Rückzug der dort eingesetzten RFID-basierten Kundenkarten. Dass diese Aktionen keine Einzelfälle darstellen, zeigen weitere Beispiele in Europa und den USA, z.B. CASPIANs Aufruf zum Boykott von Gillette-Produkten aufgrund von Tests mit RFID-Transpondern in Rasierklingenpackungen (s. Abbildung 1).

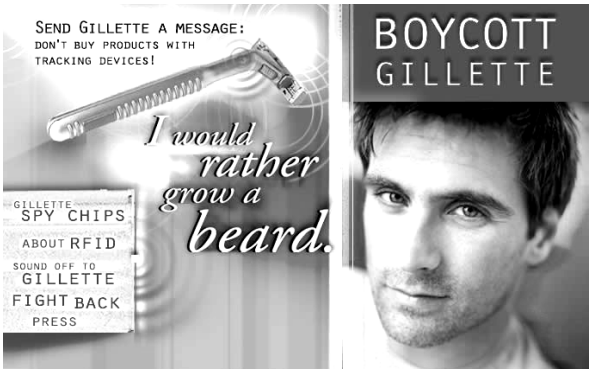

Abbildung 1: Webseite www.boycottgillette.com

In der Auseinandersetzung mit RFID-Gegnern nahmen Handel, Produzenten und Technologieanbieter gegenüber der zuweilen stark emotionalisierten Debatte bisher eine eher defensive, reagierende Position ein, die von einer sehr zurückhaltenden Informationspolitik und einem Rückzug auf eine Argumentation rund um technische Eigenschaften von RFID gekennzeichnet war. Wie die Entwicklung von Risikothemen in der Vergangenheit vielfach gezeigt hat, ist einer solchen Strategie jedoch in den meisten Fällen kein Erfolg beschieden, sondern birgt vielmehr die Gefahr einer massiven Ablehnung seitens der Kunden und damit eines Scheiterns der Technologieeinführung in sich.

Vor diesem Hintergrund unternimmt der vorliegende Beitrag den Versuch einer Analyse der Wahrnehmung von RFID in der Öffentlichkeit sowie der gegen ihre Anwendung vorgebrachten Argumente und diskutiert mögliche Instrumente zur Entwicklung einer umfassenden Strategie zum Umgang mit dem Risikothema RFID. Dabei bildet die Technologiebetrachtung nur einen Aspekt unter anderen. Zu diesem Zweck wird im Folgenden nach der Einführung der grundlegenden Konzepte auf Basis von Nachrichtenmeldungen und Internet-Diskussionsforen die Problemstellung herausgearbeitet. Darauf aufbauend werden im Anschluss Handlungsebenen identifiziert und mögliche Handlungsoptionen vorgestellt.

2 Grundlagen

2.1 RFID

RFID ist eine Technologie zur automatischen Identifikation physischer Objekte wie Industriecontainern, Paletten, Getränkedosen oder auch Personen per Funk. Der Identifikationsvorgang erfolgt über einen in oder auf dem jeweiligen Objekt befindlichen Transponder (auch „Tag" oder „Smart Label" genannt), der berührungslos von einem mit einer Antenne ausgestatteten Lesegerät angesprochen werden kann. Transponder werden in unterschiedlichsten Bauformen hergestellt, operieren in verschiedenen Frequenzbändern und haben entweder eine eigene Batterie (Aktivtransponder) oder werden über das elektromagnetische Feld des Lesers mit Energie versorgt (Passivtransponder).

Trotz des aktuellen Hypes rund um RFID ist die Technologie keineswegs neu: Die erste wissenschaftliche Publikation geht auf das Jahr 1948 zurück; die kommerzielle Verwertung begann in den 60er Jahren des letzten Jahrhunderts mit der Entwicklung von Systemen zur elektronischen Artikelsicherung (EAS) [Lan01]. Gründe für den erst in jüngster Zeit rapide zunehmenden Run auf RFID sind vielmehr in der fortgeschrittenen Miniaturisierung, Reife und Standardisierung zu suchen sowie im stetigen Preisverfall, der den RFID-Einsatz in mehr und mehr Bereichen wirtschaftlich sinnvoll erscheinen lässt.

Gegenüber dem heute zur Güteridentifikation üblichen Barcode unterscheidet sich RFID durch die Möglichkeit zur [Cav04; Gar02]

- Pulkerfassung,
- Identifikation ohne Sichtverbindung („line of sight"),
- eindeutigen Identifikation jedes einzelnen Objekts,
- Datenspeicherung auf dem Objekt sowie
- hohe Robustheit gegenüber Umwelteinflüssen und Zerstörung.

Die Gemeinsamkeit aller RFID-Transponder besteht in einer eindeutigen ID-Nummer, die z.B. bei der Produktkennzeichnung eine Erkennung nicht mehr nur auf Produkttypen- sondern auf Instanzenebene erlaubt. Das in den meisten derzeitigen Roll-out-Planungen von Unternehmen wie Wal-Mart, Airbus oder dem amerikanischen Department of Defense vorgesehene RFID-Nummerierungsschema ist der „Electronic Product Code (EPC)", der in den Jahren 1999 bis 2003 am Auto-ID Center des MIT entwickelt wurde. Der EPC ist eine 96 Bit umfassende Zahl, in die Informationen über den Hersteller, den Produkttyp und eine Seriennummer einkodiert sind [Sar+01].

Mit diesen Fähigkeiten bildet RFID eine Grundlage für verschiedene Anwendungen des Ubiquitous bzw. Pervasive Computing, dessen Vision eine Welt „smarter" Alltagsgegenstände ist, deren Gebrauchswert über ihre physische Funktion hinaus mit Hilfe digitaler Logik ergänzt und erweitert wird [Fer02; Mat03]. Das betriebswirtschaftliche Potenzial des Ubiquitous Computing liegt in der Überwindung des Medienbruchs zwischen realer und informatischer Welt [Fle01] durch Integration von physischen Abläufen mit Informationssystemen ohne den Zwischenschritt einer manuellen Datenerfassung. In umgekehrter Richtung können Entscheidungen vom IS an das Objekt delegiert werden, z.B. in Form eines Transportbehälters, der seinen Weg durch die Lieferkette ohne übergeordnete Planungsinstanz selbständig bestimmt.

Typische Einsatzgebiete von RFID liegen dementsprechend vor allem im Bereich des Supply Chain Managements, wo die Technologie einen vereinfachten Wareneingang und –ausgang, automatische Bestandskontrolle im Lager bzw. auf der Verkaufsfläche, Diebstahlschutz, Fälschungssicherheit usw. ermöglicht. Weitere Anwendungspotenziale ergeben sich in den Bereichen des Produktlebenszyklusmanagement (z.B. Rückrufaktionen, Wartung & Service) und Kundenbeziehungsmanagement (z.B. individualisierte Produktinformation, Marktforschung) bis hin zu neuartigen Geschäftsmodellen durch nutzenbasierte Bezahlung oder lieferantengeführte Bestände [FlDi03].

2.2 Risiken

Die Einführung neuer Technologien ist fast immer auch mit einer Diskussion über die mit ihr verbundenen Risiken verknüpft. Der Begriff des Risikos bezeichnet dabei im Gegensatz zur realen Gefahr ein soziales Konstrukt [Slo99; Tac01], dessen individuelle Wahrnehmung von zahlreichen Faktoren bestimmt wird, wie z.B. Bildung, Beruf, Zugehörigkeit zu einer bestimmten Subkultur usw. [Fin02, WiHe89]. Was für den einen eine ernstzunehmende, nicht akzeptable Gefahr darstellt, kann so aus anderer Perspektive als eher unbedrohlich erscheinen.

Dabei unterscheiden sich insb. Expertenurteile drastisch von der Risikobewertung durch Laien [Slo+81]. Während der Experte Risiken vor allem quantitativ definiert und andere Formen der Riskowahrnehmung typischerweise als irrational ablehnt, hat der Laie einen eher intuitiven, qualitativen Risikobegriff, der nicht auf das Produkt von Schadenswahrscheinlichkeit und –ausmaß reduziert ist [ReLe91]. Inwiefern ein Risiko von Laien als hoch oder niedrig eingeschätzt wird, ist wesentlich von der Bekanntheit des Risikos, der Freiwilligkeit der Risikoübernahme, der Schrecklichkeit der Folgen bzw. dem katastrophischen Potenzial sowie dem Nutzen der Technologie abhängig [Hen90; Slo92]. So wird bspw. regelmäßig das Risiko durch radioaktive Strahlung oder BSE geschädigt zu werden weit höher eingeschätzt als die Möglichkeit eines Verkehrs- oder Arbeitsunfalls, obwohl die Statistik eine deutlich andere Sprache spricht [TrMc03].

Eine wesentliche Schlussfolgerung für den Umgang mit Risiken ist daher, dass Kommunikation über diese sich nicht allein um die Konsequenzen bei Eintreffen des zunächst nur potenziellen Risikos drehen darf, sondern auch den Risikoentstehungsprozess selbst beeinflussen muss [Jon01]. Ist das Risikothema hingegen erst einmal etabliert, können Unternehmen und Staat nur noch reagieren [Wie94]. Dies wird darüber hinaus durch den Umstand erschwert, dass der Einzelne die zur Risikobeurteilung herangezogenen Informationen als glaubwürdiger einschätzt, wenn sie z.B. von Ärzten, Freunden oder Umweltschutzgruppen stammen als von staatlichen Behörden, Verbänden oder einzelnen Firmen [TrMc03].

Eine besondere Rolle bei der Risikowahrnehmung kommt in diesem Zusammenhang den Medien zu. Einerseits dienen sie der Öffentlichkeit als wichtigste Informationsquelle zu IT-bezogenen Risiken. So rangieren Fernsehen und Tageszeitungen deutlich vor allen anderen Quellen, während Informationsmaterial der Technologieanbieter selbst nur von einer kleinen Minderheit wahrgenommen wird [SjFr01]. Andererseits verstärken Medien die ohnehin bereits vorhandenen Informationsasymmetrien durch eine Präferenz für negative Ereignisse in Ihrer Berichterstattung [KoKl91; WiHe89].

Eine weitere Schwierigkeit, die speziell den Umgang mit technischen Risiken betrifft, ist die in den letzten Jahrzehnten grundsätzlich gewandelte Einstellung der Gesellschaft gegenüber dem technischen Fortschritt insgesamt. Während in den 60er Jahren des letzten Jahrhunderts die überwiegende Mehrheit der bundesdeutschen Bevölkerung Technik als Segen betrachtete, haben seit den 80er Jahren die Technologieskeptiker deutlich die Oberhand gewonnen [WiHe89]. Dies legt die Vermutung nahe, dass in Zeiten von Wirtschaftswunder und Mondlandung viele der aktuellen Technologiediskussionen grundsätzlich anders verlaufen wären als heute.

Entwickelt sich ein Risikothema zu einer Krise, so kann dies für betroffene Unternehmen schwerwiegende Konsequenzen haben [Wat+02], wie Beispiele der letzten Jahre zeigen (siehe [Can02] für eine Sammlung von Fallstudien). Dies können unmittelbare Umsatzeinbussen durch den Rückzug aus einzelnen Märkten sein, aber auch langfristigere Schäden des Unternehmens- oder Markenimage, negative Auswirkungen auf Börsenkurse und Investoren oder politische Auflagen und Beschränkungen durch den Gesetzgeber [Wie94]. Um dies zu verhindern, ist ein frühzeitiges und professionelles Risikomanagement vonnöten, welches Konfliktеskalationen vermeidet, bevor das Problem mit fortschreitender Entwicklung vom Unternehmen nicht mehr beeinflusst werden kann. Das Ziel aller Anstrengungen ist dabei die Vermittlung von Wissen, vor allem aber der Aufbau von Vertrauen gegenüber den involvierten Institutionen [Sie01]. Dies gilt im Besonderen auch für die Informations- und Kommunikationstechnik, in deren Zusammenhang zumeist mentale, soziale und politische Risiken diskutiert werden [Jun91].

2.3 Privacy

Eine der allerersten Formulierungen eines Rechts auf Privatheit geht zurück auf Warren und Brandeis, die 1890 ihr Konzept als „the right to be let alone" [WaBr90] definierten. Ausschlaggebend für die Beschäftigung mit dem Thema war damals noch die Berichterstattung der Bostoner Regenbogenpresse sowie die zunehmende Verbreitung von Fotoapparaten: „[…] and numerous mechanical devices threaten to make good the predicition that 'what is whispered in the closet shall be proclaimed from the house-tops'."

In der Neuzeit sind es vor allem Informations- und Kommunikationstechnologien, die als Bedrohung der individuellen Privatsphäre gesehen werden. Im Gegensatz zur „physical privacy", die sich auf den physischen Zugriff auf eine Person bezieht, steht im Zusammenhang mit IuK-Technologien insb. die „information privacy" (zu Deutsch etwa: „informationelle Selbstbestimmung") im Vordergrund [Smi01]. Den Begriff beschreibt z.B. Westin als „the right to control information about oneself" [Wes67]. Die Herausgabe von persönlichen Informationen ist dabei auf der einen Seite ein alltäglicher notwendiger Vorgang, ohne den ein soziales oder ökonomisches Miteinander nicht möglich wäre [Wes03]. Auf der anderen Seite hat der Einzelne in der heutigen Zeit aufgrund des Einsatzes von IT nahezu keine Chance mehr, die Folgen dieser Offenheit für seine Person abzuschätzen.

Die neue Bedrohung von Privatheit hat ihre Grundlage in der Möglichkeit zur dauerhaften Speicherung und Verknüpfung von Informationen über das Individuum: Hatte vor der Einführung von Computertechnik in wirtschaftliche Abläufe persönliche Information noch keinen greifbaren Wert über die einzelne Transaktion hinaus und entzog sich einer weiteren Verwendung, wurde es so auf einmal möglich, aus zahlreichen atomaren Einzeldaten detaillierte Profile von Kunden und ihrem Kaufverhalten zu erstellen [CuBi03; Spi98].

Mit RFID und anderen ubiquitären Technologien entsteht nun eine neue Qualität der Datenerhebung über die bisher gängige Praxis der Informationsgewinnung aus Kreditkartentransaktionen oder Telefonverbindungen hinaus durch

- die räumliche und zeitliche Ausdehnung von Beobachtungsaktivitäten,
- die fehlende Erkenn- und Rekonstruierbarkeit der Datenerhebung,
- die Erhebung neuer Datentypen durch Echtzeitüberwachung,
- den immer weniger nachvollziehbaren Erhebungsgrund sowie
- den unkontrollierbaren Datenzugriff durch extreme Interkonnektivität [Lan04].

Im Fall von RFID entsteht die Privacy-Problematik insb. durch die weltweit eindeutige Identifizierbarkeit jedes Gutes und die mögliche Verknüpfung mit dem Besitzer, welches grundsätzlich ein automatisches Tracking von Personen möglich macht [Sar+02].

3 Analyse der öffentlichen Diskussion

Im Folgenden sollen die Darstellung und Wahrnehmung von Risiken der RFID-Technologie in Bezug auf Privacy genauer untersucht werden. Da sowohl Anti-RFID-Kampagnen in Form diverser Homepages als auch die Berichterstattung und deren öffentliche Diskussion zu einem großen Teil im Internet stattfinden, liegt es nahe, dieses Medium als Ausgangspunkt für die weitere Analyse heranzuziehen. Den nachfolgenden Aussagen liegt eine Untersuchung auf Basis der „7-Tage-News" des Heise-Verlags (www.heise.de) zugrunde, einem auf IT spezialisierten Newsticker eines Herausgebers mehrerer Computermagazine im deutschsprachigen Raum. Diese Auswahl erscheint geeignet, da a) der Fokus auf IT eine große Zahl RFID-bezogener Nachrichten erwarten lässt, b) der Inhalt sich jedoch nicht nur an ein Fachpublikum richtet und c) die an jeden Newseintrag angeschlossenen Diskussionsforen eine unmittelbare Betrachtung der Reaktion auf einzelne Nachrichten erlaubt (vgl. [Ric01] für eine Analyse der Diskussion von Risikothemen in Internet-Newsgroups am Beispiel BSE).

In einem ersten Schritt wurden über eine Volltextsuche nach den Stichworten „RFID" und „Transponder" alle relevanten RFID-Nachrichten der letzten Jahre ermittelt, wobei Texte, die sich auf andere Themen (z.B. TV-Satelliten) bezogen manuell wieder aus der Liste entfernt wurden. Anschließend wurden all jene Nachrichten identifiziert, die die Auswirkung von RFID auf information privacy zum Thema hatten. Als Resultat dieses Untersuchungsschritts ergibt sich Abbildung 2, in der die chronologische Abfolge der gesammelten Nachrichten bis Ende Mai 2004 entlang eines Zeitstrahls dargestellt ist.

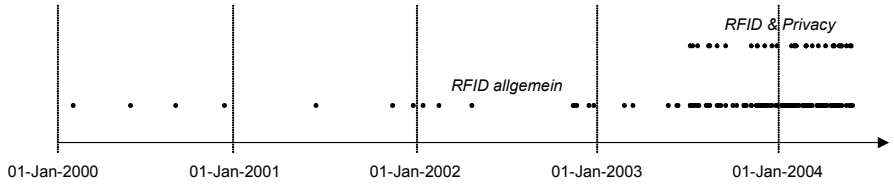

Abbildung 2: RFID-bezogene Nachrichten im Heise-Newsticker

Wie sich hier zeigt, wurde Privacy Mitte 2003 schlagartig zum Thema und ist seither unmittelbar mit RFID verknüpft bzw. als Risikothema etabliert. Beginn dieser Entwicklung war eine Meldung vom 8.7.2003 über die Veröffentlichung 68 scheinbar vertraulicher Dokumente über die Pläne des Auto-ID Centers und seiner Sponsoren für die RFID-Einführung durch die Organisation CASPIAN. Der Beitrag nannte als Motivation für den Einsatz der Technik u.a. die Möglichkeit, das Kaufverhalten und die finanziellen Verhältnisse von Verbrauchern ohne deren Wissen zu analysieren. Darüber hinaus wurde passiven RFID-Transpondern die Fähigkeit zugeschrieben, über bis zu 30 Meter hinweg identifizierbar zu sein.

Beobachtet man den Umgang von Technologieanbietern und Anwendern mit derartigen Meldungen im weiteren Zeitverlauf, so fällt ein sich wiederholendes Muster aus Aktion und Reaktion auf, wobei Unternehmen gegenüber den agierenden Pressure Groups stets in die Defensive gedrängt sind und mit einem raschen Rückzug aus einzelnen Anwendungsbereichen bzw. Projekten reagieren. Einige prominente Beispiele sind in Tabelle 1 zusammengefasst.

Firma	**Datum**	**Ereignisse**
Benetton / Philips	11.3.2003	Aktion: Benetton kündigt an, zukünftig RFID-Tags in Sisley-Textilien einnähen zu wollen. CASPIAN ruft daraufhin zwei Tage später im Internet zu einem Boykott von Benetton-Produkten auf.
	9.4.2003	Reaktion: Benetton verkündet in einer Pressemeldung, auf RFID in Textilien verzichten zu wollen.
Wal-Mart / Gillette	8.7.2003	Aktion: CASPIAN veröffentlicht 68 als „confidential" gekennzeichnete Dokumente des Auto-ID Centers, zu dessen größten Sponsoren Wal-Mart und Gillete zählen. Wal-Mart hatte zuvor am 30.4. ein RFID-Pilotprojekt zur automatisierten Inventur im Verkaufsraum gestartet.
	9.7.2003	Reaktion: Wal-Mart stoppt das Pilotprojekt und kündigt an, RFID nur noch in der internen Logistik einsetzen zu wollen.
Tesco / Gillette	22.7.2003	Aktion: Der britischen Handelskette Tesco wird vorgeworfen, Kunden bei der Entnahme von Rasierklingen aus dem Regal mittels RFID zu erfassen und automatisch zu fotografieren.
	15.8.2003	Reaktion: Gillette bestreitet alle Vorwürfe; Tesco gibt zu „sicherheitsrelevante Vorteile" der RFID-Technik getestet zu haben. Der Pilotversuch wurde Ende Juli 2003 beendet.
Metro	1.2.2004	Aktion: FoeBuD demonstriert vor dem Metro Future Store gegen den Einsatz RFID-basierter Kundenkarten.
	27.2.2004	Reaktion: Metro tauscht 10.000 Kundenkarten gegen solche ohne RFID-Tag um.

Tabelle 1: Aktion & Reaktion in der Auseinandersetzung um RFID

In einem zweiten Schritt der Untersuchung wurde analysiert, wie die Reaktionen der Leser der Heise-Seiten auf RFID-Nachrichtenmeldungen ausfielen. Die thematische Ausrichtung des Newstickers lässt wg. fehlender Repräsentativität der Teilnehmer an den Diskussionen zwar keine statistische Auswertung zu. Die Forenbeiträge selbst erlauben jedoch eine qualitative Betrachtung von Sprache, Diskussionsstil und Argumentation.

Die Kritikpunkte der Diskussionsteilnehmer an RFID lassen sich thematisch in den folgenden vier Aussagen zusammenfassen:

- Unsichere Technik: Die Fähigkeiten der Technologie sind in weiten Teilen unklar. Offensichtlich scheint jedoch, dass RFID nur unzureichend Funktionen zur Sicherstellung der Datensicherheit implementiert.
- Unklarer Nutzen: Sinn und Zweck der RFID-Einführung ist nicht ersichtlich. Dies betrifft den nicht nachvollziehbaren Nutzen auf Unternehmensseite, vor allem aber hat der Konsument selbst keinen Vorteil von der Technologie. Der Missbrauch von Kundendaten erscheint als naheliegendstes Einsatzgebiet für RFID.
- Fehlende Glaubwürdigkeit: Den Aussagen von Handelskonzernen und Produzenten kann kein Glauben geschenkt werden. Die zurückhaltende Informationspolitik zeigt, dass RFID-Anwender etwas zu verbergen haben.
- Unzureichende Gesetzeslage: Bestehende Gesetze reichen zum Schutz des Individuums vor RFID nicht aus. Der Gesetzgeber ist aufgerufen, den Einsatz von RFID zu verbieten oder zumindest stark einzuschränken.

Die Diskussion selbst verläuft in den meisten Fällen stark emotionalisiert und einzelnen Beiträgen haftet allzu häufig der Charakter von Verschwörungstheorien an, d.h. Staat und Wirtschaft wird per se die Absicht unterstellt, RFID zum Zweck der Überwachung von Privatpersonen einsetzen zu wollen. Der Vergleich zur Orwellschen Dystopie „1984" oder Huxleys „Brave new world" findet sich in zahlreichen Texten wieder. Dies korrespondiert auffällig mit einer Häufung sachlich falscher Vorstellungen von den Möglichkeiten von RFID als Überwachungstechnologie. Bspw. äußern viele Forenteilnehmer die Befürchtung, RFID-Transponder und ihre Träger seien per Satellit weltweit lokalisierbar.

Zusammengefasst lässt sich auf Grundlage der betrachteten Forendiskussionen festellen, dass die Wahrnehmung von RFID als Risiko für die Privatsphäre des Einzelnen von massiven Ängsten und einem tiefsitzenden Misstrauen gegenüber den Anwenderfirmen gekennzeichnet ist. Dabei wird auch deutlich, dass ein Mangel an Information seitens der Verbraucher eine, aber keineswegs die einzige Ursache für die Ablehnung der Technologie sind. Handlungsdefizite seitens der Unternehmen bestehen vielmehr auf mehreren Ebenen, wohingegen es den Pressure Groups erfolgreich gelungen ist, das Thema zu besetzen, die öffentliche Wahrnehmung auf die zweifellos vorhandenen Risiken von RFID zu konzentrieren und Nutzenpotenziale weitgehend auszublenden.

4 Elemente einer Privacy-Strategie

Vor dem Hintergrund der beschriebenen Haltung der Konsumenten gegenüber RFID stellt sich für Unternehmen die Frage, welche Mittel Ihnen noch zur Verfügung stehen, um die Risikowahrnehmung in Ihrem Sinn zu beeinflussen. Ziel ist dabei stets, Wissen über die Technologie zu vermitteln, bzw. dort, wo dies nicht möglich ist und Unsicherheit vorherrscht, den Aufbau eines Vertrauensverhältnisses zu fördern, welches diese Unsicherheit überwinden hilft.

Aufbauend auf den zuvor beschriebenen vier Kernaussagen der RFID-Skeptiker lassen sich unmittelbar Handlungsebenen mit jeweils eigenen Gestaltungsobjekten und Zielen ableiten (s. Abbildung 3):

- Technologie: Auf der technischen Ebene gilt es, RFID-Systeme um Funktionen zu ergänzen, die einen Datenmissbrauch unmöglich machen oder zumindest erschweren.
- Prozesse: Ziel auf der Prozessebene ist die Erhöhung des Nutzens für den Kunden bei gleichzeitiger Reduzierung der Risiken auf ein Minimum durch begleitende organisatorische Maßnahmen.
- Dialog: Der Risikodialog in und mit der Öffentlichkeit sowie dem einzelnen Konsumenten zielt auf die Wiedergewinnung verlorener Glaubwürdigkeit ab.
- Regeln: Regeln dienen der für alle Seiten verbindlichen Festlegung, welche Anwendungen bzw. Handlungsweisen im Zusammenhang mit der Technologie als zulässig gelten oder nicht.

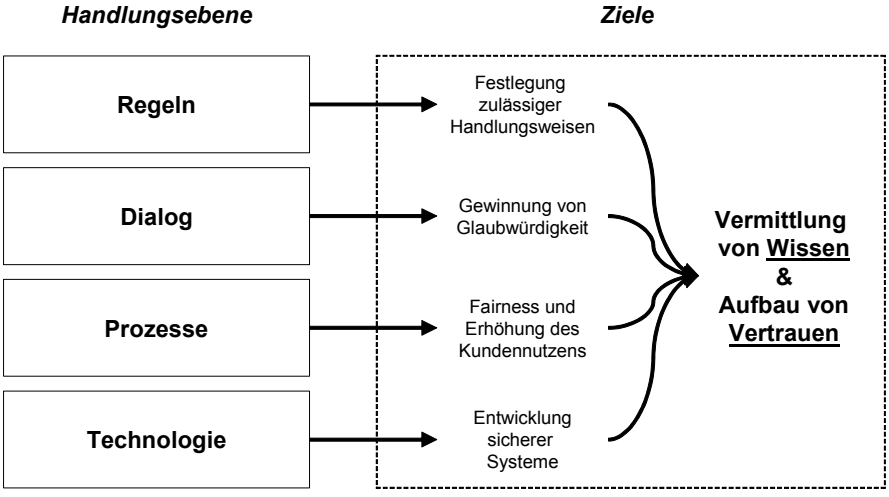

Abbildung 3: Handlungsebenen für das Risikomanagement

4.1 Technologie

Die Möglichkeiten zur Sicherung des Datenschutzes auf technischer Ebene sind vielfältig und umfassen neben allgemeinen Maßnahmen zur IT-Sicherheit auch RFID-spezifische Konzepte, um das unkontrollierte Lesen von Transpondern sowie die Manipulation der darauf gespeicherten Informationen zu verhindern. In der Literatur findet sich hierzu eine Reihe unterschiedlicher Ansätze [Cav04; Jue+03; Kum03; Lan04; Sar+02; Wei+03]:

- Abschirmung: Der einfachste Schutz vor einem Zugriff auf den Transponder durch Dritte ist die physikalische Abschirmung mittels eines metallischen Netzes oder einer Folie analog einem Faradayschen Käfig.
- Störsender: Die Kommunikation zwischen Transponder und Lesegerät kann durch den Einsatz eines Störsenders verhindert werden.
- Blocker-Tag: Bei der iterativen Suche des Lesers nach einer Transponder-ID antwortet der Blocker-Tag stets mit einer passenden ID, so dass der Leser keine Chance hat, die in seiner Umgebung befindlichen Transponder zu erkennen.
- Kill-Kommando: Das im Transponder implementierte Kill-Kommando dient zur dauerhaften Deaktivierung, z.B. bei der Übergabe eines Produkts an den Käufer an der Supermarktkasse.
- Hash-Lock-Verfahren: Der Tag wird über einen Hash-Wert, der aus einem Zufallsschlüssel generiert wird, gesperrt und reagiert nur noch auf Anfragen, die über diesen Hash-Wert autorisiert sind. Zu einem späteren Zeitpunkt kann der Transponder dann mit Hilfe des Schlüssels wieder entsperrt werden.
- Distanz-basierte Zugriffskontrolle: Art und Umfang der vom Transponder gesendeten Informationen werden vom Abstand zum Lesegerät (ermittelt z.B. durch Feldstärke oder Triangulation) abhängig gemacht.
- Abhörsichere Antikollisionsprotokolle: Abhörsichere Antikollisionsprotokolle vermeiden die Übertragung kompletter Tag-IDs auf dem Vorwärtskanal (d.h. vom Leser zu den Tags), so dass ein Abhören aus weiter Entfernung verhindert wird.

Einige der genannten Verfahren scheitern bereits an mangelnder Praktikabilität aufgrund zu hoher technischer Anforderungen, Komplexität für den Benutzer oder der Tatsache, dass verschiedene RFID-Anwendungen auf diese Weise durch technische Funktionalität von vorneherein unmöglich gemacht werden, z.B. im Rahmen von Mehrwegsystemen. Das aus Kundensicht gravierendste Problem ist jedoch, dass die gewonnene zusätzliche Sicherheit nicht spürbar bzw. sichtbar wird und vor allem keine Möglichkeit zur zuverlässigen Verifikation besteht. Trotz aller Notwendigkeit technischer Weiterentwicklung kann das Ziel der verbesserten Technologieakzeptanz somit auf diese Weise allein nicht erreicht werden.

4.2 Prozesse

Mit der Änderung von Abläufen auf der Prozessebene können in zweierlei Hinsicht Anreize geschaffen werden, die die Einstellung von Konsumenten gegenüber der RFID-Technologie positiv beeinflussen. Einerseits sollten Prozesse so gestaltet sein, dass dem Kunden der Eindruck von „procedural fairness", d.h. dem fairen Umgang mit ihm im Rahmen geschäftlicher Aktivitäten, vermittelt wird [CuAr99]. Wesentlicher Faktor ist in diesem Zusammenhang neben dem Wissen über Abläufe die Kontrolle über dieselbigen [CuBi03], bspw. durch Opt-In-Wahlmöglichkeiten. „Opt-In" bezeichnet hierbei die Notwendigkeit, im Rahmen einer Geschäftsbeziehung eine Entscheidung für einen Service (z.B. die Zusendung personalisierter Werbemails) bewusst treffen zu müssen, während „Opt-out" die positive Entscheidung durch Voreinstellungen vorwegnimmt und der Kunde gezwungen ist, explizit zu widersprechen [MaLa01; Win01]. Opt-In setzt dabei voraus, dass dem Kunden die Folgen einer positiven Entscheidung klar offen gelegt werden.

Andererseits kann durch verbesserte Prozesse die Bereitschaft des Kunden zur Technologieakzeptanz durch zusätzliche Leistungen und Nutzeffekte erhöht werden. So konnte in zahlreichen Untersuchungen auf Grundlage des weit verbreiteten „Technology Acceptance Model (TAM)" [Dav89] zu E-Mail, Telemedizin und anderen IT-Themen gezeigt werden, dass die Akzeptanz auf Nutzerseite im Wesentlichen von der wahrgenommenen Einfachheit der Nutzung sowie der wahrgenommenen Nützlichkeit einer Technologie abhängig ist [ChLa03; McC03]. Es kann daher mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass ansprechend gestaltete Dienste auf RFID-Basis auch einen positiven Einfluss auf die Akzeptanz der Technologie selbst hätten.

Beispiele für derartige Dienste sind [FlDi03; SpBe04]:

- Beschleunigter Bezahlvorgang an der Supermarktkasse durch automatische Erfassung aller eingekauften Waren im Einkaufskorb.
- Produktinformationen, die der Kunde im Geschäft oder daheim abrufen kann, z.B. Verbraucherinformationen, Bedienungsanleitungen oder Softwareupdates.
- Nutzungs- bzw. Risiko-basierte Abrechnungsmodelle, bei denen z.B. die Miete für eine Maschine oder die Versicherungsprämie für ein Auto nicht über die Dauer, sondern die Art der Nutzung berechnet werden.
- Wartungs- und Reparaturdienste, die als Service über das Internet angeboten werden, sowie effizientere Durchführung von Rückholaktionen und Bearbeitung von Garantiefällen.
- Vermeidung von Fälschungen von Luxusgütern, Autoersatzteilen oder Medikamenten, die durch einen RFID-Transponder eindeutig als Original identifiziert und deren Weg in der Lieferkette zurückverfolgt werden kann.

4.3 Dialog

Obwohl die Erkenntnis, dass der Sinn und Zweck von Marketing sowohl in der Gewinnung als auch in der Bindung von Kunden besteht, nicht grundsätzlich neu ist, lag der Schwerpunkt in der Vergangenheit eher auf Akquise von Neukunden als in der Beziehungspflege zu Bestandskunden. Während z.B. Finanzdienstleister im Übergang vom Transaktions- zum Beziehungsmarketing bereits relativ weit fortgeschritten sind, wird im Handel der Begriff der „customer relation" weitgehend auf „customer loyalty" reduziert. Ziel entsprechender Loyalty- oder Frequency-Programme ist weniger der Aufbau einer Beziehung zum Kunden als die Erhöhung der Transaktionshäufigkeit durch Schaffung von Anreizen [Win01], z.B. durch Rabattkarten (vgl. hierzu bspw. die Beschreibung des Loyalty-Programms der Handelskette Tesco bei [Hum+04]). Während somit auf der einen Seite der Aufbau einer Beziehung des Kunden zum Unternehmen unterbleibt, führt die Art und Weise der Datensammlung in den gängigen Kundenkartensystemen zu einem Vertrauensverlust seitens der Kunden [Fle03].

Vor diesem Hintergrund kommt dem offenen Dialog mit Kunden unabhängig von der einzelnen Transaktion eine wichtige Rolle in der (Wieder-)Gewinnung von Vertrauen und Glaubwürdigkeit zu. In der konkreten Auseinandersetzung um RFID herrschen hingegen Strategien vor, die auf das Herunterspielen von Risiken bzw. die Belehrung der Öffentlichkeit ausgerichtet sind, oder schlichte Kommunikationsenthaltung – Kommunikationsstrategien also, die wenig geeignet erscheinen, um den Konsumenten für das Unternehmen zu gewinnen. Wiedemann nennt folgende typische Fehler in der Kommunikation, die sich nahezu 1:1 in der aktuellen Diskussion wiederfinden [Wie94]:

- Verleugnung und defensive Informationspolitik
- Beschwichtigung (Versuch des „Weg-Redens")
- Aggressive und konfrontative Auseinandersetzungen sowie Polemik
- Nur Worte, keine Taten
- Zu späte Information
- Reaktive Informationspolitik
- Mangelnde Klarheit und Verständlichkeit der Informationen
- Unzureichender Bezug auf die vorhandenen Informationsbedürfnisse und Vorstellungen der Öffentlichkeit

Die Entwicklung eines konstruktiven Dialogs ist aufgrund häufig verhärteter Fronten und Verständigungsprobleme schwierig. Nichtsdestotrotz sind z.B. die Bereitschaft zu Interviews, praktische Demonstrationen, Kooperation mit Interessenverbänden, Vermittlung von Experten usw. langfristig erfolgreiche Maßnahmen einer offenen und offensiven Kommunikationskultur [WiHe89].

4.4 Regeln

Die Festlegung verbindlicher Regeln kann entweder durch Gesetze und Verordnungen oder in Form einer Selbstverpflichtung erfolgen. Während die Einbindung der neutralen Institution des Staates einen gewissen Vertrauensbonus mit sich bringt, hat die Selbstverpflichtung der Industrie den Vorteil informellerer Kontrollmechanismen. In beiden Fällen ist für die Entwicklung einer Strategie zunächst wichtig, bereits bestehende Regelungen zu kennen.

In den USA und Europa haben sich im Verlauf der letzten Jahrzehnte grundsätzlich verschiedene Herangehensweisen zum Schutz der Privatsphäre etabliert (s. Tabelle 2) [Lan04; Smi01]: Dem vor allem in Europa favorisierten Ansatz umfassender, sektorenübergreifender Datenschutzgesetze steht in den USA ein Mix aus spezifischer Gesetzgebung und freiwilliger Selbstbeschränkung von Industrie und Handel gegenüber. Vor diesem Hintergrund erklärt sich u.a. die amerikanische Forderung nach einem „RFID Bill of Rights" [Gar02], wohingegen entsprechende Vorhaben in Europa bereits im Vorfeld verworfen wurden.

	USA	**Europa**
Legislativer Ansatz	sektoriell	universell
Regulative Struktur	Selbstinitiative und freiwillige Kontrolle	zentralisierte Behörde (Beauftragter, Registrierstelle oder Lizenzierung)
Rechte des Datensubjekts	Keine oder Opt-out (anwendungsabhängig)	Prüfung / Korrektur, Opt-out (teilw. Opt-in)
Rolle von Privacy in der Gesellschaft	Verhandlungssache	Menschenrecht

Tabelle 2: Unterschiede im Datenschutzrecht in USA und Europa [Smi01]

Unabhängig von der Gesetzeslage erfüllt eine öffentliche Selbstverpflichtung darüber hinaus die Aufgabe, das Bekenntnis eines Unternehmens zur Einhaltung bestimmter Standards nach außen zu dokumentieren. Beispiele hierfür sind die vorgeschlagene Kennzeichnung EPC-bestückter Produkte (s. Abbildung 4) oder die organisatorische Verankerung in Form eines „Chief Privacy Officer" [HB01; Jon04].

Abbildung 4: Label zur Kennzeichnung von Produkten mit EPC-Transpondern [EPC04]

5 Zusammenfassung und Ausblick

Wie die vorangegangenen Ausführungen gezeigt haben, ist die Wahrnehmung von RFID als Risiko mittlerweile etabliert und entwickelt sich in ähnlicher Weise wie bereits andere technologische Risikothemen in der Vergangenheit. Inwiefern das Thema das Stadium der Krise erreicht oder vorher abflaut, ist zurzeit noch völlig offen und hängt vom weiteren Verlauf der Auseinandersetzung ab (s. Abbildung 5). Ob es Technologieanbietern und -anwendern gelingt, die öffentliche Wahrnehmung noch zu drehen und das Thema positiv zu besetzen, wird in jedem Fall wesentlich von der gewählten Risikomanagementstrategie bestimmt.

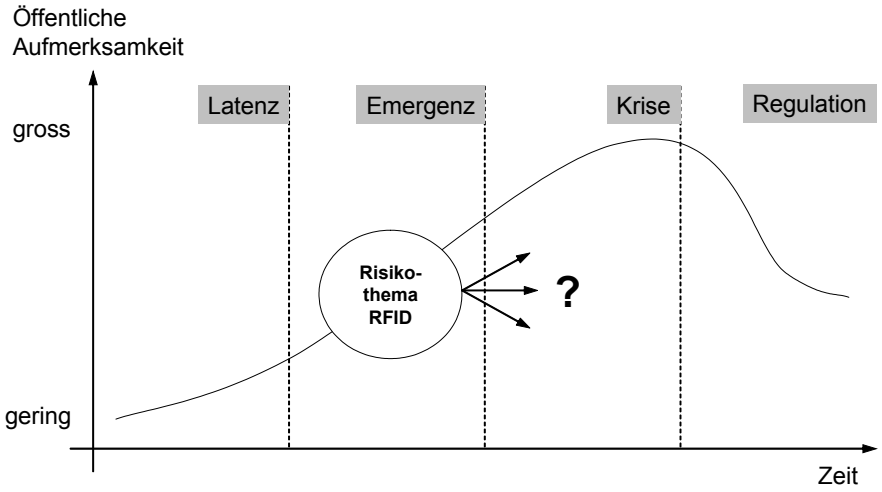

Abbildung 5: Lebenslauf des Risikothemas RFID (in Anlehnung an [Car+00, S. 14])

Durch ihren Rückzug aus einzelnen kritischen Anwendungsbereichen und die Entscheidung, RFID zunächst nicht auf Einzelproduktebene, sondern nur auf Paletten und Umverpackungen einzusetzen (s. hierzu bspw. Angaben der METRO Group zum geplanten RFID-Roll-out in [MET04]), haben Industrie und Handel etwas Zeit gewonnen. Mit der Weiterentwicklung der Technologie bei gleichzeitig sinkenden Preisen werden jedoch voraussichtlich auch nach und nach Anwendungen wirtschaftlich attraktiv werden, die aktivierte Transponder auf Einzelprodukten über den Kauf- und Bezahlvorgang hinaus beim Kunden voraussetzen. Vor diesem Hintergrund können der vorliegende Beitrag und insb. das vorgestellte Ebenenmodell als ein Gestaltungsrahmen für das Risikomanagement jenseits der derzeit noch zumeist vorherrschenden technologiezentrischen Sichtweise dienen.

6 Danksagung

Die vorliegende Arbeit wurde durch das M-Lab – The Mobile and Ubiquitous Computing Lab und seine Partnerunternehmen unterstützt. Das M-Lab ist ein Gemeinschaftsprojekt der Universität St. Gallen und ETH Zürich und Mitglied des internationalen Auto-ID Lab Network.

Literatur

[Can02] Cantwell, B.: Why Technical Breakthroughs Fail: A History of Public Concern with Emerging Technologies. White Paper, Auto-ID Center, Cambridge, 2002

[Car+00] Carius, R.; Henschel, C.; Kastenholz, H.G.; Nothdurft, W.; Ruff, F.; Uth, H.J.; Wiedemann, P.M.: Risikokommunikation für Unternehmen. Verein deutscher Ingenieure (VDI), Düsseldorf, 2000

[Cav04] Cavoukian, A.: Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology. Information and Privacy Commissioner Ontario, Toronto, 2004

[ChLa03] Chau, P.Y.K.; Lai, V.S.K.: An Empirical Investigation of the Determinants of User Acceptance of Internet Banking. Journal of Organizational Computing and Electronic Commerce, Jg. 13, Nr. 2, 2003, S. 123-145

[CuAr99] Culnan, M.J.; Armstrong, P.K.: Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science, Jg. 10, Nr. 1, 1999, S. 104-116

[CuBi03] Culnan, M.J.; Bies, R.J.: Consumer Privacy: Balancing Economic and Justice Considerations. Journal of Social Issues, Jg. 59, Nr. 2, 2003, S. 323-342

[Dav89] Davis, F.D.: Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology. MIS Quarterly, Jg. 13, Nr. 3, 1989, S. 319-339

[Duc03] Duce, H.: Public Policy: Understanding Public Opinion. Executive Briefing, Auto-ID Center, Cambridge, 2003

[EPC04] EPCglobal Consumer Information. EPCglobal Inc., 2004 http://www.epcglobalinc.org/consumer/index.html (Abruf 14.7.2004)

[Fer02] Ferguson, G.: Have Your Objects Call My Objects. Harvard Business Review, Jg. 80, Nr. 6, 2002, S. 138-144

[Fin02] Finucane, M.L.: Mad Cows, Mad Corn & Mad Money: Applying What We Know About the Perceived Risk of Technologies to the Perceived Risk of Securities. The Journal of Psychology and Financial Markets, Jg. 3, Nr. 4, 2002, S. 236-243

[FlDi03] Fleisch, E.; Dierkes, M.: Ubiquitous Computing aus betriebswirtschaftlicher Sicht. Wirtschaftsinformatik, Jg. 41, Nr. 6, 2003, S. 661-670

[Fle01] Fleisch, E.: Betriebswirtschaftliche Perspektiven des Ubiquitous Computing. In: Buhl, H.U.; Huther, A.; Reitwiesner, B.: Information Age Economy, Physica-Verlag, Heidelberg, 2001, S. 177-191

[Fle03] Fletcher, K.: Consumer power and privacy: the changing nature of CRM. International Journal of Advertising, Jg. 22, Nr. 2, 2003, S. 249-272

[Gar02] Garfinkel, S.L.: Adopting Fair Information Practices to Low Cost RFID Systems. International Conference on Ubiquitous Computing, Göteborg, 2002

[HB01] Chief Privacy Officer. Harvard Business Review, Jg. 78, Nr. 6, 2001, S. 20-21

[Hen90] Hennen, L.: Risiko-Kommunikation: Informations- und Kommunikationstechnologien. In: Jungermann, H.; Rohrmann, B.; Wiedemann, P.M. (Hrsg.): Risiko-Konzepte – Risiko-Konflikte – Risiko-Kommunikation. Forschungszentrum Jülich, 1990, S. 209-258

[Hum+04] Humby, C.; Hunt, T.; Phillips, T.: Scoring Points: How Tesco Is Winning Customer Loyalty. Kogan Page, London, 2004

[Jon01] Jones, K.E.: BSE, Risk and the Communication of Uncertainty: A Review of Lord Phillips' Report from the BSE Inquiry. Canadian Journal of Sociology, Jg. 26, Nr. 4, 2001, S. 655-666

[Jon04] Jonietz, E.: Tracking Privacy. Technology Review, Jg. 107, Nr. 6, 2004, S. 74-75

[Jue+03] Juels, A., Rivest, R., Szydlo, M.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. ACM Conference on Computer and Communications Security, Washington D.C., 2003

[Jun91] Jungermann, H.: Inhalte und Konzepte der Risikokommunikation. In: Jungermann, H.; Rohrmann, B.; Wiedemann, P.M. (Hrsg.): Risikokontroversen – Konzepte, Konflikte, Kommunikation. Springer Verlag, Berlin, 1991, S. 335-354

[KoKl91] Koren, G; Klein, N.: Bias against negative studies in newspaper reports of medical research. Journal of the American Medical Association, Jg. 266, Nr. 13, 1991, S. 1824-1826

[Kum03] Kumar, R.: Interaction of RFID Technology and Public Policy. RFID Privacy Workshop @ MIT, Boston (MA), 2003

[Lan01] Landt, J.: Shrouds of Time: The history of RFID. AIM Inc., Pittsburgh (PA), 2001

[Lan04] Langheinrich, M.: Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie. Institut für Pervasive Computing, ETH Zürich, 2004 (noch nicht erschienen)

[MaLa01] Mattern, F.; Langheinrich, M.: Allgegenwärtigkeit des Computers – Datenschutz in einer Welt intelligenter Alltagsdinge. In: Müller, G.; Reichenbach, M. (Hrsg.): Sicherheitskonzepte für das Internet, Springer Verlag, Berlin, 2001

[Mat03] Mattern, F.: Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing. In: Mattern, F. (Hrsg.): Total vernetzt. Springer Verlag, Berlin, 2003, S. 1-41.

[McC03] McCloskey, D.: Evaluating Electronic Commerce Acceptance with the Technology Acceptance Model. Journal of Computer Information Systems, Jg. 4, Nr. 2, 2003, S. 49-57

[MET04] Leitlinien für den RFID-Roll-out der METRO Group. METRO Group, Düsseldorf, 2004

[ReLe91] Renn, O.; Levine, D.: Credibility and trust in risk communication. In: Kasperson, R.E.; Stallen, P.J.M. (Hrsg.): Communicating Risks to the Public, Kluwer, Dordrecht, 1990, S. 175-218

[Ric01] Richardson, K.: Risk news in the world of Internet newsgroups. Journal of Sociolinguistics, Jg. 5, Nr. 1, 2001, S. 50-72

[Sar+02] Sarma, S.; Weis, S.; Engels, D.: RFID Systems, Security & Privacy Implications. White Paper, Auto-ID Center, Cambridge, 2002

[Sar+01] Sarma, S.; Brock, D.; Engels, D.: Radio Frequency Identification and the Electronic Product Code. IEEE Micro, Jg. 21, Nr. 6, 2001, S. 50-54

[Sch04] Schneider, R.: Emerging Risks – Analyse or Exclude. Reinsurance Lecture, The Institute of London, London, 13. Januar 2004
http://www.iilondon.co.uk/pdf/RSchneider140104.pdf (Abruf 14.7.2004)

[Sie01] Siegrist, M.: Die Bedeutung von Vertrauen bei der Wahrnehmung und Bewertung von Risiken. Arbeitsbericht Nr. 197, Akademie für Technikfolgenabschätzung in Baden-Württemberg, Stuttgart, 2001

[SjFr01] Sjöberg, L.; Framm, J.: Information Technology Risks as Seen by the Public. Risk Analysis, Jg. 21, Nr. 3, 2001, S. 427-441

[Slo+81] Slovic, P.; Fischhoff, B.; Lichtenstein, S.: Facts and Fears: Societal Perception of Risk. Advances in Consumer Research, Jg. 8, Nr. 1, 1981, S. 497-502

[Slo92] Slovic, P.: Perception of risk: Reflections on the psychometric paradigm. In: Krimsky, S.; Golding, D. (Hrsg.): Social theories of risk. Praeger, Westport (CT), 1992, S. 117-152

[Slo99] Slovic, P.: Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield. Risk Analysis, Jg. 19, Nr. 4, S. 689-701

[Smi01] Smith, H.J.: Information Privacy and Marketing: What the U.S. should (and shouldn't) learn from Europe. California Management Review, Jg. 43, Nr. 2, 2001, S. 8-33

[SpBe04] Spiekermann, S.; Berthold, O.: Maintaining privacy in RFID enabled environments – Proposal for a disable-model. Workshop on Security and Privacy in Pervasive Computing, Int. Conference on Pervasive Computing, 2004

[Spi98] Spinello, R.A.: Privacy Rights in the Information Economy. Business Ethics Quarterly, Jg. 8, Nr. 4, 1998, S. 723-742

[Tac01] Tacke, V.: BSE as an organizational construction: a case study on the globalization of risk. British Journal of Sociology, Jg. 52, Nr. 2, 2001, S. 293-312

[TrMc03] Trumbo, C.W.; McComas, K.A.: The Function of Credibility in Information Processing for Risk Perception. Risk Analysis, Jg. 23, Nr. 2, 2003, S. 343-353

[WaBr90] Warren, S.D.; Brandeis, L.D.: The Right to Privacy. Harvard Law Review, Jg. 4, Nr. 5, 1890, S. 193-220

[Wat+02] Watson, T.; Osborne-Brown, S.; Longhurst, M.: Issues Negotiation – investing in stakeholders. Corporate Communications, Jg. 7, Nr. 1, 2002, S. 54-61

[Wei+03] Weis, S., Sarma, S., Rivest, R., & Engels, D.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. Int. Conference on Security in Pervasive Computing, Boppard, 2003

[Wes03] Westin, A.: Social and Political Dimensions of Privacy. Journal of Social Issues, Jg. 59, Nr. 2, 2003, S. 431-453

[Wes67] Westin, A.: Privacy and Freedom. Atheneum, New York, 1967

[Wha98] Whawell, P.: The ethics of pressure groups. Business Ethics, Jg. 7, Nr. 3, 1998, S. 178-181

[Wie94] Wiedemann, P.: Krisenmanagement & Krisenkommunikation. Arbeiten zur Risiko-Kommunikation, Heft 41, Forschungszentrum Jülich, 1994

[WiHe89] Wiedemann, P.; Hennen, L.: Schwierigkeiten bei der Kommunikation über technische Risiken. Arbeiten zur Risikommunikation, Heft 9, Forschungszentrum Jülich, 1989

[Win01] Winer, R.S.: A Framework for Customer Relationship Management. California Management Review, Jg. 43, Nr. 4, 2001, S. 89-105

[Zei04] Zeidler, M.: RFID: Der Schnüffel-Chip im Joghurtbecher. Monitor, Westdeutscher Rundfunk, Köln, 8. Januar 2004
http://www.wdr.de/tv/monitor/pdf/040108f_rfid.pdf (Abruf 14.7.2004)