

Martin Kähmer

ExPDT

VIEWEG+TEUBNER RESEARCH

Martin Kähmer

# ExPDT

Vergleichbarkeit von Richtlinien für Selbstregulierung  
und Selbstdatenschutz

VIEWEG+TEUBNER RESEARCH

Bibliografische Information der Deutschen Nationalbibliothek  
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der  
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über  
<<http://dnb.d-nb.de>> abrufbar.

Dissertation an der Technischen Fakultät der Albert-Ludwigs-Universität Freiburg, 2009

1. Auflage 2010

Alle Rechte vorbehalten

© Vieweg+Teubner | GWV Fachverlage GmbH, Wiesbaden 2010

Lektorat: Dorothee Koch | Anita Wilke

Vieweg+Teubner ist Teil der Fachverlagsgruppe Springer Science+Business Media.  
[www.viewegteubner.de](http://www.viewegteubner.de)



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt.  
Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürfen.

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg  
Druck und buchbinderische Verarbeitung: STRAUSS GMBH, Mörlenbach  
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.  
Printed in Germany

ISBN 978-3-8348-1000-7

Für die nie endende Unterstützung danke ich  
meinen Eltern und Euch, Heidi und Sebastian

## Zusammenfassung

Dem Angebot personalisierter Dienste stehen die Probleme des Kundendatenschutzes gegenüber. Personalisierte Dienste erfordern einerseits eine umfassende Datensammlung. Andererseits müssen die Kundendaten auch vor unautorisiertem Zugriff und unerwünschter Verwendung geschützt werden. Nur so kann gewährleistet werden, dass das Angebot personalisierter Dienste nicht an den Anforderungen des Datenschutzes scheitert.

Die bisherigen Herangehensweisen an den Datenschutz bestanden einerseits in der Selbstregulierung durch die Dienstanbieter mittels einseitig vorgegebener Datenschutzrichtlinien, andererseits im Selbstdatenschutz der Kunden mittels Datensparsamkeit. Allerdings sind Kunden oft bereit, für besser auf sie zugeschnittene Dienste mehr Daten herauszugeben, falls deren Schutz gewährleistet wird. Doch ist diese Bereitschaft individuell und abhängig vom jeweiligen Dienst und der aktuellen Situation. Ansatz ist hier die Zusammenführung von Selbstregulierung und Selbstdatenschutz durch die Vereinbarung individueller Datenschutzrichtlinien zwischen Anbieter und Kunden.

Diese Arbeit präsentiert mit den Extended Privacy Definition Tools (ExPDT) eine formale Richtliniensprache. Basierend auf dem NAPS-Rahmenwerk ermöglicht sie die Spezifikation ausdrucksstarker Datenschutzrichtlinien. Zur Unterstützung der Vereinbarung individueller Richtlinien zwischen Anbieter und Kunden wird der Differenzoperator definiert. Mit ihm lassen sich Datenschutzrichtlinien automatisiert vergleichen und Konflikte zwischen ihnen identifizieren. Die Funktionsweise der ExPDT-Sprache sowie der prototypisch entwickelten Werkzeuge zur Richtlinienauswertung und -anzeige wird anhand des konkreten Anwendungsbeispiels eines Einkaufszentrums demonstriert.

# Inhaltsverzeichnis

<b>1</b>	<b>Privatsphäre als gesellschaftliche Forderung</b>	<b>1</b>
1.1	Personalisierung auf Kosten der Privatsphäre? . . . . .	1
1.1.1	Personalisiertes Einkaufen . . . . .	2
1.1.2	Risiko des Privatsphärenverlustes . . . . .	4
1.2	Schutz der Privatsphäre . . . . .	5
1.2.1	Bereiche der Privatsphäre . . . . .	6
1.2.2	Bedeutung des Datenschutzes . . . . .	6
1.2.3	Rechtliche Definitionen von Datenschutz . . . . .	7
1.3	Selbstregulierung und Selbstdatenschutz . . . . .	10
1.4	Beitrag der Arbeit . . . . .	12
1.5	Aufbau der Arbeit . . . . .	13
<b>2</b>	<b>Datenschutz in der Informatik</b>	<b>15</b>
2.1	Bedrohungsanalyse im Systemmodell . . . . .	15
2.2	Technologien für den Datenschutz . . . . .	17
2.2.1	Anonymisierung . . . . .	17
2.2.2	Benutzerseitige Datenverarbeitung . . . . .	17
2.2.3	Identitätsmanagement . . . . .	18
2.2.4	Nutzungskontrolle . . . . .	18
2.3	Rahmenwerk für Selbstregulierung und Selbstdatenschutz . . . . .	19
2.4	Sprachanforderungen für Datenschutzrichtlinien . . . . .	22
2.4.1	Ausdrucksstärke . . . . .	23
2.4.2	Richtlinienoperatoren . . . . .	26
<b>3</b>	<b>Gegenwärtige Richtliniensprachen</b>	<b>27</b>
3.1	Richtlinien für den Selbstdatenschutz . . . . .	27
3.1.1	Vertrauenssiegel . . . . .	27
3.1.2	Platform for Privacy Preferences (P3P) . . . . .	29
3.1.3	Customer Profile Exchange (CPExchange) . . . . .	37
3.2	Richtlinien für die Selbstregulierung . . . . .	38

3.2.1	Enterprise Privacy Authorisation Language (EPAL) . . . . .	38
3.2.2	Obligation Specification Language (OSL) . . . . .	46
3.2.3	eXtensible Access Control Markup Language (XACML) . . . . .	48
3.3	Zusammenfassung . . . . .	52
<b>4</b>	<b>Richtliniensprache der Extended Privacy Definition Tools (ExPDT)</b>	<b>55</b>
4.1	Richtlinienkombination im NAPS-Rahmenwerk . . . . .	56
4.2	Ebenen von ExPDT . . . . .	61
4.3	Syntax von ExPDT-Richtlinien . . . . .	63
4.3.1	Richtlinien und Regeln . . . . .	63
4.3.2	Wächter . . . . .	66
4.3.3	Bedingungen . . . . .	67
4.3.4	Obligationen . . . . .	68
4.3.5	Regelentscheidung und Richtlinienanfrage . . . . .	69
4.4	Semantik einer ExPDT-Richtlinie . . . . .	70
4.4.1	Entscheidung einer Regel . . . . .	70
4.4.2	Entscheidung einer Richtlinie . . . . .	71
4.5	Vergleich von Richtlinien . . . . .	73
4.5.1	Äquivalenz und Verfeinerung . . . . .	74
4.5.2	Differenz zweier Richtlinien . . . . .	75
4.6	Konstruktion der Differenz . . . . .	77
4.6.1	Normalisierung . . . . .	77
4.6.2	Differenz über regelweisen Vergleich . . . . .	87
4.6.3	Wächterhülle . . . . .	89
4.6.4	Erfüllbarkeitsrelation für Bedingungen . . . . .	90
4.6.5	Normalisierung mit Domänenwissen . . . . .	92
4.6.6	Regelweiser Vergleich mit Domänenwissen . . . . .	94
<b>5</b>	<b>Implementierung der ExPDT-Werkzeuge</b>	<b>95</b>
5.1	Werkzeugkette von ExPDT . . . . .	95
5.2	Auswertungseinheit . . . . .	98
5.3	Richtlinieditor . . . . .	100
<b>6</b>	<b>Evaluation von ExPDT</b>	<b>103</b>
6.1	Datenschutz mit ExPDT im Einkaufszentrum . . . . .	103
6.2	Definition von Domänenwissen . . . . .	105
6.3	Spezifikation und Auswertung von Richtlinien . . . . .	108
6.3.1	Fallbeispiele für ExPDT-Richtlinien . . . . .	109
6.3.2	Auswertung von Richtlinienanfragen . . . . .	111

6.4	Vergleich von Richtlinien . . . . .	114
6.4.1	Differenzvergleich mit restriktiveren Richtlinie . . . . .	115
6.4.2	Differenzvergleich mit freizügigeren Richtlinie . . . . .	117
6.5	Ergebnis . . . . .	119
<b>7</b>	<b>Zusammenfassung und Perspektiven</b>	<b>123</b>
<b>Anhang</b>		<b>129</b>
A.1	Wahrheitstabellen für die Łukasiewicz-Logik $L_3$ . . . . .	129
A.2	Von XML zu OWL DL . . . . .	130
A.3	ExPDT-Spezifikation in OWL DL . . . . .	134
<b>Literaturverzeichnis</b>		<b>145</b>

## Abbildungsverzeichnis

1.1	Personalisierte Dienste im Szenario Einkaufszentrum . . . . .	3
2.1	Systemmodell für den Datenschutz . . . . .	16
2.2	Rahmenwerk zur Datenschutzautomatisierung . . . . .	20
2.3	Kundenpräferenzen im Rahmenwerk . . . . .	22
2.4	Elemente einer Datenschutzregel . . . . .	23
2.5	Zugriffskontrollmonitor nach Lampson . . . . .	24
2.6	Zeitliche Einordnung von Bedingungen und Obligationen . . . . .	25
3.1	Vergabe und Verwendung von Vertrauenssiegeln . . . . .	28
3.2	Interaktionen im P3P-Rahmenwerk . . . . .	30
3.3	Vererbung einer Autorisierung bei EPAL . . . . .	43
3.4	Vererbung eines Verbots bei EPAL . . . . .	43
3.5	Sticky Policy-Paradigma . . . . .	45
3.6	Modell für die Umsetzung von XACML . . . . .	49
4.1	NAPS-Operatoren zur Richtlinienkombination . . . . .	56
4.2	Logische Ebenen der ExPDT-Sprache . . . . .	61
4.3	OWL DL-Klassendiagramm der ExPDT-Sprache . . . . .	64
4.4	Benutzerhierarchie für Szenario Einkaufszentrum . . . . .	66
4.5	Beispiel für ein Obligationenmodell . . . . .	69
4.6	Anwendungsbereich einer Regel mit Anfrageelementen . . . . .	72
4.7	Auswertungsdurchlauf einer Richtlinie . . . . .	74
4.8	Normalisierung durch Segmentierung . . . . .	78
4.9	Regelweiser Vergleich zweier normalisierter Richtlinien . . . . .	87
4.10	Konstruktion der Wächterhülle . . . . .	90
4.11	Beschneidung des Rekursionsbaums zur Konstruktion von $\mathcal{R}_D^{\text{norm}}$ . . . . .	92
4.12	Anwendungsbereiche der Beispielwächter . . . . .	93
5.1	Werkzeugkette von ExPDT . . . . .	96
5.2	Abhängigkeiten der Ein- und Ausgabedateien . . . . .	99

5.3	ExPDT-Richtlinie für die Gesundheitsberatung im ExPDT-Editor . . . . .	100
5.4	Richtlinienoperationen im ExPDT-Editor . . . . .	101
6.1	Szenario des Einkaufszentrums . . . . .	104
6.2	Domänenansicht im ExPDT-Editor . . . . .	107
6.3	Erstellung und Auswertung von Anfragen im ExPDT-Editor . . . . .	114
6.4	Richtlinienvergleiche im Szenario . . . . .	115
6.5	Kundenrichtlinie in normierter Form . . . . .	116
6.6	Richtlinie des Beratungsdienstes in normierter Form . . . . .	118
6.7	Differenz der Richtlinien von Beratungsdienst und Kunden . . . . .	118
7.1	Geschäftsprozess- mit Compliance-Management . . . . .	125
7.2	Workflow mit zwei alternativen Kontrollprozessen . . . . .	127

## Tabellenverzeichnis

3.1	Bewertung von Vertrauenssiegeln . . . . .	29
3.2	Bewertung der Platform for Privacy Preferences (P3P) . . . . .	35
3.3	Bewertung des Customer Profile Exchange (CPExchange) . . . . .	37
3.4	Bewertung der Enterprise Privacy Authorisation Language (EPAL) . . . . .	46
3.5	Bewertung der Obligation Specification Language (OSL) . . . . .	48
3.6	Bewertung der eXtensible Access Control Markup Language (XACML) . . . . .	52
3.7	Bewertungsüberblick gegenwärtiger Richtliniensprachen . . . . .	53
4.1	NAPS Komposition . . . . .	59
4.2	NAPS Konjunktion . . . . .	60
4.3	Modalitäten in ExPDT . . . . .	71
4.4	Normalisierte Richtlinie . . . . .	85
4.5	Differenz zweier Richtlinien . . . . .	87
4.6	Erfüllbarkeitstests . . . . .	94
6.1	ExPDT im Vergleich zu gegenwärtigen Richtliniensprachen . . . . .	119
A.1	Wahrheitstabellen für die Łukasiewicz-Logik $L_3$ . . . . .	129
A.2	Für ExPDT wichtige Operatorkombinationen . . . . .	129

## **Algorithmenverzeichnis**

4.1	Auswertung einer ExPDT-Richtlinie . . . . .	73
4.2	Normalisierung einer Richtlinie – finale Regeln . . . . .	81
4.3	Normalisierung einer Richtlinie – anwendbare Regeln . . . . .	82
4.4	Normalisierung einer Richtlinie – Standardregeln . . . . .	83
4.5	Differenz zweier normalisierter Richtlinien . . . . .	88

## Quelltextverzeichnis

3.1	Beispiel einer P3P-Richtlinie . . . . .	32
3.2	Beispiel einer XPref-Benutzerpräferenz . . . . .	34
3.3	Beispiel einer EPAL-Richtlinie . . . . .	40
3.4	Beispiel einer EPAL-Anfrage . . . . .	41
3.5	Beispiel einer OSL-Richtlinie . . . . .	47
3.6	Beispiel einer XACML-Richtlinie . . . . .	51
4.1	ExPDT-Richtlinie für den Allergieberatungsdienst in OWL DL . . . . .	65
4.2	Komposition und Konjunktion in ExPDT . . . . .	70
6.1	Spezifikation einer Benutzerhierarchie . . . . .	106
6.2	Spezifikation einer Bedingungsrelation . . . . .	108
6.3	Bedingungsformel in OWL DL-Repräsentation . . . . .	108
6.4	Klassendefinition von Elementarobligationen . . . . .	109
6.5	Obligationsmenge als Instanz mehrerer Elementarobligationen . . . . .	109
6.6	ExPDT-Richtlinie für den Kasserdienst . . . . .	110
6.7	Komposition zweier Richtlinien . . . . .	110
6.8	ExPDT-Kompositionsoperator für zwei Richtlinien . . . . .	111
6.9	ExPDT-Richtlinie für Kunden . . . . .	112
6.10	Auswertungsanfrage für eine Richtlinie . . . . .	113
6.11	Beispiel für eine Variablenbelegung . . . . .	113

# 1 Privatsphäre als gesellschaftliche Forderung

## 1.1 Personalisierung auf Kosten der Privatsphäre?

Fast zwanzig Jahre nach Mark Weisers inspirierendem Artikel über Ubiquitous Computing [Weis91] wird seine Vision des allgegenwärtigen Rechnens technisch umsetzbar. Objekte des alltäglichen Lebens werden zunehmend miteinander vernetzt, die Kommunikation bezieht mobile Geräte jeglicher Größe und Leistung ein [GüSK03]. So entstehen hochdynamische Systeme mit neuen Herausforderungen an die Informationsverarbeitung [MAHK07]: Kontinuierlich werden neue Geräte mit ihren Diensten in das System aufgenommen, andere Geräte verlassen es wieder; Reaktionen auf solche Veränderungen müssen im System möglichst autonom ablaufen [KrKF04, KrKä04, KrKS05, MüAK05]. Zu berücksichtigen sind dabei die sich über die Zeit ändernden und möglicherweise sogar miteinander im Konflikt stehenden Geräteanforderungen und Benutzerpräferenzen, die einer dynamischen Aushandlung der Anforderung bedürfen. Ständig steigt die Flut gesammelter Daten, die auf verschiedenste Weise weiter verarbeitet und genutzt werden.

Mit der Lösung dieser technischen Herausforderungen gehen hohe Erwartungen an das ökonomische Potential solcher Systeme einher [SaSA06]. Eine erste Realisierung ist die Einführung von Radio Frequency Identification (RFID) bei bedeutenden Einzelhandelsgruppen. Während dabei zunächst nur die Einsparung durch Prozessautomatisierung im Vordergrund steht, geht im Einzelhandel die mögliche Verwendung solcher Technologien weit über die Optimierung der Lieferketten hinaus. Es können nicht nur Kosten gesenkt werden, sondern durch verbesserte Dienstleistungen kann auch mehr Umsatz erzielt werden. Eine Umsatzsteigerung kann erreicht werden, indem man neben der Auszeichnung von Artikeln mit RFID und Einsatz anderer Funk- und Sensortechnologien die Kunden mit mobilen Kommunikationsmitteln ausstattet und ihnen personalisierte Angebote und Dienste zur Verfügung stellt, wie dies etwa bereits im E-Commerce mit Recommender-Systemen geschieht [MuSa03].

### 1.1.1 Personalisiertes Einkaufen

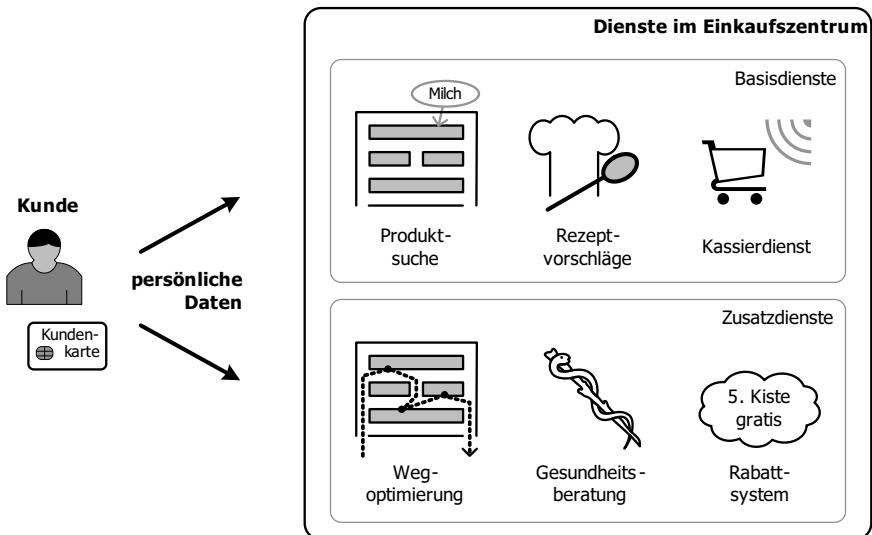
Heutzutage werden in Geschäften des Einzelhandels Kunden<sup>1</sup> mit tausenden Produkten konfrontiert. Häufig müssen sie eine große Fläche absuchen, bis sie die gewünschten Artikel gefunden haben. Zur Lösung dieses Problems stehen dynamische IT-Systeme zur Verfügung, die den Aufbau direkter, elektronischer Eins-zu-eins-Kommunikationskanäle zu den Kunden ermöglichen, um sie beispielsweise einem Navigationssystem gleich durch die Angebotspalette leiten, und gleichzeitig eine vergleichsweise billige und effektive Sammlung Kontextdaten erlauben.

In Geschäften wie dem Extra-Future-Store der METRO Gruppe werden kleine Computer mit Touch-Screen als Personal Shopping-Assistenten (PSA) an die Einkaufswagen angebracht und über die persönlichen Kundenkarten konfiguriert [LiWo06]. Aktuell sind diese Geräte mit Barcode-Lesern ausgestattet und können über WLAN mit dem Informationssystem des Händlers kommunizieren. Zukünftige Formen der Interaktion mit den Kunden könnten die Benutzung privater Mobiltelefone einschließen, um mit RFID ausgezeichnete Produkte zu identifizieren und Informationen vom Händlersystem zu erfragen [StSa04]. Des Weiteren könnten Sensoren, die in die Kleidung des Kunden eingearbeitet sind, Bestandteil der Interaktion werden. Eine solche technische Infrastruktur ermöglicht es, den Kontext des Kunden zu erfassen und mit in die Personalisierung der angebotenen Dienste einzubeziehen.

In Abbildung 1.1 ist ein solches Geschäft mit seinen Diensten skizziert. Betreten ihn nun mit entsprechenden PSAs ausgestattete Kunden, müssen sie, um ein bestimmtes Produkt zu finden, nur dessen Namen bzw. Beschreibung eingeben und bekommen gleich den Weg durch die Regalketten dorthin beschrieben. Um zusätzliche Informationen abzurufen, wie beispielsweise eine Liste möglicher Rezepte mit diesem Produkt als Zutat, scannen die Kunden nur dessen RFID-Tag. Ebenso können besondere Angebote entsprechend ihrer aktuellen Position im Ladengeschäft präsentiert werden. Auch können PSAs dafür verwendet werden, die laufenden Gesamtkosten der Artikel in den Warenkörben anzuzeigen und den Kunden so eine bessere Kontrolle über ihre Ausgaben zu gewähren. Schließlich müssen Kunden aufgrund automatisierter Kassierdienste nicht mehr in langen Schlangen anstehen und dann nach Kleingeld oder Karten suchen [LiWo06].

Solche Basisdienste können bereits auf Grundlage einfacher Kontextdaten angeboten werden. Deren Kombination mit Kundenprofilen erlaubt dem Händler jedoch, das Einkaufserlebnis der Kunden durch auf sie jeweils zugeschnittene Zusatzdienste weiter zu bereichern und durch Lock-in-Situationen eine möglichst enge Kundenbin-

<sup>1</sup> In dieser Arbeit verwendete Berufs- oder Funktionsbezeichnungen wie etwa Kunden, Händler oder Diensteanbieter gelten gleichermaßen für das weibliche wie für das männliche Geschlecht.



**Abbildung 1.1:** Für ein verbessertes Einkaufserlebnis und möglichst enge Kundenbindung werden die im Szenario angebotenen Dienste personalisiert und auf die jeweiligen Bedürfnisse der Kunden hin zugeschnitten.

dung zu erreichen [CDAL99, TaHo03, Choi06], um schließlich einen größeren Absatz von Produkten zu realisieren [SrBh05]. Für diese Personalisierung bedarf es allerdings umfangreicher persönlicher Daten wie etwa Name, Alter, Kaufhistorie oder Mitgliedschaft im Kundenprogramm.

Nach der Identifizierung der Kunden, beispielsweise durch ihre Kundenkarten, können ihre Einkaufszettel, die zuvor elektronisch auf den Kundenkarten selbst oder im Internet hinterlegt und dann verwendet werden, um eilige Kunden zielgerichtet durch den Geschäftsraum zu leiten. Ein solches System ermöglicht es Kunden nicht nur, in der Fülle der Waren die gewünschten Produkte zu finden, sondern darüber hinaus auf Angebote zu treffen, die genau auf ihre individuellen Bedürfnisse zugeschnitten sind. Den Kunden können besondere Angebote auf Bildschirmen angezeigt werden, nicht nur entsprechend der Position im Geschäftsraum, sondern auch entsprechend der Artikel auf den Einkaufslisten oder passend zu den Artikeln, die sich bereits in den Warenkörben befinden. Diese Angebote können dabei an den persönlichen Bedürfnissen der Kunden wie etwa nach fettfreier Nahrung oder Biokost ausgerichtet werden. In gleicher Weise können Allergiker von einer Gesundheitsberatung vor bestimmten Inhaltsstoffen in den ausgewählten Produkten gewarnt werden. Schließlich liefert die Historie zurückliegender Einkäufe die Basis für besondere Rabattpogramme.

me, die vom Händler selbst oder von externen Dienstleistern wie beispielsweise dem Unternehmen Loyalty Partner angeboten werden können [Laue04, Loya08].

### 1.1.2 Risiko des Privatsphärenverlustes

Mit der fortschreitenden Technologieentwicklung werden die zur Datensammlung genutzten Geräte kleiner, nahezu unsichtbar für die Kunden. Zugleich werden die gesammelten Daten qualitativ hochwertiger. Nicht nur liefern einzelne Dienste mehr und Sensoren genauere Daten, sondern die für die Personalisierung erzielten Erkenntnisse decken durch Zusammenschluss, Verkettung und Interpretation der Daten ein breites Spektrum ab.

Dies trifft in dem hier betrachteten Szenario des Einzelhandels auf besonders große Skepsis bei Kunden, denn die Datensammlung dringt immer tiefer bis in die innersten privaten Lebensbereiche vor. Anders als im E-Commerce wird das reale Leben unmittelbar betroffen, die Konsequenzen aus der Personalisierung von den Kunden noch direkter wahrgenommen. Angewiesen auf die angebotenen Waren und Dienste der Einzelhändler, können sich Kunden der Datensammlung nicht mehr entziehen. Ihr ausgeliefert können Kunden Besorgungen nicht mehr anonym erledigen und müssen befürchten, gleichsam gläsern zu werden und so eine Analyse ihrer persönlichen Bedürfnisse und innersten Wünsche zuzulassen.

Obwohl das ökonomische Potential der Personalisierung im Einzelhandel sowohl für die Händler als auch die Kunden vielversprechend und gewinnbringend zu sein scheint, haben die Einzelhandelsgruppen als Reaktion ihr Engagement und ihre Aktivitäten in diesem Bereich reduziert. Während Wal-Mart die RFID-Auszeichnung von Artikeln mit einer Videoüberwachung kombinierte, versuchte die METRO Gruppe in die Kundenkarte einen RFID-Tag einzubetten. Nach scharfer Kritik, dass aufgrund der Verkettung von Informationen Kunden ihre Privatsphäre aufgeben müssten, stoppte Wal-Mart seine RFID-basierte Überwachung [KöWF06], und die METRO entschied sich gegen eine weitere Verwendung von RFID in ihren Kundenkarten. Des Weiteren werden nun auch die Auswirkungen dieser Technologien auf die Privatsphäre außerhalb der Geschäfte untersucht. So laufen etwa Bestrebungen, die RFID-Auszeichnung auf Artikelebene nur dann einzuführen, wenn eine Personenverfolgung und ein Eindringen in die Privatsphäre außerhalb der Geschäftsräume beispielsweise durch Zerstörung der Tags unterbunden werden kann [SWKG07].

Geprägt von Prognosen wie „the death of privacy“ [Froo00] und „will privacy remain a luxury good?“ [BöKo07] sowie der Aufdeckung versteckter Überwachungs-techniken [FoeB03] weisen Benutzer bei ihrer Interaktion mit solchen Umgebungen eine negative Grundeinstellung auf. Eine Analyse der entscheidenden Bedenken zeigt,