Beiträge zur Untersuchung der informationellen Privatheit im Rahmen des Experiential Computing

Dissertation

zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaft

der Rechts- und Wirtschaftswissenschaftlichen Fakultät

der Universität Bayreuth

Vorgelegt

von

Christoph Buck

aus

Dettingen an der Erms

Dekan:	Prof. Dr. Martin Leschke
Erstberichterstatter:	Prof. Dr. Torsten Eymann
Zweitberichterstatter:	Prof. Dr. Claas Christian Germelmann
Tag der mündlichen Prüfung:	26. September 2017

Für meine Eltern

Zusammenfassung

Durch *pervasive computing* und bedienerfreundliche Anwendungen durchdringen Informationssysteme die Gesellschaft. Digitale Geräte wie beispielsweise vernetzte Gegenstände, Wearables, Smart Homes und Smartphones unterstützen durch bedienerfreundliche Anwendungen den Alltag von beruflichen und privaten Nutzern. Über Smart Mobile Devices und mobile Applikationen verfügt die breite Masse von Nutzern über hochleistungsfähige und weltweit vernetzte Informationssysteme, welche die Möglichkeiten und Fähigkeiten eines jeden Einzelnen erweitern. Diese rapide Entwicklung hin zu Nutzer-zentrierten Informationssystemen ist ausschließlich unter der starken Einbindung der Nutzer selbst verwirklichbar, wodurch die Möglichkeiten der Aufnahme, Verarbeitung und Speicherung von persönlichen Informationen massiv ausgeweitet werden. Die vorliegende Dissertation nimmt mit der Einführung des *experiential computing* einen Perspektivenwechsel hin zum *neuen Nutzer* von Informationssystemen vor. Dieser stellt in Nutzer-zentrierten Systemen, die in Smart Mobile Devices und mobilen Applikationen zu sehen sind, einen selbständigen Teil des Informationssystems dar. Der dadurch substantielle Wertbeitrag von Nutzern in Informationssystemen, vornehmlich durch die Preisgabe persönlicher Daten, führt zu weitreichenden individuellen gesellschaftlichen Herausforderungen hinsichtlich deren Privatheit.

Die vorliegende Dissertation trägt zur Untersuchung des Privatheitsverhaltens bei und leistet einen Forschungsbeitrag zur Erklärung des vermeintlich paradoxen Nutzungsverhaltens. Die Arbeit nimmt sich der zugrundeliegenden übergeordneten Forschungsfrage an: Welche Einflussvariablen bedingen Privatheitsentscheidungen beim Bezug und der Nutzung von mobilen Applikationen?

Informationelle Privatheit wird im Rahmen der Dissertation definitorisch eingeordnet und in Bezug zu relevanten Forschungsarbeiten der Forschungsdomäne des Information Systems Research gesetzt. Zentrale Elemente der Privatheitsforschung, wie die Privatheitsbedenken, das Privatheitskalkül und das Privatheitsparadox werden aufgearbeitet und durch bestehende Makromodelle in Bezug zueinander gesetzt.

Um zur Beantwortung der aufgeworfenen Forschungsfrage beizutragen werden acht Beiträge zur Untersuchung der informationellen Privatheit im Rahmen des *experiential computing* in einem Forschungsrahmen strukturiert und vorgestellt. Im Rahmen von drei Forschungsbeiträgen wird der Entscheidungskontext von Privatheit

in mobilen Ökosystemen untersucht. Hierbei werden Forschungsergebnisse hinsichtlich möglicher Wahrnehmungsverzerrungen und dem Informations-Such-Verhalten von Nutzern in mobilen Ökosystemen erzielt. Zwei Forschungsbeiträge tragen zu einem besseren Verständnis des wahrgenommenen Werts der Privatheit durch die Nutzer bei. Aufgrund der Beschaffenheit von Privatheit kann deren Wert als abstrakt klassifiziert werden. Die Nutzer sehen in der Wahrung ihrer Privatheit ein kaufrelevantes Attribut von mobilen Applikationen. Im Rahmen von drei weiteren Forschungsbeiträgen wird der Bereich der Privatheitsbedenken und deren Einflussfaktoren erforscht. Hierbei kann ein an den Entscheidungskontext angepasstes Messinstrument vorgestellt und verschiedene Einflussfaktoren auf die Privatheitsbedenken identifiziert werden. Die Dissertation schließt mit einer kritischen Reflexion und identifizierten Forschungsbedarfen.

Inhaltsverzeichnis

1 Einleitung 1

2 Der Nutzer im Rahmen des Experiential Computing 4

2.1 Der neue Nutzer von Informationssystemen 4

2.2 Mobile Applikationen als Bestandteil des Experiential Computing 9

2.3 Der Wertbeitrag des Nutzers in Informationssystemen 11

3 Privatheit und Informationssysteme 13

3.1 Informationelle Privatheit 13

3.2 Informationelle Privatheitsbedenken in Informationssystemen 18

3.3 Informationelle Privatheit als Teil einer ökonomischen Austauschbeziehung 20

3.4 Das Privatheitsparadox in Informationssystemen 24

3.5 Makromodelle der Privatheitsforschung 25

4 Privatheit und mobile Applikationen 31

4.1 Forschungsagenda 31

4.2 Der Kontext des Entscheidungsverhaltens beim Bezug mobiler Applikationen 33

4.2.1 Das Privacy Paradox bei mobilen Applikationen: Kontextuale Besonderheiten mobiler Applikationen (Buck & Eymann, 2013) ... 34

4.2.2 Der unbewusste App-Nutzer: Das Informations-Such-Verhalten von App-Nutzern (Buck, Horbel, Germelmann et al., 2014) 38

4.2.3 Ein Kontextrahmenwerk für die Wahrnehmung mobiler Applikationen (Buck, Horbel et al., 2017) 42

4.3 Privatheit als wahrgenommener Wert 46

4.3.1 Privatheit als abstrakter Wert (Buck, 2015) 47

4.3.2 Privatheit als kaufrelevantes Produktattribut von mobilen

Applikationen (Buck, Stadler et al., 2017) 50

4.4 Privatheitsbedenken bei mobilen Applikationen.....53

4.4.1 Privatheitsbedenken bei mobilen Applikationen (Buck & Burster, 2017) 54

4.4.2 Der Zusammenhang zwischen kognitiven Verzerrungen und Privatheitsbedenken (Buck, Burster et al., 2017) 58

4.4.3 Der Zusammenhang zwischen der Identifikation mit dem zukünftigen Selbst und Privatheitsbedenken (Buck, 2017)..... 61

5 Kritische Reflexion und zukünftige Forschung.....64

6 Literaturverzeichnis 67

Abbildungsverzeichnis

Abbildung 1. Schematic Framework of Experiential Computing (Yoo, 2010, p. 219). 9

Abbildung 2. Dreiwertige, verzögerte Transaktion (Buck, Germelmann et al., 2016, p. 60). 23

Abbildung 3. Information Privacy Concern Multilevel Framework (Bélanger & Crossler, 2011, p. 1032). 27

Abbildung 4. Integrative Framework for the Study on CFIP (Li, 2011, p. 466). 28

Abbildung 5. APCO Macro Model (Smith et al., 2011, p. 998). 29

Abbildung 6. Enhanced APCO Model (Dinev et al., 2015, p. 643). 30

Abbildung 7. Einordnung der Forschungsbeiträge im erweiterten APCO-Modell (in Anlehnung an Dinev et al., 2015, p. 643). 32

Abbildung 8. Entscheidungskontext mobiler Applikationen (Buck & Eymann, 2013, p. 1992). 36

Abbildung 9. General framework of an app purchase decision-making process (Buck, Horbel, Germelmann et al., 2014, p. 5). 39

Abbildung 10. The context framework of app perception (Buck, Horbel et al., 2017). 44

Abbildung 11. Setup of the Study (Buck, 2015, p. 109). 48

Tabellenverzeichnis

Tabelle 1. Einflüsse auf die Entwicklung des Privatheitsbegriffs (Smith et al., 2011; Westin, 2003). 14

Tabelle 2. Übersicht über Messinstrumente für Privatheitsbedenken (in Anlehnung an Buck & Burster, 2017; Xu et al., 2012). 20

Table 3. Items of the AIPC (Buck & Burster, 2017, pp. 6–7). 55

Abkürzungsverzeichnis

A	Antecedents
AIPC	App Information Privacy Concern
CBC	Choice-Based-Conjointanalyse
CFIP	Concern for Information Privacy
CVM	Contingent Valuation Method
DCA	Discrete Choice Analysis
FSC	Future Self-Continuity
IS	Information Systems
IUIPC	Internet Users‘ Information Privacy Concerns
MAT	Mensch-Aufgabe-Technik
MUIPC	Mobile Users’ Information Privacy Concerns
O	Outcomes
PC	Privacy Concerns
SDK	Software Development Kit
SDL	Service Dominant Logic
SMD	Smart Mobile Devices
TCA	Traditional Conjoint Analysis

1 Einleitung

„Privatsphäre sollte nicht nur eine Wahl sein, die wir treffen können, und sie sollte sicherlich nicht der Preis sein, den wir bezahlen müssen, nur um im Internet surfen zu dürfen.“ (Kovacs, 2012).

Durch technologische Errungenschaften wie dem *pervasive computing* sind die Umgebung und der Alltag von Nutzern durchdrungen mit vernetzter Informationstechnologie. Digitale Geräte wie beispielsweise vernetzte Gegenstände, Wearables, Smart Homes und Smartphones sind, meist über mobile Applikationen, für private Nutzer zugänglich. Die hierbei generierten und von den Nutzern preisgegebenen Daten werden dynamisch verarbeitet und ermöglichen teilweise vollkommen neuartige digitale Services. Die immer weiter steigende Nutzerfreundlichkeit wird bedingt durch die Selbstverständlichkeit der digitalen Anwendungen und eine damit verbundene zunehmende *Unsichtbarkeit* von Informationssystemen. Die fortschreitende Alltagsintegration und das zunehmende Verschwinden von Informationssystemen in den Hintergrund führt zu einem *personal data paradox*: Je tiefer verankert und *unsichtbarer* Informationssysteme werden, desto selbstverständlicher und weniger hinterfragt wird deren Nutzung und desto höher ist das durch die freigegebenen Daten verbundene Risiko und der hierdurch entstehende Wert.

Persönliche Daten stellen in der digitalisierten Wirtschaft und Gesellschaft mittlerweile einen hohen ökonomischen Wert dar. Durch (persönliche) Daten können neue Wertangebote geschaffen, bestehende verbessert und zahlreiche betriebliche Fragestellungen optimiert werden (Spiekermann-Hoff et al., 2015). Das Weltwirtschaftsforum hat aus diesen Gründen persönliche Daten als eigene Güterklasse definiert und folgt damit zahlreichen Stimmen aus Wissenschaft und Wirtschaft, die in persönlichen Daten und informationeller Privatheit ein handelbares Gut sehen (Schwab et al., 2011). Die initiale ökonomische Austauschbeziehung findet hierbei zwischen den Nutzern und den jeweiligen Anbietern von digitalen Anwendungen im Hinblick auf die Preisgabe ihrer persönlichen Daten statt. Hierbei wird den Nutzern im Rahmen des Privatheitsparadox ein widersprüchliches Verhalten

unterstellt (Norberg et al., 2007). In zahlreichen Befragungen geben Nutzer hohe Bedenken bezüglich ihrer Privatheit an, messen dieser einen hohen Wert zu und formulieren die Absicht keine Anwendungen zu nutzen die ihre Privatheit bedrohen. Das tatsächliche Nutzerverhalten steht aber in konträrer Beziehung zu der formulierten Verhaltensabsicht. Mit dem Bezug von Milliarden mobilen Applikationen, der Freischaltung von zahlreicher Sensorik und der zunehmenden Integrationen von vernetzten Geräten geben Nutzer zunehmend weite Teile ihrer Privatheit preis – oft ohne dies zu wissen oder wahrzunehmen. Demnach muss die ökonomische Austauschbeziehung auch vor dem Hintergrund der Chancengleichheit und der Bewertbarkeit durch die Nutzer hinterfragt werden. Privatheit darf keine Wahl sein, die Nutzer nur wählen können indem sie Informationssysteme nicht nutzen. Privatheit darf im Gegensatz dazu aber auch kein Zwang sein, der die, durch Informationssysteme entstehenden, Möglichkeiten verhindert.

Um diese drängenden gesellschaftlichen Herausforderungen in der digitalen Zukunft meistern zu können, müssen Nutzer in ihrem jeweiligen Nutzungskontext verstanden werden. Die wissenschaftliche Forschung muss Erkenntnisse hinsichtlich dem Entscheidungskontext, aber auch der Rollenwahrnehmung der Nutzer in Informationssystemen und des damit verbundenen Wertbeitrags erzielen. Hierauf aufbauend muss ein Verständnis für das Verhalten von Nutzern in digitalen Systemen entwickelt werden.

Die vorliegende Dissertation trägt zur Untersuchung des Privatheitsverhaltens bei und leistet einen Forschungsbeitrag zur Erklärung des vermeintlich paradoxen Nutzungsverhaltens. Die Arbeit nimmt sich der zugrundeliegenden übergeordneten Forschungsfrage an: Welche Einflussvariablen bedingen Privatheitsentscheidungen beim Bezug und der Nutzung von mobilen Applikationen?

Um einen wissenschaftlichen Beitrag zur Beantwortung der Forschungsfrage leisten zu können ist die Dissertation wie folgt aufgebaut. Im zweiten Kapitel wird mit dem *experiential computing* eine neue Perspektive auf Informationssysteme im Allgemeinen und den Nutzer im Speziellen eingeführt. Der Wertbeitrag von Nutzern in Informationssystemen wird neu beschrieben. Das dritte Kapitel legt die definitorischen Grundlagen für die informationelle Privatheit, auf welche sich die Forschungsarbeiten fokussieren. Zudem werden die zentralen Begrifflichkeiten und Theorien der Privatheitsforschung der Forschungsdomäne des Information Systems

Research aufgearbeitet. Im vierten Kapitel werden die Forschungspublikationen in einen Forschungsrahmen eingeordnet. Die insgesamt acht Forschungsbeiträge werden in Unterkapitel 4.1 in drei zentrale Forschungsbereiche mit bestehendem Forschungsbedarf strukturiert. Unterkapitel 4.2 stellt Forschungsbeiträge vor, die den Kontext der Entscheidungssituation bezüglich der Preisgabe von Privatheit in mobilen Ökosystemen beleuchten. In Kapitel 4.3 werden zwei Forschungsbeiträge vorgestellt, die den Wert von persönlichen Daten aus Sicht der Nutzer untersuchen. Unterkapitel 4.4 widmet sich mit drei Forschungsbeiträgen den Privatheitsbedenken in mobilen Ökosystemen und möglichen Einflussfaktoren. Die vorliegende Dissertation schließt mit dem fünften Kapitel und einer kritischen Reflexion sowie der Vorstellung von identifizierten Forschungsbedarfen.

2 Der Nutzer im Rahmen des Experiential Computing

2.1 Der neue Nutzer von Informationssystemen

Ein Informationssystem stellt ein System dar, welches „… für die Zwecke eines Teils eines bestimmten Unternehmens entwickelt und implementiert beziehungsweise in diesem Betrieb eingesetzt wird. Ein Informationssystem enthält die dafür notwendige Anwendungssoftware und Daten und ist in die Organisations-, Personal- und Technikstrukturen des Unternehmens eingebettet." (Laudon et al., 2010, p. 17).

Zwar findet sich keine einheitliche Definition des Begriffs Informationssystem, da Information in der Literatur entweder als Tätigkeit oder als Objektart verstanden wird (Ferstl & Sinz, 2013), doch steht die Definition von Laudon und Laudon (2010) hinsichtlich der grundlegenden Perspektive im Einklang mit klassischen Definitionen von Informationssystemen aus der deutschsprachigen Wirtschaftsinformatik und der internationalen Forschungsdomäne des Information Systems Research (IS).[1] In der Literatur beziehen sich zahlreiche Autoren in ihren Definitionen auf eine eindeutige organisationale Verankerung und sehen für Informationssysteme in der Nutzung zur betrieblichen Anwendung ein konstituierendes Merkmal (Grochla, 1975; Mertens, 2013; Scheer, 1998).

Die originären Nutzer spielen in der Betrachtung von Informationssystemen und deren Auswirkungen in der gängigen IS-Literatur nur eine untergeordnete Rolle. Heinrich et al. (2011) beschreiben durch das Mensch-Aufgabe-Technik-Paradigma (MAT) im Nutzer zwar ein zentrales Objekt, doch wird die Nutzungsmotivation von Informationssystemen durch die Erfüllung von klar formulierten (betrieblichen) Aufgaben beschrieben (Heinrich et al., 2011). Somit handelt es sich bei Informationssystemen um computergestützte Systeme „aus Menschen und Maschinen" (Hansen et al., 2015, S. 131) bei denen Informationen durch leistungsfähige Informations- und Kommunikationstechniken erfasst, verarbeitet, gespeichert und übertragen werden (Hansen et al., 2015; Pearlson et al., 2016).

Nutzer von Informationssystemen werden in der Forschungsdomäne der IS klassischerweise als atomistische Anwender des Gesamtsystems, beziehungsweise

[1] In der folgenden Ausarbeitung werden beide Domänen einheitlich mit Information Systems Research (IS) bezeichnet.

dessen Anwendungssystemen, angesehen (Lamb & Kling, 2003). Die Motivation zur Nutzung der Informationssysteme wird mit der Erfüllung vorab definierter Aufgaben begründet. Hierbei nutzen die Anwender die Informationssysteme zur Unterstützung ihrer geistigen Arbeiten und zur Optimierung der bestehenden Geschäftsprozesse (Lamb & Kling, 2003).

Aufgrund von zwei maßgeblichen und zusammenhängenden Entwicklungen muss die Sichtweise der IS auf die Nutzer von Informationssystemen grundlegend geändert werden: Der Allgegenwärtigkeit und Unsichtbarkeit von Informationssystemen in der Gesellschaft und einem neuen Nutzer von Informationssystemen (Yoo, 2010).

Die Allgegenwärtigkeit von Informationssystemen wird durch unterschiedliche Begrifflichkeiten diskutiert, meist aber mit *ubiquitous computing* benannt. Der Begriff wurde vor allem durch Weiser (1991) geprägt, welcher darunter Umgebungen versteht, die durch vernetzte Informationssysteme in jeder erdenklichen Hinsicht unterstützt werden (Weiser, 1991). Somit können Nutzer jederzeit und an jedem Ort auf Informationssysteme zugreifen (Lyytinen et al., 2004). Zwar konnte sich keine einheitliche Definition des Begriffs entwickeln, doch kann unter *ubiquitous computing* die Allgegenwärtigkeit von Informationstechnik und Computerleistung verstanden werden, durch die prinzipiell alle Alltagsgegenstände vernetzt werden können (Weiser, 1993). Ein maßgeblicher Faktor des *ubiquitous computing* ist dessen Bezug zur Gesellschaft. So vollzieht sich die Mensch-Maschine-Interaktion beim *ubiquitous computing* nahtlos und wird unbemerkt in den Nutzungsabläufen verankert (Silva et al., 2014). Während der Nutzer in der traditionellen Betrachtung das Informationssystem aktiv bedient und eine Interaktion anstößt, kehrt sich dieses Szenario um. Informationssysteme sind in der Umwelt integriert und dienen dem Nutzer nicht als persönliche Assistenten, sondern vielmehr als Erweiterung der eigenen Möglichkeiten und Fähigkeiten (Olson et al., 2015). *Ubiquitous Computing* stellt keine Abkehr von traditionellen (betrieblichen) Informationssystemen, sondern deren natürliche Weiterentwicklung dar (Avital & Germonprez, 2003).

Die Integration in den Alltag der Nutzer wird durch den oft synonym verwendeten Begriff des *pervasive computing* enger erfasst (Dhawan et al., 2016; Saha & Mukherjee, 2003), wenngleich konzeptionelle Unterschiede zwischen beiden Begrifflichkeiten bestehen (Lyytinen et al., 2004). Während sich der Term *ubiquitous computing* hauptsächlich auf die Vernetzung von Rechnerknoten, deren unbewusste

Nutzung, deren Aktivität im Hintergrund und die Errungenschaften der drahtlosen Kommunikation fokussiert, schließt der Begriff des *pervasive computing* hierauf aufbauend die Integration des Nutzerkontexts und -umfelds mit ein (Zhao & Wang, 2011). Demnach integriert der Begriff *pervasive computing* smarte Umwelten mit möglichst unaufdringlicher und unsichtbarer Rechnerleistung, welche zu jeder Zeit und an jedem Ort verfügbar ist (Satyanarayanan, 2001). *Pervasive computing* erweitert somit den Anwendungsbereich von Informationssystemen von der betrieblichen Nutzung auf den Bereich der Nutzung im privaten Alltag. Damit können der menschliche Körper und sämtliche Alltagsgegenstände durch die Integration und Nutzung von Sensoren und Prozessoren vernetzt werden. Hierdurch kann eine smarte Umgebung geschaffen werden, welche unsichtbar, unaufdringlich aber jederzeit verfügbar ist (Dhawan et al., 2016). Das *pervasive information system* kann den Kontext des Nutzers erfassen, Hintergrund- und Kontextinformationen zielgerichtet nutzen und die Fähigkeiten und Möglichkeiten des Nutzers situativ und dynamisch erweitern (Segura & Thiesse, 2015; Zhao & Wang, 2011). In Verbindung mit *pervasive computing* erfährt die Begrifflichkeit des *invisible computing* in der Literatur Aufmerksamkeit (Borriello, 2000; Saha & Mukherjee, 2003; Tripathi, 2005), welche die Eigenschaft von modernen Informationssystemen, für den Nutzer weitestgehend unsichtbar zu sein, hervorhebt (Borriello, 2008; Hayes et al., 2007; Thompson, 2005; Zhao & Wang, 2011).[2]

Die Entwicklung hin zu Allgegenwärtigkeit von Informationssystemen wäre jedoch ohne eine Ausweitung der Anwendungsgebiete, weg von der rein betrieblichen Anwendung und hin zur alltäglichen Nutzung, nicht möglich gewesen. Durch rasante Entwicklungen wie der Miniaturisierung, steigender Prozessor- und Speicherkapazitäten und der Ausweitung weltweiter Kommunikationsnetze gelangt das *pervasive computing* in den Alltag der privaten Anwender. Durch Sensoren, smarte Objekte und die Interaktion durch und mit Informationssystemen (*tangible computing*) wird der Alltag von Nutzern zunehmend mit Informationssystemen angereichert. Die Nutzer selbst stellen in derartigen Systemen zentrale Akteure dar. Dieser interagiert mit den Informationssystemen, nutzt vernetzte smarte Alltagsgegenstände, und erweitert das bestehende System durch seine alltägliche

[2] Für die drei vorgestellten Computing-Begriffe wird im weiteren Verlauf der vorliegenden Ausarbeitung einheitlich der Begriff *pervasive computing* verwendet, da die graduellen Unterschiede für die weitere Betrachtung unerheblich sind.

Nutzung (Yoo, 2010). Der Nutzer dieser Informationssysteme kann nicht mehr verstanden werden als ein auf Funktionalität und Praktikabilität fokussierter atomistischer Nutzer im betrieblichen Arbeitsumfeld. Vielmehr wird *pervasive computing* für den Nutzer erlebbar, wodurch die Nutzungsmotivation nicht mehr auf die Erfüllung einer Aufgabe beschränkt werden kann (Sullivan et al., 2009). Da *pervasive computing* als eine *post-Desktop Ära* angesehen wird (Segura & Thiesse, 2015; Zhao & Wang, 2011), in der Nutzer in smarten Umgebungen und mit smarten Alltagsobjekten interagieren, muss auch die Perspektive auf die Nutzer geändert werden (Lamb & Kling, 2003; Yoo, 2010).

Um dieser Sichtweise gerecht zu werden hat Yoo (2010) den Begriff des *experiential computing* eingeführt, welcher definiert wird als „digitally mediated embodied experiences in everyday activities through everyday artifacts with embedded computing capabilities." (Yoo, 2010, S. 215). Yoo (2010) erweitert die Sichtweise von Lamb und Kling (2003), welche den Nutzer im Rahmen von (betrieblichen) Organisationen betrachten, der seine Informationsbedürfnisse befriedigt und hierbei als sozialer Akteur auftritt. Im Rahmen des *experiential computing* werden diese kritischen Dimensionen erweitert. Nutzer werden nicht mehr zwingend als Angehörige einer Organisation betrachtet, sondern vielmehr als für sich stehende Individuen.[3] Hierdurch trägt Yoo (2010) dem Fakt Rechnung, dass grundlegende Fragen der Technologie-Akzeptanzforschung, aufgrund des natürlichen Kontakts von beispielsweise „digital natives" mit Informationssystemen (Prensky, 2001), in Zukunft an Relevanz verlieren werden (Yoo, 2010). Die Nutzung von Informationssystemen muss über organisationale Grenzen hinaus und jenseits der Erfüllung von vorgegebenen Aufgaben betrachtet werden. Diese erweiterte Perspektive drückt sich auch in der Anwendung von Informationssystemen aus (Yoo, 2010). So werden zunehmend alltägliche Gegenstände digital, d.h. durch Sensorik angereichert, um das bestehende Informationssystem zu erweitern. Dadurch ändert sich auch die Motivationsrichtung der Nutzung von Informationssystemen durch die Anwender. Nutzer greifen auf Informationssysteme nicht nur zur Erfüllung von Informationsbedürfnissen zurück, sondern zunehmend um hedonische Bedürfnisse zu

[3] Die Perspektive des experiential computing kann jedoch wiederum starken Einfluss auf die Nutzung von betrieblichen Informationssystemen durch die Nutzer haben Buck et al. (2015); Buck and Eymann (2014).

befriedigen (Sullivan et al., 2009).

Durch die tiefgreifende Integration von Informationssystemen in das Alltagsleben der Nutzer sollte in der Forschungsdomäne der IS vielmehr der Nutzer selbst und seine Interaktion mit dem von ihm genutzten Informationssystem, als die reine Betrachtung des Artefakts, im Mittelpunkt des Interesses stehen (Yoo, 2010). Die Betrachtung des Begriffs *computing* ändert sich damit zunehmend vom Nomen hin zum Verb. Vor allem die Tatsache, dass Informationssysteme weitestgehend im Hintergrund und für den Nutzer oft unsichtbar und ohne aktive Bedienung agieren, bedarf einer erhöhten Aufmerksamkeit für den Nutzer selbst.

Experiential computing beschreibt eine neue Sichtweise auf die Verwendung von Informationssystemen und setzt sich deutlich von den bisherigen Perspektiven der hermeneutischen Beziehung zwischen Informationssystemen und ihren Nutzern und klaren Abgrenzung zwischen Nutzern und Informationssystemen ab (Ihde, 2010; Yoo, 2010).

Im Rahmen des *experiential computing* nehmen Nutzer Informationssysteme nicht mehr als fremdartige Technologie wahr, sondern verstehen sich selbst als Teil des Systems in dem sie leben und an dem sie partizipieren (Yoo, 2010). Demnach muss *experiential computing* verstanden werden als die verkörperte Beziehung zwischen Informationssystemen als Technologie, der realen Welt und den Nutzern (Ihde, 2010). Damit stellt die soziale und physische Realität im Rahmen von Informationssystemen nicht mehr eine abstrakte, sondern eine tatsächliche Erfahrung dar, die durch das Selbstverständnis des Nutzers „I am in the world and my existence in the world shapes the way I understand it" (Yoo, 2010, S. 218) beschrieben werden kann. Hierdurch unterstreicht die Verkörperung des Informationssystems die bedeutende Rolle der physischen, direkten und existentiellen Partizipation in der realen Welt in der die Nutzer leben. Dewey (1934) und Merlau-Ponty (1962) folgend, kann die verkörperte menschliche Erfahrung als Zusammenspiel zwischen dem Körper und der Umwelt dargestellt werden (Dewey, 1934; Merleau-Ponty, 1962). Das Umfeld wird charakterisiert durch die vier Dimensionen Raum, Zeit, andere Akteure und Dinge. Abbildung 1 stellt das Rahmenkonzept des *experiential computing* dar.

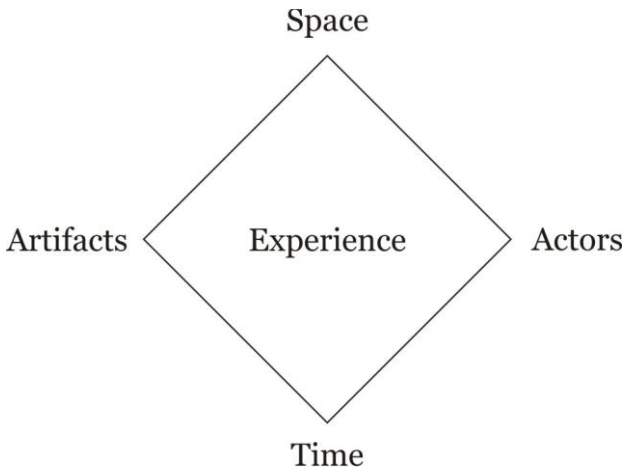

Abbildung 1. Schematic Framework of Experiential Computing (Yoo, 2010, S. 219).

2.2 Mobile Applikationen als Bestandteil des Experiential Computing

Mobile Ökosysteme stellen die am meisten genutzte Klasse an Informationssystemen in der Gesellschaft dar und bestehen aus den Hardwarekomponenten Smart Mobile Devices (SMD) und den Softwarekomponenten mobiles Betriebssystem und mobile Applikationen (Apps).[4] Aufgrund der computergestützten Erfassung, Verarbeitung, Speicherung und Übertragung von Informationen durch den Einsatz leistungsfähiger und automatisierter Informations- und Kommunikationstechniken handelt es sich bei mobilen Ökosystemen um Informationssysteme (Hansen et al., 2015; Pearlson et al., 2016).

Das SMD stellt hierbei die Hardwareschnittstelle des Nutzers zum Informationssystem dar. Aufgrund der Integration unterschiedlicher Geräteklassen und der vielfältigen und durch Apps individualisierbaren Anwendung gelten SMD als sogenannte Killerapplikationen des *pervasive computing* (Abowd et al., 2005).

Das konstituierende Merkmal von SMD ist in Apps zu sehen. Diese stellen aktuell die häufigste Mensch-Maschine-Schnittstelle dar. Als Nutzer-zentrierte Anwendungssoftware sind sie eine „… optimierte Schnittstelle zwischen dem Benutzer und dem Smartphone/Tablet …“ (Achten & Pohlmann, 2012, S. 161). Apps werden von Buck und Eymann (2013) definiert als „Softwareprogramme, die auf SMD abhängig von deren mobilem Betriebssystem, installiert werden können. Die Programme nutzen

[4] Unter SMD werden im Rahmen der vorliegenden Ausarbeitung alle Ausprägungen zwischen den Geräteklassen Smartphone und Tablet subsumiert.

Internet- und Cloud-Computing-Anwendungen, um zum Teil stark fragmentierte (Alltags-) Bedürfnisse der Nutzer durch digitalisierte Anwendungs- und Dienstleistungsangebote zu befriedigen." (Buck & Eymann, 2013, S. 1987).

Hierbei können Apps aufgrund der offen gestalteten Software Development Kits (SDK) der Ökosystemanbieter auf nahezu alle Ressourcen des SMD (in Abhängigkeit der gewährten Zugriffsrechte) zugreifen (Holzer & Ondrus, 2011). Durch die Nutzung der vorgehaltenen Sensoren, Hardware-Ressourcen und Nutzerdaten können Apps angeboten werden, welche individuelle und stark fragmentierte Alltagsbedürfnisse der Nutzer befriedigen können.

Die Erlebbarkeit und tiefgreifende Alltagsverankerung, weswegen Apps als Bestandteil des *experiential computing* angesehen werden können, wird durch die Ökosystemintegration der Softwareprogramme erreicht. Durch die Individualisierbarkeit von SMD durch Apps werden die vier Erfahrungsdimensionen durch das Informationssystem direkt beeinflusst.

Durch SMD wurde Software in Form von Apps fest in das Alltagsleben von Nutzern integriert. Weiter wachsende Möglichkeiten des Einsatzes von Sensorik und Vernetzung erweitern das Erfahrungsspektrum laufend. Die rasant steigende Anzahl von Apps als Mensch-Maschine-Schnittstelle unterstreicht diese Entwicklung. Der Soft- und Hardwareanbieter Apple fasst dieses Selbstverständnis treffend mit seinem Werbeslogan „There's an app for that" zusammen (Apple Inc., 2017). Die drei Teile *There's*, *an app* und *for that* drücken die enorme Innovationskraft, die wachsende Vielfalt und die damit verbundene Alltagsverankerung aus.

Mit dem *There's* drückt Apple eine grundlegende Voraussetzung für den hohen Diffusionsgrad von SMD im Massenmarkt und die starke Alltagsverankerung von Software im Leben von durchschnittlichen Nutzern aus. Die Plattformanbieter schaffen durch die Integration von externen Entwicklern eine massive Ausweitung ihres Wertangebots und ermöglichen es den Nutzern dadurch das SMD in seiner Funktionalität nahezu beliebig zu erweitern (Holzer & Ondrus, 2011). Durch die Bindung des großen Nutzerkreises entwickeln Drittanbieter unablässig neue Wertangebote (*an app*) für die mobilen Ökosysteme. Die tiefgreifende Integration von Apps in den Alltag (*for that*) von Nutzern wird in erster Linie durch das Zusammenspiel der ersten beiden Faktoren erreicht. Durch die zentrale Plattformorganisation und die niederschwellige Nutzung des jeweiligen SDK stellen

die Ökosystemanbieter sicher, dass Apps von Nutzern für Nutzer entwickelt werden können. Hierdurch werden Nischenangebote zur Befriedigung der unterschiedlichsten individuellen Bedürfnisse einem breiten Massenmarkt angeboten.

2.3 Der Wertbeitrag des Nutzers in Informationssystemen

Durch die technische Umsetzung des *pervasive computing* ändert sich, im Rahmen des *experiential computing*, die Sichtweise auf den Wertbeitrag des Nutzers. Während der Nutzer in der klassischen Sichtweise auf Informationssysteme nur einen atomistischen Teilnehmer darstellt, der durch Bedienung des Systems eine klar definierte Aufgabe erfüllt, steht beim *experiential computing* der Nutzer selbst im Mittelpunkt.

Aufgrund Ihrer tiefgreifenden Integration in den Alltag und der Allgegenwärtigkeit ermöglichen moderne Informationssysteme ihren Nutzern Erfahrungen, die weit über die funktionellen und praktischen Anwendungen von betrieblich motivierten Informationssystemen hinausgehen (Sullivan et al., 2009). Die zugrundeliegende Technologie hält für die Nutzer eine Umgebung bereit, in der sie Inhalte, Erfahrungen, Kenntnisse und Fähigkeiten sowie Möglichkeiten und sogar Technologie selbst austauschen können (Sullivan et al., 2009). Dies verdeutlicht die veränderte Rolle, die Produkte und Dienstleistungen in Bezug auf Bedürfnisbefriedigung bei Nutzern einnehmen (Merli, 2013). Digitale Systeme sind, aufgrund ihrer Beschaffenheit der automatisierten Verwertung von Informationen, Nutzer-zentrierte Angebote und integrieren den Nutzer in die Erstellung des Wertangebots im Sinne einer Ko-Kreation. Durch die Preisgabe persönlicher Nutzer- und Nutzungsdaten ermöglichen eben diese erst das Wertangebot digitaler Services (Kessler & Buck, 2017; Mai, 2016).

Wie die klassische Sichtweise auf den Nutzer, muss im Rahmen des *experiential computing* auch die klassische Sichtweise auf Erstellung des Werts in digitalen Systemen und damit auf den Wertbeitrag des Nutzers angepasst werden. Klassische Ansätze vermögen die ko-kreierte Werterstellung in Nutzer-zentrierten Informationssystemen nicht zu erklären (Vargo et al., 2011). Eine neue Sichtweise auf den Nutzer wird seit der Einführung der *Service Dominant Logic* (SDL) diskutiert (Vargo & Lusch, 2004). Im Rahmen der SDL stellt der Austausch von Services (im Sinne von beispielsweise Fähigkeiten, Kompetenzen und Interessen) die Grundlage eines ökonomischen Austauschs dar. Die Perspektive impliziert, dass Wert immer

durch einen kollaborativen Prozess aller Beteiligten ko-kreiert wird (Lusch & Vargo, 2014). Demnach haben Nutzer unabdingbar einen maßgeblichen Anteil an der Werterstellung in Austauschsituationen, wie sie auch der Bezug und die Nutzung von Informationssystemen darstellen (Bettencourt et al., 2014).

Während die grundsätzliche Perspektive der SDL auf den Wertbeitrag von Nutzern als Basis der Betrachtung herangezogen werden kann, müssen deren Annahmen für die Betrachtung von Informationssystemen im Allgemeinen und mobilen Ökosystemen im Speziellen erweitert werden. Der Weitbeitrag der Nutzer in mobilen Ökosystemen, also die Datenpunkte, die sie im System hinterlassen, steht in direkter Verbindung mit ihrer Integration. Damit muss die *actor-to-actor*-Sichtweise, welche einen aktiven Austausch zwischen den verschiedenen Akteuren unterstellt, erweitert werden. Zwar erkennen Lusch und Vargo (2014), dass Nutzer ihre Rolle und ihren Wertbeitrag aufgrund der Komplexität des Austauschsystems nicht zwingend verstehen, doch unterstellt die *actor-to-actor*-Sichtweise einen aktiven Austausch (Lusch & Vargo, 2014).

So kann der Wertbeitrag der Nutzer durch zwei Dimensionen klassifiziert werden: Bewusstheitsgrad der Datenpreisgabe und Aktivitätslevel der Datenpreisgabe. Die beiden Dimensionen stellen jeweils ein Kontinuum dar, welches mit zwei Extrempunkten beschrieben werden kann. Abhängig vom Nutzungskontext kann der Wertbeitrag der Nutzer durch die beiden Dimensionen klassifiziert werden. Der Bewusstseinsgrad der Datenpreisgabe kann durch die beiden Extrempunkte *bewusst* und *unbewusst* dargestellt werden. Das Aktivitätslevel der Datenpreisgabe kann durch die Extrempunkte *aktiv* und *passiv* dargestellt werden. Die Aufnahme und Verarbeitung der Nutzungsdaten zur Verbesserung von digitalen Services kann beispielsweise als passiv und unbewusst eingestuft werden. Das Freischalten des Standorts durch den Nutzer für die Befriedigung eines unmittelbaren Bedürfnisses (beispielsweise das Auffinden eines Bankautomaten) kann als aktiv und bewusst klassifiziert werden.[5]

[5] Die Klassifikation stellt ein Meta-Level auf der Ebene der direkten Verwendung der Daten dar. Die Weiterverwertung der Daten (beispielsweise im Sinne des *secondary use*) wird in dieser Betrachtung nicht berücksichtigt.

3 Privatheit und Informationssysteme

3.1 Informationelle Privatheit

Da Privatheit (*privacy*) viele Bereiche des menschlichen Lebens umfasst, in zahlreichen Disziplinen Verwendung findet und damit einen Sammelbegriff darstellt (Solove, 2006), muss der Begriff für die Betrachtung im Rahmen der Nutzung von Informationssystemen genauer bestimmt und definiert werden.[6]

In der Literatur ist Privatheit nicht einheitlich definiert und wird häufig in Bezug auf den jeweiligen Untersuchungsgegenstand nicht exakt abgegrenzt (Smith et al., 2011; Solove, 2006). Unter dem Überbegriff der Privatheit werden unterschiedliche Teilbereiche subsumiert. Smith et al. (2011) unterteilen Privatheit in physische Privatheit und informationelle Privatheit, Rössler (2001) beschreibt für „das Private" zwei semantische, quer zueinander liegende Modelle (Rössler, 2001, S. 18). Während das Eine den (räumlichen) Bereich des Privaten beschreibt, adressiert das Andere die Handlungs- und Verantwortungsdimensionen des Privaten sowie Dimensionen von Interesse und Betroffenheit (Rössler, 2001, S. 18). Unter dem bestehenden Sammelbegriff leitet Rössler (2001) drei Dimensionen der Privatheit ab: Dezisionale, lokale und informationelle Privatheit.

Aufgrund des betrachteten Untersuchungsgegenstands von Informationssystemen konzentriert sich die vorliegende Ausarbeitung auf die Dimension der informationellen Privatheit. Die Perspektive auf und die Definition von informationeller Privatheit steht in direktem Zusammenhang mit der Entwicklung von Informationssystemen (Dinev & Hart, 2006; Krasnova & Kift, 2012; Nissenbaum, 2010). Die Entwicklung des Begriffs kann demnach an fünf Epochen der Privatheit, in Abhängigkeit der technologischen Entwicklung, beobachtet werden. Die fünf Epochen und deren Einflüsse auf den Privatheitsbegriff sind in Tabelle 1 dargestellt.

Die sogenannte *privacy baseline* wird von Westin (2003) durch die Nachkriegszeit des zweiten Weltkriegs (1945 bis 1960) beschrieben (Westin, 2003). Aufgrund von hohem Vertrauen in Politik und Wirtschaft und fehlenden Technologiesprüngen in der Informations- und Kommunikationstechnologie, stellte informationelle Privatheit in

[6] Im Folgenden werden die Begrifflichkeiten Privatheit, Privatsphäre und Privacy synonym verwendet Geminn and Roßnagel (2015).

dieser Zeit kein öffentlich diskutiertes Thema dar und fand auch im Bereich der Rechtsprechung wenig Aufmerksamkeit (Geminn & Roßnagel, 2015; Smith et al., 2011; Westin, 2003).[7]

Tabelle 1. Einflüsse auf die Entwicklung des Privatheitsbegriffs (Smith et al., 2011; Westin, 2003).

Epoche	**Einflüsse auf den Begriff der informationellen Privatheit**
Privacy Baseline	Nur wenige, für die Nutzer spürbare, Entwicklungen in der Informationstechnologie; hohes Vertrauen in den öffentlichen Sektor und die Wirtschaft
Erste Epoche	Bekanntwerden von potentiellen Schattenseiten von Informationssystemen; öffentlicher Diskurs bezüglich informationeller Privatsphäre; erste regulatorische Maßnahmen
Zweite Epoche	Aufkommen des Personal Computer; Entstehung weitreichender Netzwerksysteme; rapide Entwicklungen in der Informations- und Kommunikationstechnologie; Entwicklung weitführender regulatorischer Maßnahmen
Dritte Epoche	Entwicklung und flächendeckende Verbreitung des Internet; Entwicklung von Web 2.0-Anwendungen; Veränderung der öffentlichen Überwachung aufgrund der Terrorangriffe des 11. September; starke Zunahme von Privatheitsbedenken
Vierte Epoche	Entwicklung und Massentauglichkeit von SMD; Software in Form von Apps; *Pervasive computing* und explosionsartige Vernetzung von Sensoren und smarten Geräten; zunehmende Verbreitung von beispielsweise sozialen Netzwerken und Plattformökonomien; zunehmende Terrorattacken und politische Umwälzungen; starke Zunahme der Missbrauchstatbestände hinsichtlich der informationellen Privatheit; weitere Zunahme der Privatheitsbedenken

Durch die Entwicklung von ersten High-Tech-Anwendungen wurde informationelle Privatheit in der Zeit zwischen 1961 und 1979 ein ausdrückliches soziales, politisches

[7] Aus deutscher Perspektive ist anzumerken, dass weder im Grundgesetz, noch im Herrenchiemseer Entwurf von 1948 die Begriffe Privatheit oder Privatsphäre Erwähnung finden Geminn and Roßnagel (2015).

und rechtliches Thema. Potentielle Schattenseiten von Technologie wurden von der Gesellschaft kritisch hinterfragt und führten zu ersten Berücksichtigungen in der Gesetzgebung (Geminn & Roßnagel, 2015; Westin, 2003). Die zweite Epoche der Privatheit (1980 bis 1989) wurde geprägt durch den Einsatz des *Personal Computer*. Der *Personal Computer* erweiterte private Haushalte mit komplexen Informationssystemen, welche in der Regel noch unvernetzt blieben (*stand alone*). Die dritte Epoche der Privatheit (1990 bis 2006) kann beschrieben werden anhand der weltweit vernetzten Kommunikationstechnologie. Durch das Internet konnten sich Nutzer durch Informationssysteme weltweit vernetzen, wodurch sich neue Formen der Kommunikation und des Informationsaustausches entwickelten.[8] Eine vierte Epoche der informationellen Privatheit kann durch die Entwicklung des *pervasive computing* und der damit verbundenen Perspektive des *experiential computing* gesehen werden. Durch sensor- und prozessorgestützte Umgebungen können Nutzer ihre Fähigkeiten und Möglichkeiten erweitern. Dies führt zu einer massiven Ausweitung der Möglichkeiten der Aufnahme, Verarbeitung und Speicherung von persönlichen Informationen.

In Anbetracht der historischen Entwicklung von Informationstechnologie und Informationssystemen, haben sich unterschiedliche definitorische Perspektiven auf den Begriff der informationellen Privatheit entwickelt.[9]

Eine grundsätzliche Diskussion wird in der Perspektive auf Privatheit als ein menschliches Grundrecht geführt. Hierauf stützt sich eine der bekanntesten Privatheitsdefinitionen von Warren und Brandeis (1890), die in ihrem 1890 im Harvard Law Review erschienenen Artikel Privatheit mit „the right to be let alone" definieren (Warren & Brandeis, 1890, S. 193). Wenngleich die Diskussion von Privatheit als menschliches Grundrecht einen philosophischen Ursprung in sich trägt, führte die gesellschaftliche Diskussion zur Verankerung von Privatheit in der weltweiten Rechtsprechung (Geminn & Roßnagel, 2015; Schmidt-Kessel & Grimm,

8 Neben der Entwicklung von Informations- und Kommunikationstechnologien haben politische Systeme und gesellschaftliche Umwälzungen und externe Schocks wie beispielsweise Terrorattacken Einfluss auf die Entwicklung der Privatheitsperspektive genommen Westin (2003); Smith et al. (2011); Geminn and Roßnagel (2015).

9 Smith et al. (2011) unterscheiden *Value-Based Definitions* und *Cognate-Based Definitions* Smith et al. (2011, S. 994–995).

2017; Smith et al., 2011).[10] Der gesellschaftliche Diskurs über Privatheit als menschliches Grundrecht wurde durch zwei konträre Ansichten darüber genährt, wer Privatheit zu garantieren hat (Hotter, 2011). Für Vertreter von Privatheit als menschlichem Grundrecht muss der Staat Privatheit sicherstellen, während sich die liberale Ansicht für eine marktwirtschaftliche Perspektive ausspricht, nach der sich Privatheit zu einem handelbaren Gut entwickelt hat (Bennett, 1995).

Mit der Perspektive auf Privatheit als Zustand führen Westin (1968) und Altman (1975) eine Sichtweise ein, welche auf den individuellen und situativen Kontext des Nutzers abstellt (Westin, 2003). Hierbei wird Privatheit in Beziehung zu anderen Individuen betrachtet und als ein Zustand des „limited access to a person" bezeichnet (Schoeman, 1984, S. 199). Vor dem Hintergrund der Durchdringung der Gesellschaft mit Informationssystemen wird informationelle Privatsphäre als „state of limited access to information" definiert (Smith et al., 2011, S. 995). Mit den wechselnden Bedürfnisse, Präferenzen und Situationen in denen sich Nutzer bewegen, ergibt sich ein Kontinuum an Zuständen von absoluter bis hin zu minimaler Privatheit (Schoeman, 1984; Smith et al., 2011).

Immer deutlicher kristallisiert sich im wissenschaftlichen Diskurs die kontroll-basierte Definition von Privatheit heraus (Altman, 1975; Margulis, 1977; Smith et al., 1996; Westin, 1968). Margulis (1977) definiert Privatheit „... as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which ist to enhance autonomy and/or to minimize vulnerability." (Margulis, 1977, S. 10). Während klassische kontroll-basierte Perspektiven Privatheit mit Kontrolle gleichsetzen, entwickeln sich zunehmend Definitionsansätze, die Privatheit mit der Möglichkeit zur Kontrolle definieren. Laut Rössler (2001) gilt als privat dann etwas, „... wenn man selbst den Zugang zu diesem »etwas« kontrollieren kann." (Rössler, 2001, S. 24).

Für die Definition von informationeller Privatheit können die marktwirtschaftliche Sichtweise und der kontroll-basierte Definitionsansatz von Privatheit zusammengeführt werden. Informationelle Privatheit hat sich zu einer Handelsware entwickelt (Bennett, 1995; Campbell & Carlson, 2002), welche in Informationssystemen durch den Nutzer kontrolliert werden kann. Diese Perspektive

[10] Trotz allem finden sich die Begriffe Privatsphäre, Privatheit oder *Privacy* nicht in der Gesetzgebung Smith et al. (2011); Geminn and Roßnagel (2015); Schmidt-Kessel and Grimm (2017).

wird gestützt durch die Entwicklung des *self-surveillance* (Smith et al., 2011), nach welchem Nutzer persönliche Informationen in Informationssystemen freiwillig preisgeben. Das Konzept der selbstbestimmten und eigenverantwortlichen Kontrolle über die Preisgabe von persönlichen Informationen steht in engem Zusammenhang mit der Entwicklung von Informationstechnologie und Informationssystemen (Dinev & Hart, 2006). Mit der Weiterentwicklung und Erweiterung von Informationssystemen steigt zunehmend die Aufnahme, Verarbeitung und Speicherung persönlicher Informationen.[11]

In Anbetracht der Wirkungsweise des *experiential computing* wird informationelle Privatheit definiert als „… individuelle[r] Anspruch, den Zugriff Dritter auf personenbezogene Daten zu beschränken, wobei dieser Anspruch im Rahmen einer vertraglichen Vereinbarung frei ausgestaltet werden kann, so dass das Recht auf Privatsphäre verwirkbar ist." (Hotter, 2011)

Der Privatheitsklassifikation von Clarke (1999) folgend wird für die vorliegende Ausarbeitung, aufgrund der Beschaffenheit von Informationssystemen, informationelle Privatheit mit *data privacy* gleichgesetzt (Bélanger & Crossler, 2011; Clarke, 1999; Malhotra et al., 2004). In Informationssystemen, im Speziellen SMD und Apps, geben Nutzer ihre persönlichen Daten für den Bezug einer digitalen Dienstleistung oder eines digitalen Produkts frei. Demnach werden persönliche Daten und deren Preisgabe mit informationeller Privatheit gleichgesetzt.[12]

Somit kann der Schutz der informationellen Privatheit als Schutz vor unerwünschtem Zutritt gesehen werden – auch und gerade im Sinne des unerwünschten Zugriffs auf persönliche Daten. Von einer derartigen informationellen Privatheit wird dann gesprochen, „… wenn Personen den Anspruch haben, vor unerwünschtem Zugang im Sinne eines Eingriffs in persönliche Daten über sich geschützt zu werden, also vor dem Zugang zu Informationen über sie, die sie gerade nicht in den falschen Händen sehen

[11] Für die vorliegende Ausarbeitung werden die Begrifflichkeiten persönliche Informationen und persönliche Daten synonym verwendet.

[12] Laut der EU-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr werden persönliche oder personenbezogene Daten definiert als „… alle Informationen über eine bestimmte oder bestimmbare natürliche Person; als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen." (Richtline 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr).

wollen.“ (Rössler, 2001, S. 25). Dies trifft auf Nutzer von SMD und Apps im Besonderen zu, da sie die Einschränkung ihrer Privatheit vollständig kontrollieren können. So sind sie in der Lage die Preisgabe persönlicher Informationen und deren Aufnahme durch Dritte aktiv zu steuern und nicht erwünschte Services und Apps nicht zu beziehen.[13]

3.2 Informationelle Privatheitsbedenken in Informationssystemen

Mit der zunehmenden Durchdringung des Alltags mit Informationssystemen steigen auch die Bedenken der Nutzer bezüglich ihrer informationellen Privatheit (*privacy concerns*) (Dinev et al., 2015; Kokolakis, 2017; Li, 2011; Smith et al., 2011). Privatheit selbst basiert auf Erkenntnissen, Wahrnehmungen und Erfahrungen und kann nicht rational erfasst werden (Smith et al., 2011). Die Messung von Privatheit stellt sich somit als nur schwerlich operationalisierbar dar.

Privatheitsbedenken haben sich in der Forschungsdomäne der IS als zentraler Untersuchungsgegenstand und als weithin anerkanntes Proxy für Privatheit etabliert (Li, 2011; Smith et al., 2011).[14] Aufgrund der breiten Anwendung der Bedenken haben sich im wissenschaftlichen Diskurs unterschiedliche Perspektiven und Definitionen von Privatheitsbedenken entwickelt. Grundlegend definiert werden können sie als Bedenken der Nutzer bezüglich eines möglichen zukünftigen Verlustes der Privatheit als Folge von freiwilliger oder unfreiwilliger Preisgabe von persönlichen Daten (Dinev & Hart, 2006). Diesem definitorischen Ansatz schließt sich eine weiter gefasste Definition von Privatheit an, nach welcher Privatheit als die subjektive Ansicht von Nutzern bezüglich der Fairness im Umgang mit persönlichen Daten definiert wird (Malhotra et al., 2004). Eine engere Definition von Privatheitsbedenken verwenden zahlreiche Forscher und definieren diese als Bedenken, die Nutzer gegenüber dem Umgang von Unternehmen und Organisationen mit persönlichen Daten haben (Smith et al., 1996).

Im Rahmen der empirischen Forschung werden überwiegend drei Konstrukte für

[13] Smith et al. (2011) grenzen darüber hinaus informationelle Privatheit ab von den vier Strategien des Identitätsmanagements: Anonymität, Transparenz, Geheimhaltung und Vertraulichkeit Smith et al. (2011).

[14] Teilweise werden Privatheitsbedenken als Einstellungen, Wahrnehmungen oder Ansichten benannt Bélanger and Crossler (2011); Smith et al. (2011).

Privatheitsbedenken verwendet. Der *Concern for Information Privacy* (CFIP) stellt das als erstes entwickelte und überprüfte Konstrukt zur Messung von informationeller Privatheit dar (Smith et al., 1996; Stewart & Segars, 2002). Mit dem *Internet Users' Information Privacy Concerns* (IUIPC) wurde ein weiteres Messinstrument für Privatheitsbedenken entwickelt, welches versucht, spezifischer auf die technologischen Gegebenheiten des Internet einzugehen (Malhotra et al., 2004). Mit dem *Mobile Users' Information Privacy Concerns* (MUIPC) wurde ein Konstrukt entwickelt, welches den Kontext und die Besonderheiten von Privatheitsbedenken im Rahmen mobiler Systeme berücksichtigt (Xu et al., 2012). Da der IUIPC und der MUIPC auf dem grundlegenden Konstrukt des CFIP aufbauen, weisen die Messinstrumente einen hohen Grad an Überschneidung auf (Buck & Burster, 2017). Tabelle 2 stellt die drei Konstrukte exemplarisch gegenüber. Aufgrund der hohen Kontextabhängigkeit von Privatheitsbedenken wurde von Buck und Burster (2017), aufbauend auf den drei Konstrukten CFIP, IUIPC und MUIPC, ein Messinstrument für die Privatheitsbedenken hinsichtlich Apps entwickelt (Buck & Burster, 2017).[15]

[15] Das entwickelte Messinstrument wird im Rahmen des Forschungsbeitrags in Kapitel 4.4.1 gesondert vorgestellt.

Tabelle 2. Übersicht über Messinstrumente für Privatheitsbedenken (in Anlehnung an Buck & Burster, 2017; Xu et al., 2012).

Privatheitsbedenken			
	CFIP	**IUIPC**	**MUIPC**
Gegenstand	Privatheits-bedenken von Individuen hinsichtlich des Umgangs von Organisationen mit Privatheit und persönlichen Daten	Privatheits-bedenken von Internetnutzern	Privatheits-bedenken von Anwendern mobiler Systeme
Fokus	Verantwortung von Organisationen für den angemessenen Umgang mit persönlichen Daten	Subjektive Perspektive der Nutzer hinsichtlich der Fairness im Bereich informationeller Privatheit	Das Gefühl der Nutzer hinsichtlich der Datenhoheit von Dritten über persönliche Daten
Dimensionen	• Sammlung • Nicht autorisierte Weitergabe • Fehler • Unerlaubter Zugang	• Sammlung • Kontrolle • Bewusstsein für den Umgang mit Privatheit	• Wahr-genommene Überwachung • Wahr-genommenes Eindringen • Datenweitergabe
Anzahl der Items	15	10	9
Autoren	(Smith et al., 1996)	(Malhotra et al., 2004)	(Xu et al., 2012)

3.3 Informationelle Privatheit als Teil einer ökonomischen Austauschbeziehung

Die besondere Relevanz von informationeller Privatheit bei SMD und Apps als Informationssystem entsteht aus dem in Kapitel 2.3 beschriebenen Wertbeitrag des Nutzers im Rahmen des *experiential computing*“ (Ackerman, 2004).

Von entscheidender Bedeutung ist Privatheit nach Müller et al. (2012) dann, „… wenn sie auf das Marktverhalten Einfluss nimmt, zum Beispiel wenn im Vertrauen auf die Erfüllung eines Privatheitsversprechens ein Kauf getätigt oder abgelehnt wird.“ (Müller et al., 2012, S. 144). In der einzelwirtschaftlichen Betrachtung, also der Austauschsituation zwischen Nutzer und App-Anbieter, kann Privatheit als eigenständige Produkteigenschaft angesehen werden, welche einen wirtschaftlichen

Wert darstellt (Buck, Stadler et al., 2017; Müller et al., 2012). Beim Bezug von Apps tauscht der Nutzer oftmals die Preisgabe seiner persönlichen Daten gegen den Bezug des Dienstes beziehungsweise des Service.

In mobilen Ökosystemen ist das Bezahlen mit persönlichen Daten eine *Binsenweisheit* (Schmidt-Kessel & Grimm, 2017, S. 84). Mit der Definition von persönlichen Daten als eigenständige Güterklasse folgt das Weltwirtschaftsforum der Sichtweise zahlreicher Wissenschaftler (Schwab et al., 2011), die durch die Kommodifizierung von Privatheit persönliche Daten als handelbares Gut betrachten (Bennett, 1995; Spiekermann-Hoff et al., 2015). Dies führt dazu, dass Privatheit nicht mehr als absoluter gesellschaftlicher Wert, sondern als Teil einer individuellen oder gesellschaftlichen Kosten-Nutzen-Abwägung angesehen wird (Mai, 2016; Spiekermann & Korunovska, 2017).

Diese Kosten-Nutzen-Abwägung wird in der Literatur durch das Privatheitskalkül (*privacy calculus*) beschrieben (Culnan & Armstrong, 1999; Dinev & Hart, 2006; Stone & Stone, 1990). Nutzer wägen demzufolge Risiken der Preisgabe persönlicher Daten mit deren ökonomischen oder sozialen Vorteilen ab und entscheiden sich entsprechend ihrer Präferenzen. In Einklang mit der Sichtweise des neoklassischen *Homo Oeconomicus* nehmen Nutzer im Rahmen der Entscheidungsfindung für den Download oder Bezug einer digitalen Dienstleistung oder eines digitalen Gutes diese rationale Abwägung vor (Culnan & Armstrong, 1999; Dinev & Hart, 2006; Stone & Stone, 1990). Das Privatheitskalkül unterstellt den Nutzern demnach in der Entscheidungssituation eine rationale Abwägung der Kontrolle der Privatheit und damit die Fähigkeit der objektiven Bewertung der Datenpreisgabe und deren Folgen.

Um persönliche Daten in mobilen Ökosystemen bewerten zu können, müssen die unterschiedlichen Verwendungs- und Entstehungsebenen sowie Verwertungsszenarien berücksichtigt werden. Daten aus mobilen Ökosystemen weisen, bedingt durch den Aufbau des IT-Systems, eine sehr hohe Datengüte auf (Buck, Horbel, Kessler et al., 2014). Der daraus entspringende hohe Wert der Daten ist dadurch begründet, dass durch die Architektur des Informationssystems Herausforderungen des Big Data Managements beherrschbar gemacht wurden. Bereits bei der erstmaligen Nutzung des mobilen Endgeräts ist der Nutzer gezwungen, sich mit einem personalisierten und auf Richtigkeit verifizierten Profil anzumelden. Die hierbei preisgegebenen und fundamentalen Nutzerdaten werden der zukünftigen Nutzung zugrunde gelegt. Hierdurch wird die Datenvielfalt (*variety*) auf ein Profil

konzentriert und die Datengüte (*veracity*) grundlegend erhöht. Zudem wird durch die Anbindung der einzelnen Apps an das Nutzerprofil die Wertigkeit des Datensatzes durch einen erhöhten Vernetzungsgrad (*valence*) gesteigert.

Eine grundlegende Unterscheidung ist in Nutzerdaten und Nutzungsdaten vorzunehmen. Nutzerdaten stellen in mobilen Ökosystemen und plattformgetriebenen Systemen Profildaten und persönliche Daten dar, welche dem Nutzer eindeutig zuzuordnen sind. In mobilen Ökosystemen umfassen grundlegende Nutzerdaten beispielsweise Name, E-Mail-Adressen sowie Telefon- und Gerätenummern (Buck, Horbel, Kessler et al., 2014). Darüber hinaus können Nutzer- oder Profildaten retrospektiv durch Datenhistorien angereichert werden. Die Nutzungsdaten hingegen ergeben sich aus der Nutzung digitaler Services. Hierbei wird das Nutzungsverhalten festgehalten, welches sich über die Häufigkeit der Nutzung, die Nutzungszeiten, die Nutzungsvorlieben bis hin zu Kaufverhalten erstreckt (Mai, 2016).

Eine wichtige weitere Perspektive bei der Bewertung von persönlichen Daten stellt die Entstehungsebene der Daten und die damit verbundene Wertentwicklung dar. Apps sind sogenannte „datenzentrische Dienste“ (Müller et al., 2012, S. 146). Anbieter derartiger Dienste spalten den Kaufprozess in mehrere voneinander abhängige Teil-Transaktionen auf. Diese, in Abbildung 2 dargestellte, dreiwertige, verzögerte Transaktion macht die Geschäftsmodellvariante kostenloser digitaler Güter erst möglich. Es entsteht ein Wert zwischen Kunde und Anbieter und zwischen Anbieter und Datenaggregator, welcher die persönlichen Daten aggregiert und sie beispielsweise auf einem Sekundärmarkt weiter veräußern kann (Buck, Germelmann et al., 2016).

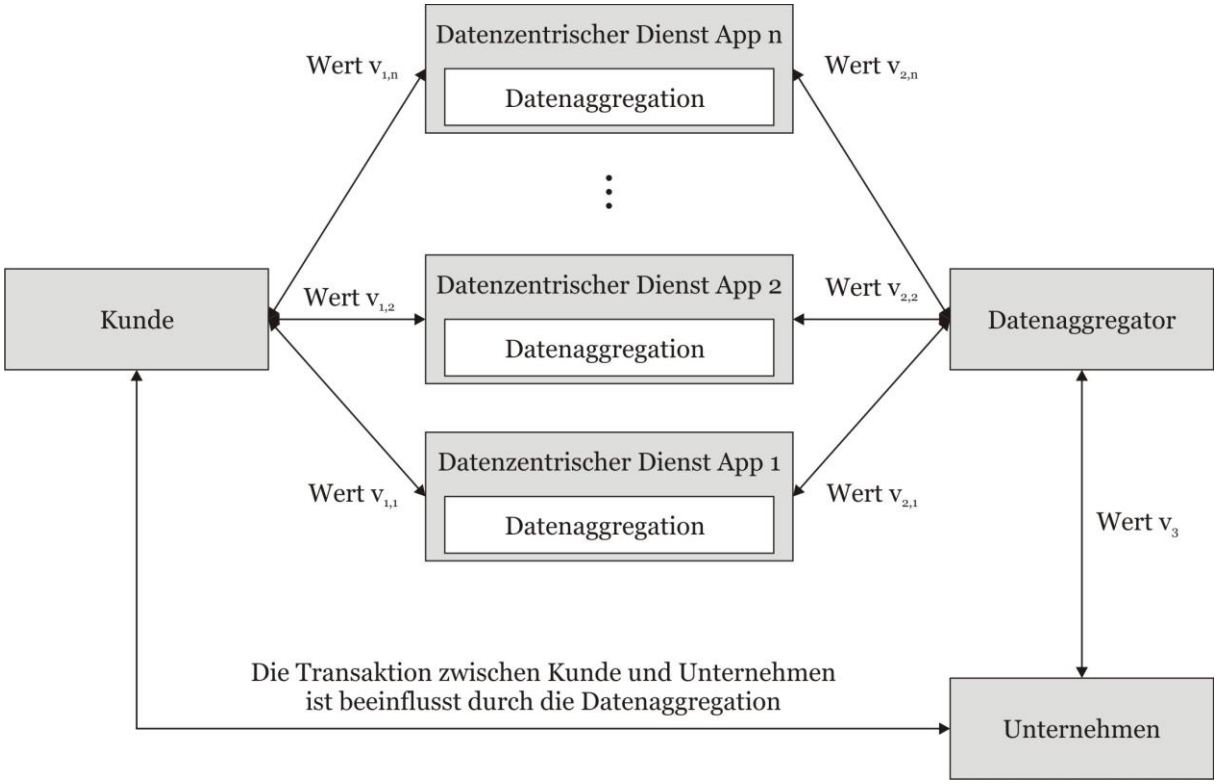

Abbildung 2. Dreiwertige, verzögerte Transaktion (Buck, Germelmann et al., 2016, S. 60).

Der Wert von, über mobile Ökosysteme erzeugten, Daten entsteht demnach an unterschiedlichen Stellen und ist somit auch situativ zu bewerten. Auf der ersten Wertebene entsteht der Wert der Nutzerdaten durch den direkten Austausch der persönlichen Daten gegen das digitale Gut. Diese Daten kann der Anbieter wiederum veräußern und damit auf der zweiten Wertebene eine Monetarisierung erwirken. Ebenso kann der Anbieter die Nutzungsdaten zur Verbesserung seiner Services verwenden. Hierbei tragen die Nutzer durch ihre Nutzung zur Weiterentwicklung des digitalen Gutes direkt bei. Die Verbesserung des Angebots steigert das Nutzererlebnis, bindet den Nutzer nachhaltig an das System und kann zu einer Ausweitung des Bezugs des bestehenden Leistungsangebots führen. Der Anbieter nutzt dementsprechend seine Nutzer zu Marktforschungs- und Entwicklungszwecken. Darüber hinaus entsteht der Wert aus persönlichen Daten auf der Ebene der Datenaggregatoren. Aufgrund der Aggregation der Datensätze von hochgradig fragmentierten Anwendungen können ganzheitliche Nutzerprofile erstellt werden.

Die neoklassische Sichtweise des Privatheitskalküls unterstellt den Nutzern eine rationale Abwägung zwischen Mehrwert und Risiken bei der Preisgabe persönlicher Daten. Im Rahmen der Entscheidungen in mobilen Ökosystemen muss das

Privatheitskalkül in seiner klassischen Form jedoch in Frage gestellt werden, da die Nutzer faktisch nicht in der Lage sind, den Wert ihrer Daten bestimmen zu können. Aufgrund der zu komplexen Struktur der Entstehungs- und Verwertungsebenen können potentielle Folgen aus der Preisgabe der persönlichen Daten von Nutzern nicht abgeschätzt werden. Risiken bei der Preisgabe persönlicher Daten werden definiert durch den vom Nutzer empfunden Grad an potentiellen Einbußen, die durch die Preisgabe der Daten entstehen (Malhotra et al., 2004). Dinev und Hart (2006) zeigen einen negativen Zusammenhang zwischen Privatheitsrisiken und der Preisgabe persönlicher Daten auf (Dinev & Hart, 2006). Da Nutzer die Risiken in Abhängigkeit der Eintrittswahrscheinlichkeit von Konsequenzen aus der Preisgabe persönlicher Daten ableiten (Peter & Tarpey, Sr., Lawrence X., 1975), muss das Risikoempfinden bei Entscheidungen in mobilen Ökosystemen hinterfragt werden.

Beschreibend für das Paradigma des *experiential computing* ist somit dessen *personal data paradox*. Je intimer die durch moderne Informationssysteme aufgenommenen, gespeicherten und verwendeten Daten, desto unsichtbarer und intransparenter ist das dahinterliegende Informationssystem für den Nutzer (Zhao & Wang, 2011). Das *personal privacy paradox* impliziert demnach bei mobilen Ökosystemen einen sehr hohen Grad an Informationsasymmetrien. Durch die zunehmende technologische Komplexität und eine immer alltäglichere Nutzung werden Informationssysteme derart selbstverständlich, „that we use it without even thinking about it." (Weiser, 1996). Die gegensätzlichen Entwicklungen der immer komplexer werdenden Systeme bei zunehmender Alltagsintegration führen dazu, dass Apps immer mehr als Erfahrungs- und Vertrauensgüter klassifiziert werden müssen (Buck, Dettweiler et al., 2014).

3.4 Das Privatheitsparadox in Informationssystemen

Die Sichtweise der neoklassischen Ökonomie des rational entscheidenden Nutzers wirft vor dem Hintergrund der Bezugssituation von Apps in mobilen Ökosystemen zahlreiche Fragen auf. Gemäß der ökonomischen Theorie geben Nutzer ihre Daten nicht preis, wenn sie sich davon keinen Mehrwert versprechen (Varian, 2009). Darüber hinaus kommt es bei Märkten mit hohen Informationsasymmetrien unweigerlich zu Marktversagen (Akerlof, 1970; Hirshleifer, 1973). Da die Entstehung des (monetären) Werts von persönlichen Daten in mobilen Ökosystemen vielschichtig

ist und in der Bezugssituation vom Nutzer nicht bewertet werden kann, muss das in der Literatur oft isoliert untersuchte Privatheitskalkül kritisch hinterfragt werden. Ebenfalls zeigen die wachsenden Anwender- und Bezugszahlen von Apps, dass mobile Ökosysteme weit von klassischem Marktversagen entfernt sind.

In der Literatur wird dieses Phänomen des Nutzerverhaltens unter dem Privatheitsparadox (*privacy paradox*) subsumiert.[16] Unter dem Privatheitsparadox versteht die Literatur das widersprüchliche Verhalten der Nutzer bezüglich der Preisgabe ihrer persönlichen Daten. Varian (2009) beschreibt das Paradox (ohne es derart zu nennen) in seiner Arbeit mit dem Titel „Economic Aspects of Personal Privacy" (Varian, 2009). Gemäß des Paradox artikulieren Nutzer hohe Privatheitsbedenken und beabsichtigen keine Services zu beziehen, die ihre Privatheit verletzen könnten, verhalten sich jedoch in entgegengesetzter Art und Weise (Acquisti & Grossklags, 2005; Norberg et al., 2007). Demnach weisen Nutzer eine hohe Aufmerksamkeit bezüglich Datenmissbrauch auf, ändern ihr Verhalten hinsichtlich Datenweitergabe und potentiellem Missbrauch jedoch nicht mehrheitlich (Acquisti & Grossklags, 2003). Ein theoriebegründetes und einheitliches Modell zur Erklärung der durch das Privatheitsparadox beschriebenen Dichotomie fehlt bislang (Kokolakis, 2017).

Im Rahmen eines strukturierten Literaturüberblicks konnte Kokolakis (2017) 51 für das Privatheitsparadox relevante Artikel analysieren. So hinterlässt die bestehende Dichotomie zwischen den vorhandenen Privatheitseinstellungen und dem Privatheitsverhalten Zweifel an den Annahmen der neoklassischen ökonomischen Theorie. Unterschiedliche Forschungsrichtungen versuchen die vermeintliche Gegensätzlichkeit zu erklären. Hierbei konnte Kokolakis (2017) fünf Forschungsfelder identifizieren: die Theorie des Privatheitskalküls, die Soziallehre, kognitive Verzerrungen und Heuristiken, Entscheidungen unter eingeschränkter Rationalität und Informationsasymmetrien und die Quantentheorie (Kokolakis, 2017).

3.5 Makromodelle der Privatheitsforschung

Mit der rasanten Entwicklung der Informations- und Kommunikationstechnologien und der damit einhergehenden öffentlichen Diskussion der informationellen

[16] Analog zur Definition von informationeller Privatheit werden in der vorliegenden Ausarbeitung die Begrifflichkeiten *privacy paradox* und *information privacy paradox* als Synonyme verwendet.

Privatheit, hat auch der wissenschaftliche Diskurs über Fächergrenzen hinweg zugenommen. Seit Anfang der 1990er-Jahre (dritte Epoche der Privatheit) sind die Forschungsarbeiten auf dem Gebiet der informationellen Privatheit rasant gestiegen (Bélanger & Crossler, 2011; Li, 2011; Smith et al., 2011). Aufgrund des *experiential computing*, der steigenden Alltagsintegration von Informationssystemen und den zunehmenden Möglichkeiten der Aufnahme, Verarbeitung und Speicherung persönlicher Daten gewinnt die Privatheitsforschung weiterhin an Bedeutung (Smith et al., 2011). Als zentrale Arbeiten der neueren IS-getriebenen Privatheitsforschung gelten die Publikationen von Li (2011), Bélanger und Crossler (2011) und Smith et al. (2011). Alle drei Publikationen arbeiten bestehende Literatur anhand eines strukturierten Literaturüberblicks auf und leiten daraus übergreifende Forschungsmodelle ab.

In ihrer Arbeit zu „Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems“ untersuchen Bélanger und Crossler (2011) den aktuellen Stand der Forschung zur informationellen Privatheit und führen einen strukturierten Literaturüberblick mit anschließender Literaturanalyse durch (Bélanger & Crossler, 2011). Bélanger und Crossler (2011) nutzen für ihre Literaturanalyse die Theorie-Klassifikation von Gregor (2006) und passen diese auf den Forschungsgegenstand an (Gregor, 2006). In ihrer strukturierten Aufbereitung ordnen die Autoren die analysierte Literatur in fünf Theorietypen (Analyse, Erklärung, Prognose, Erklärung & Prognose, Design & Handlung) und fünf Themenfelder (Informations Privacy Concern, Information Privacy & E-Business Impacts, Information Privacy Attitudes, Information Privacy Practices, Information Privacy and Technologies) ein. Der Kategorisierung des Levels der Privatheit folgend wurde eine weitere Analyse durchgeführt. Smith et al. (2011) unterteilen Privatheit in die vier Level: Individuell, Gruppe, Organisational, Gesellschaftlich. Hier zeigen die Ergebnisse der Analyse von Bélanger und Crossler (2011) einen deutlichen Überhang zum individuellen Level.

Auf Basis der analysierten Literatur stellen Bélanger und Crossler (2011) das „Information Privacy Concern Multilevel Framework“ vor (Bélanger & Crossler, 2011). Im, in Abbildung 3 illustrierten, Framework zeigen Bélanger und Crossler (2011) die (unterstellten) Zusammenhänge zwischen den vier Privatheitslevel und möglichen externen Faktoren.

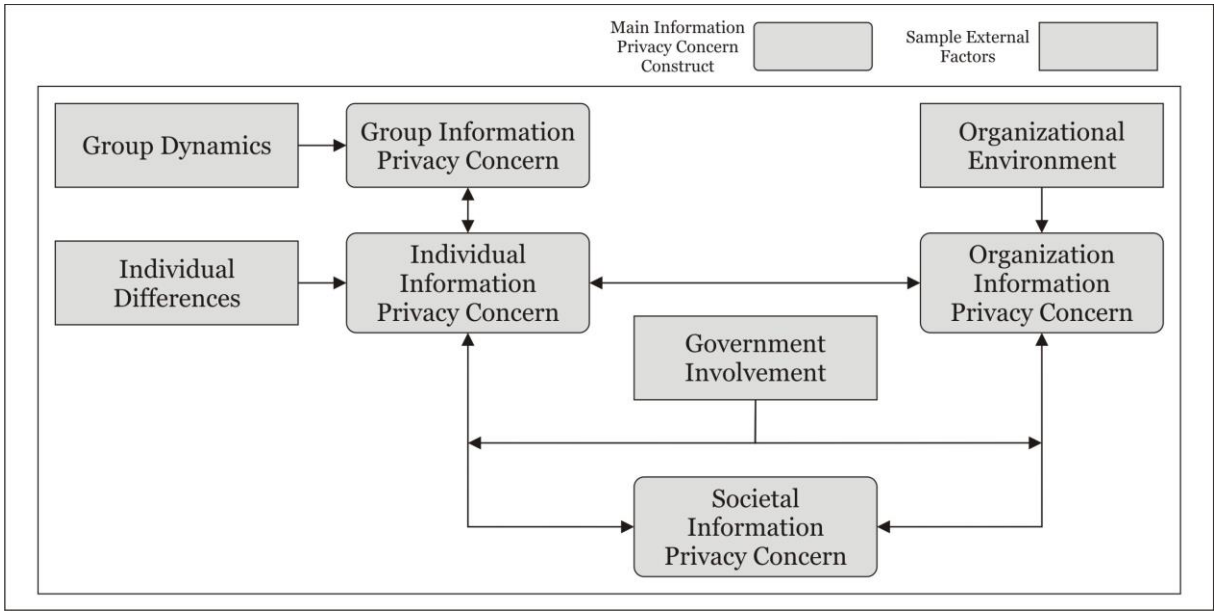

Abbildung 3. Information Privacy Concern Multilevel Framework (Bélanger & Crossler, 2011, S. 1032).

Die Arbeit von Bélanger und Crossler (2011) zeigt den aktuellen Stand der Privatheitsforschung und bestehende Forschungslücken auf und stellt ein Rahmenwerk für zukünftige Forschungsarbeiten bereit.

In seiner Arbeit „Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework“ führt Li (2011) einen strukturierten Literaturüberblick durch und stellt ein Rahmenwerk für zukünftige Privatheitsforschung zur Verfügung (Li, 2011). Der Literaturüberblick von Li (2011) untersucht Literatur, die das individuelle Privatheitslevel erforscht, verhaltensorientierte empirische Studien verwendet und sich als zentrale Konstrukte auf Privatheitsbedenken und verwandte Konstrukte konzentriert. Die Ergebnisse der Analyse konsolidiert Li (2011) in seinem „Integrative Framework for the Study on CFIP“ (Li, 2011).

Als zentrale Konstrukte definiert Li (2011) den *General CFIP* und den *Specific CFIP*. Während der *General CFIP* die allgemeinen Privatheitsbedenken des Nutzers (im Kontext E-Commerce) widerspiegelt, betrachtet der *Specific CFIP* die individuellen Privatheitsbedenken eines Nutzers in einer spezifischen Situation. Darüber hinaus identifiziert Li (2011) zahlreiche Faktoren, die vorwiegend auf den *General CFIP* und den *Specific CFIP* wirken. In Abbildung 4 wird der „Integrative Framework for the Study on CFIP“ dargestellt (Li, 2011).

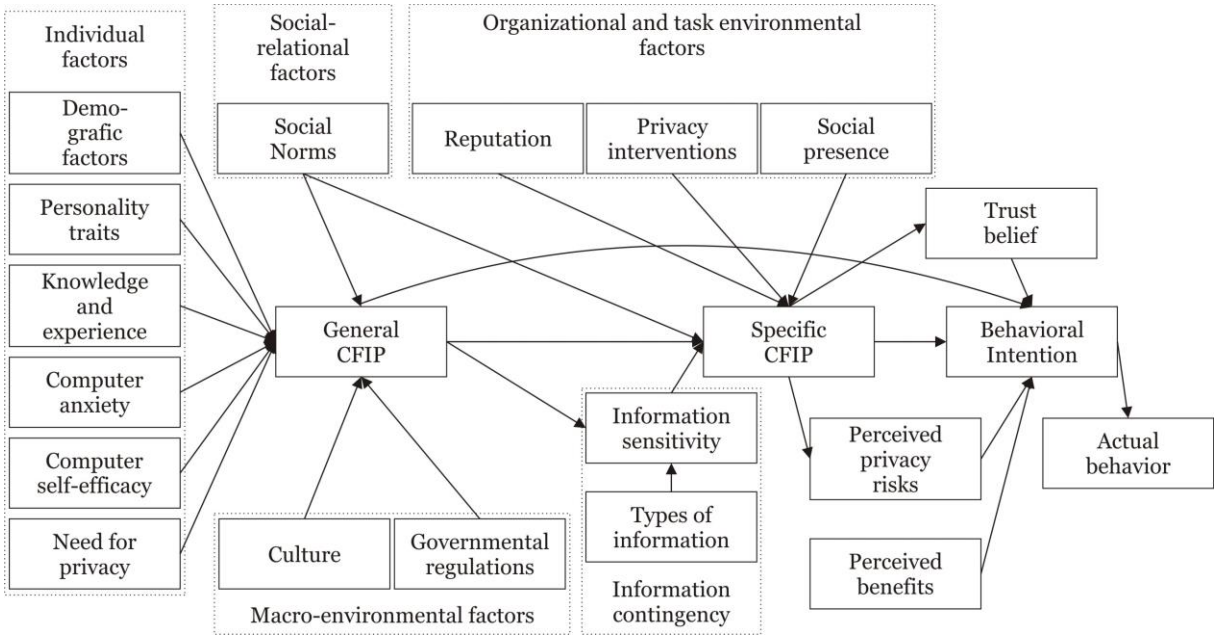

Abbildung 4. Integrative Framework for the Study on CFIP (Li, 2011, S. 466).

Die im wissenschaftlichen Diskurs meist beachtete Arbeit wurde von Smith et al. (2011) unter dem Titel „Information Privacy Research: An Interdisciplinary Review“ veröffentlicht (Smith et al., 2011). Der interdisziplinäre Literaturüberblick inkludiert 320 Forschungsbeiträge und stellt damit eine breite Datenbasis zur Verfügung. Als Ergebnis ihrer Literaturanalyse stellen die Autoren ein Makromodell der Privatheitsforschung zur Verfügung. Das sogenannte APCO-Modell unterteilt sich in drei Hauptkategorien: Die *Antecedents* (A), die *Privacy Concerns* (PC) und die *Outcomes* (O). Das APCO-Modell wird dargestellt in Abbildung 5.

Als zentrales und am meisten untersuchtes Konstrukt der Privatheitsforschung identifizieren Smith et al. (2011) die Privatheitsbedenken. Privatheitsbedenken werden in der Literatur sowohl als abhängige als auch als unabhängige Variable untersucht. Die Untersuchung von Privatheitsbedenken als abhängige Variable klassifizieren Smith et al. (2011) unter der übergeordneten Beziehung zwischen *Antecedents* und *Privacy Concerns* (A-PC). Unter *Antecedents* subsumieren Smith et al. (2011) Konstrukte, die Bedenken bezüglich der Privatheit beeinflussen. Hierunter sehen die Autoren Erfahrungen, Bewusstsein und Wahrnehmung, Persönlichkeit, Demografie und Kultur.

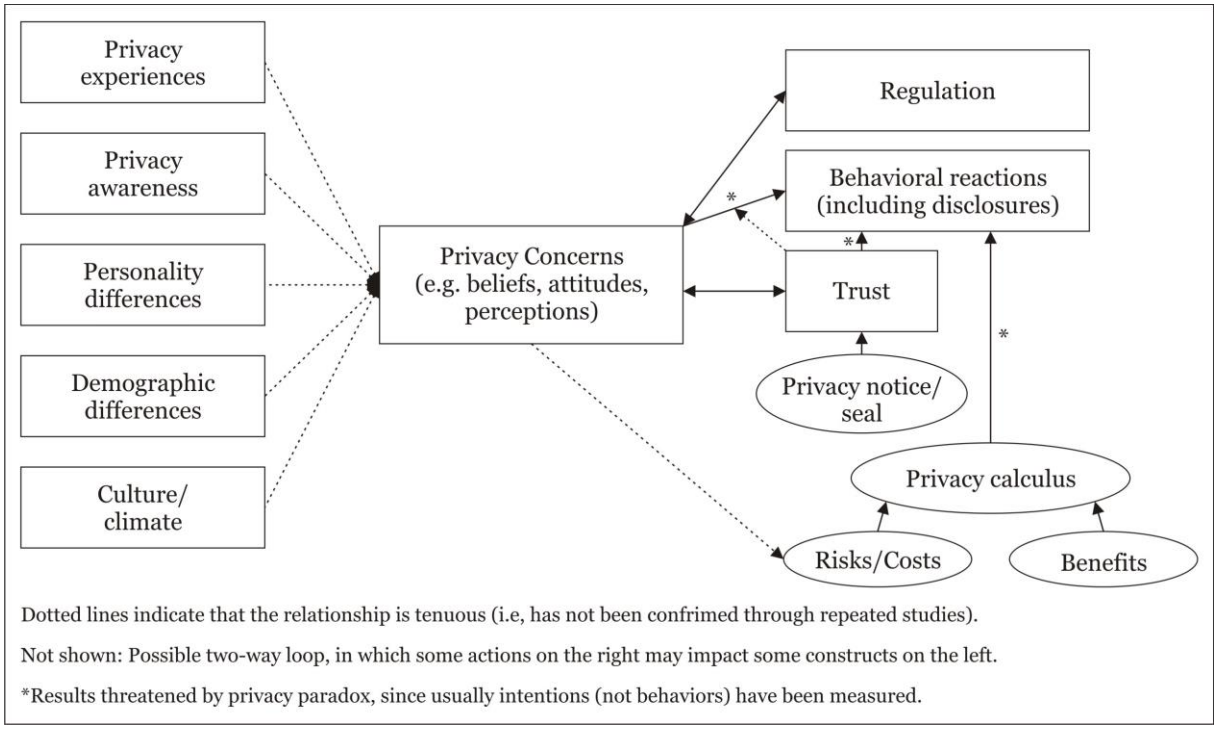

Abbildung 5. APCO Macro Model (Smith et al., 2011, S. 998).

Bei der Betrachtung von Privatheitsbedenken als unabhängige Variable werden die Auswirkung von Privatheitsbedenken auf nachgelagerte Konstrukte untersucht (PC-O).[17] Unter *Outcomes* verstehen Smith et al. (2011) Konstrukte wie beispielsweise Regulierung, Vertrauen, Risikoeinschätzung und Verhaltensreaktionen. Über die Kategorisierung A-PC-O hinaus leiten die Autoren die hohe Kontextabhängigkeit von Privatheit aus zahlreichen Forschungsarbeiten ab.

Dinev et al. (2015) äußern die allgemeine Kritik an den drei Makromodellen, und am APCO-Modell im Speziellen, dass individuelle Kontextvariablen der Entscheidungssituation der Individuen keine oder nur eine untergeordnete Rolle spielen (Dinev et al., 2015).[18] Im von Dinev et al. (2015) vorgestellten *enhanced APCO-Model*, dargestellt in Abbildung 6, führen die Autoren das *level of effort* als moderierende Variable (M1) der APCO-Beziehungen ein, welches durch Faktoren wie beispielsweise Affekt, Motivationen und zeitliche Restriktionen beeinflusst wird (P1-P4) (Dinev et al., 2015). Hierbei betonen die Autoren den kontextuellen und situativen Einfluss auf Privatheitsentscheidungen von Individuen und bestehenden

[17] Zwischen Privacy Concerns (PC) und Outcomes (O) bestehen teilweise wechselseitige Beziehungen.

[18] Dinev et al. (2015) formulieren im Rahmen des erweiterten APCO-Modells unterschiedliche Thesen bezüglich der unterstellten Wirkungsbeziehungen (M1; P1-P4; D1-D8).

Forschungsergebnissen außerhalb des APCO-Modells, welche Einfluss auf die Konstrukte des APCO-Models haben können (D1-D8). Dinev et al. (2015) stellen mit dem erweiterten APCO-Modell ein anschlussfähiges Rahmenwerk für weitere Forschungsarbeiten bereit (Dinev et al., 2015).

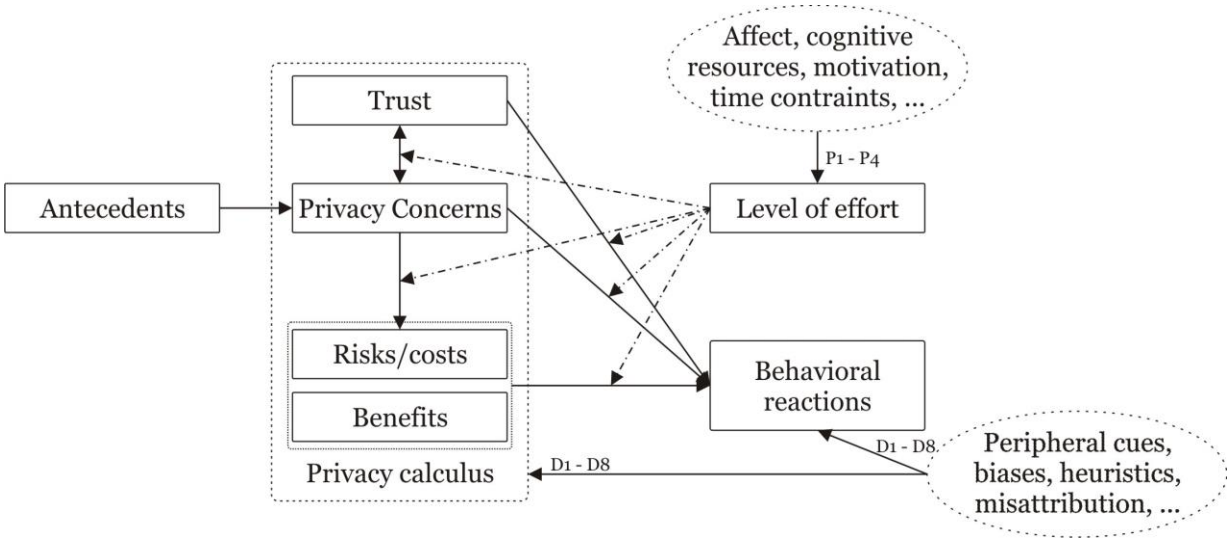

Abbildung 6. Enhanced APCO Model (Dinev et al., 2015, S. 643).

4 Privatheit und mobile Applikationen

4.1 Forschungsagenda

Mit der zunehmenden Alltagsintegration von Informationssystemen nehmen die Fragestellungen der Privatheitsforschung und deren Relevanz zu. Das Paradigma des *experiential computing* zeigt deutlich auf, dass Informationssysteme als soziotechnische Systeme begriffen werden müssen, in welchen die Nutzer als Teil des Systems einen festen Bestandteil einnehmen. Durch die alltägliche und selbstverständliche Integration des Informationssystems SMD und Apps partizipieren die Nutzer oft von hochkomplexen Softwaresystemen, ohne dies (bewusst) wahrzunehmen. Aufgrund des Wertbeitrags von Nutzern in Informationssystemen, in erster Linie durch das Beisteuern persönlicher Daten, entstehen zahlreiche Herausforderungen für die Privatheitsforschung (Dinev et al., 2015; Nissenbaum, 2010).

Der Fokus der vorliegenden Dissertation besteht darin, in verschiedenen Bereichen der Privatheitsforschung einen wissenschaftlichen Beitrag zu leisten. Die acht bereitgestellten Beiträge adressieren die Bereiche des Kontexts, des Werts und der Privatheitsbedenken, in denen im wissenschaftlichen Diskurs Forschungsbedarfe identifiziert wurden. Die Struktur der wissenschaftlichen Beiträge orientiert sich am APCO-Model und dessen jüngster Weiterentwicklung (Dinev et al., 2015; Smith et al., 2011). Dem Aufruf zahlreicher Forschungsbeiträge folgend, nimmt die Dissertation explizit die Perspektive der Nutzer von Informationssystemen ein (Dinev et al., 2015; Yoo, 2010). Abbildung 7 zeigt die Verortung der Publikationen im Rahmen des erweiterten APCO-Models (Dinev et al., 2015).[19][20]

In Unterkapitel 4.2 werden die ersten drei Publikationen (1-3) unter dem Titel *Der Kontext des Entscheidungsverhaltens beim Bezug mobiler Applikationen* zusammengefasst. Es werden wichtige kontextuale Gegebenheiten in mobilen Ökosystemen, Einflüsse auf die Wahrnehmung der Nutzer und deren Informations-

[19] Aufgrund der Vielschichtigkeit des Forschungsfelds der informationellen Privatheit kommt es zu zahlreichen Überschneidungen und Anknüpfungspunkten der acht Publikationen. Die Verortung der Publikationen dient der grundlegenden Orientierung.

[20] Die acht Beiträge werden jeweils durch eine Zusammenfassung und Informationen zur Publikation dargestellt. Die Forschungsbeiträge sind in vollem Umfang und originaler Formatierung im Anhang zu finden.

Such-Verhalten identifiziert. Dies kann sich, wie in Abbildung 7 dargestellt, auf sämtliche Elemente des zugrunde gelegten Modells auswirken.

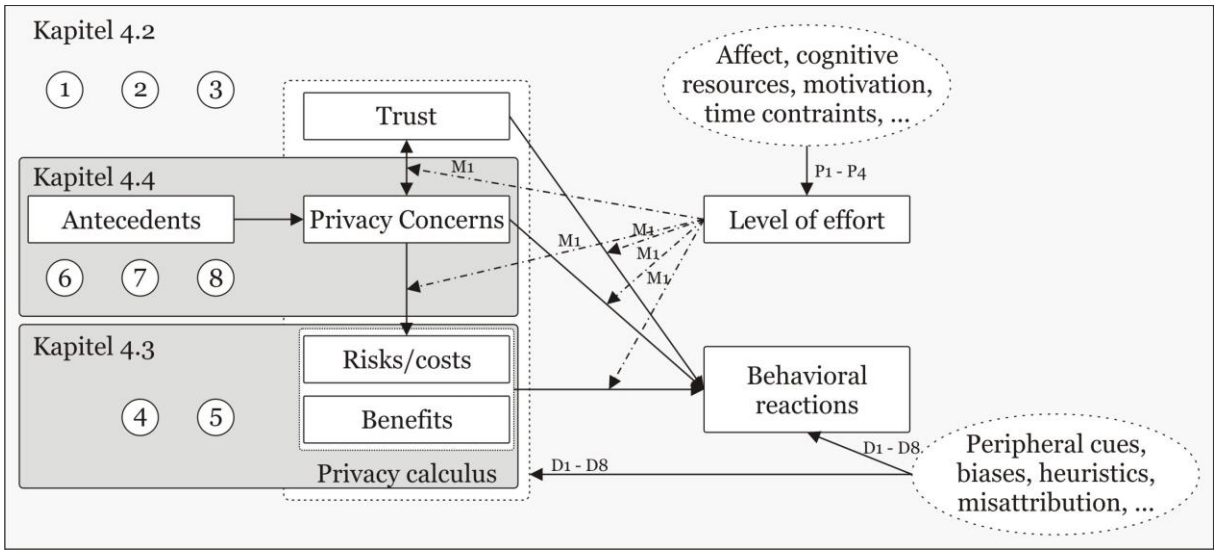

Abbildung 7. Einordnung der Forschungsbeiträge im erweiterten APCO-Modell (in Anlehnung an Dinev et al., 2015, S. 643).

In Unterkapitel 4.3 werden zwei Publikationen (4-5) unter dem Titel *Privatheit als wahrgenommener Wert* zusammengefasst. Die Publikationen adressieren das Privatheitskalkül als relevantes Konstrukt in der Privatheitsforschung und gehen hierbei insbesondere auf den Bereich der *Benefits* ein.

In Unterkapitel 4.4 werden drei Publikationen (6-8) unter dem Titel *Privatheitsbedenken bei mobilen Applikationen* zusammengefasst. Die Publikationen adressieren Privatheitsbedenken als das zentrale Konstrukt in der Privatheitsforschung.

4.2 Der Kontext des Entscheidungsverhaltens beim Bezug mobiler Applikationen

Das Verhalten von Nutzern in Informationssystemen ist zu einem hohen Grad abhängig vom Kontext, in welchem es stattfindet (Aarts & Dijksterhuis, 2000; Dijksterhuis et al., 2005). Zahlreiche Autoren messen dem Kontext einen maßgeblichen Einfluss auf das Entscheidungsverhalten bezüglich der informationellen Privatheit in Informationssystemen zu (Bansal et al., 2008; Nissenbaum, 2010). Dinev et al. (2015) identifizieren in der Untersuchung von kontextuellen und situativen Einflüssen auf Privatheitsentscheidungen große Forschungslücken (Dinev et al., 2015).

Die Publikation „Das Privatsphäre Paradox bei mobilen Applikationen: Kontextuale Besonderheiten mobiler Applikationen“ beleuchtet Apps als Softwareprodukte vor dem Hintergrund des Entscheidungsverhaltens durchschnittlicher Nutzer (Buck & Eymann, 2013). Hierbei wird die Diskrepanz zwischen Softwareprodukten in deren Beschaffenheit als Investitionsgüter und deren potentieller Wahrnehmung als schnell drehende Konsumgüter dargestellt. Im Rahmen der Publikation werden für Apps besondere Kontexteigenschaften herausgearbeitet und hierauf aufbauend für den Forschungsbereich relevante Hypothesen formuliert.

Die anschließende Publikation „The unconscious app consumer: Discovering and comparing the information-seeking patterns among mobile application consumers“ untersucht die im Bezugsprozess vorgehaltenen Informationen zum Softwaregut App sowie ob und inwiefern diese vom Nutzer wahrgenommen und für seine Bezugsentscheidung als relevant angesehen werden (Buck, Horbel, Germelmann et al., 2014). Im Rahmen einer Hauptkomponentenanalyse werden sieben Faktoren extrahiert. Eine anschließende Clusteranalyse beschreibt sechs unterschiedliche Gruppen von Nutzern.

Die Publikation „A four-factor framework of consumers’ perception of mobile applications” beleuchtet die Wahrnehmung mobiler Applikationen (Apps) (Buck, Horbel et al., 2017). Ausgehend von der technischen Beschaffenheit werden mögliche Wahrnehmungsverzerrungen aufgrund der kontextuellen Besonderheiten von Apps dargestellt. Ein Kontext-Rahmenwerk für die Wahrnehmung und Betrachtung von Apps aus der Perspektive der Nutzer wird abgeleitet.

4.2.1 Das Privacy Paradox bei mobilen Applikationen: Kontextuale Besonderheiten mobiler Applikationen (Buck & Eymann, 2013)

SMD und Apps sind seit Anfang der 2010er-Jahre in der modernen Gesellschaft und Wirtschaft omnipräsent. Durch ihre tiefe Alltagsintegration und ihren hohen Fragmentierungsgrad unterstützen Apps die Befriedigung von nahezu jedem alltäglichen Bedürfnis. Apps werden von Buck und Eymann (2013) definiert als „Softwareprogramme, die auf SMD abhängig von deren mobilem Betriebssystem, installiert werden können. Die Programme nutzen Internet- und Cloud-Computing-Anwendungen, um zum Teil stark fragmentierte (Alltags-) Bedürfnisse der Nutzer durch digitalisierte Anwendungs- und Dienstleistungsangebote zu befriedigen." (Buck & Eymann, 2013).

Die besondere Relevanz mobiler Ökosysteme, wie sie SMD in Verbindung mit Apps darstellen, für Wirtschaft und Gesellschaft liegt in der umfangreichen Generierung von persönlichen Daten. Durch die Adressierung von subjektiv empfundenen Nutzerbedürfnissen weisen diese persönlichen Daten in Bezug auf die Beschreibbarkeit eines einzelnen Nutzers einen besonders hohen Wert auf. Hierin begründet ist eine grundlegende ökonomische Austauschbeziehung beim Bezug von Apps: Die Aufnahme und Verarbeitung persönlicher Daten gegen die Nutzung des digitalen Service. Aufgrund der tiefgreifenden Verankerung von Apps im Alltag der Nutzer werden zwar stark fragmentierte, aber hochgradig personalisierbare Daten aufgezeichnet. Apps weisen, als konstituierendes Merkmal von SMD, eine Besonderheit in der Softwarebranche auf: Einen sehr hohen Grad an Aufnahme, Aggregation und Verwertung persönlicher Daten. Die sehr spezifischen Daten einzelner Apps können aufgrund der Architektur des IT-Systems anschließend ausgewertet und zu einem ganzheitlichen Nutzerprofil aggregiert werden. Demnach muss die unterstellte ökonomische Austauschbeziehung weiter gefasst werden in: Den Austausch der informationellen Privatheit gegen die Nutzung des digitalen Service.

Privatheit im Kontext einer ökonomischen Austauschbeziehung ist laut Müller et al. (2012) dann von Relevanz, „… wenn sie auf das Marktverhalten Einfluss nimmt, zum Beispiel wenn im Vertrauen auf die Erfüllung eines Privatheitsversprechens ein Kauf getätigt oder abgelehnt wird." (Müller et al., 2012, S. 144). Gerade im Kontext von Apps und den dahinterliegenden Geschäftsmodellen kann Privatheit als eigenständige Produkteigenschaft dargestellt werden. Hiernach sollte beim Bezug von Apps die zur

Disposition stehende Privatheit der Nutzer von diesen als wichtiger Wert wahrgenommen werden. Zwar weist die bestehende Literatur die hohe Relevanz von Privatheit für Nutzer bei der Teilnahme an digitalen Systemen nach, trotzdem findet keine entsprechende Anpassung des Konsumverhaltens statt (Acquisti & Grossklags, 2003). Die als Privatheitsparadox benannte Erklärungslücke beschreibt den Widerspruch zwischen der Absicht der Nutzer nur Services zu nutzen, die ihre Privatheit achten und dem in der Realität gegensätzlichen Verhalten.

Der Kontext des Bezugs und der Nutzung von Apps muss zur Erklärung des vermeintlich paradoxen Verhaltens von Nutzern näher beleuchtet werden. Einige verwandte Forschungsdomänen geben hierfür bereits wertvolle Impulse. Die Verhaltens- und Sozialpsychologie sieht den Nutzer nicht als rational handelnden Akteur im ökonomischen Sinne, sondern betrachtet seine Entscheidungen unter beispielsweise unvollständigen Informationen, instabilen Präferenzen und kognitiven Verzerrungen (Acquisti & Grossklags, 2003). Das Nutzerverhalten thematisiert die kontextabhängige Produktwahrnehmung, welche Umwelteinflüsse in ihre Betrachtung mit einbezieht (Aarts & Dijksterhuis, 2000). Die Theorie des unbewussten Nutzers betont ebenfalls den situativen Einfluss des Kontexts auf das Entscheidungsverhalten der Nutzer (Dijksterhuis et al., 2005).

Mobile Ökosysteme können als *digitale Konsum-Parallelwelten* angesehen werden und weisen zahlreiche kontextuale Besonderheiten auf, welche sich auch auf die Abwägung von Kosten (auch im Sinne der Preisgabe persönlicher Daten) und Nutzen auswirken. Die Besonderheiten von mobilen Ökosystemen, und Apps im Speziellen, werden durch technologische Entwicklungen wie beispielsweise Miniaturisierung und Steigerung der Rechnerleistungen sowie der deutlichen Nutzerzentrierung begründet. Bei der Nutzung eines SMD erhält der Nutzer ein rudimentär ausgestattetes Betriebssystem, kann dieses jedoch über den Bezug von Apps nahezu beliebig erweitern und durch zahlreiche Zusatzprogramme individuell auf seine Bedürfnisse abstimmen. Hierbei ist der Nutzer zu einem hohen Grad an das vorinstallierte Betriebssystem gebunden. Aufgrund der komplexen IT- und Softwarearchitektur muss jedoch angezweifelt werden, ob der durchschnittliche Nutzer über die nötige App-Literacy verfügt um dem System zugrundeliegende Wirkungsmechanismen verstehen und nachvollziehen zu können (Buck, Eymann et al., 2016).

Darüber hinaus kann der Kontext für Entscheidungen bezüglich des Bezugs und der

Nutzung von Apps anhand von drei übergeordneten Einflussfaktoren beschrieben werden, die in Abbildung 8 dargestellt sind.

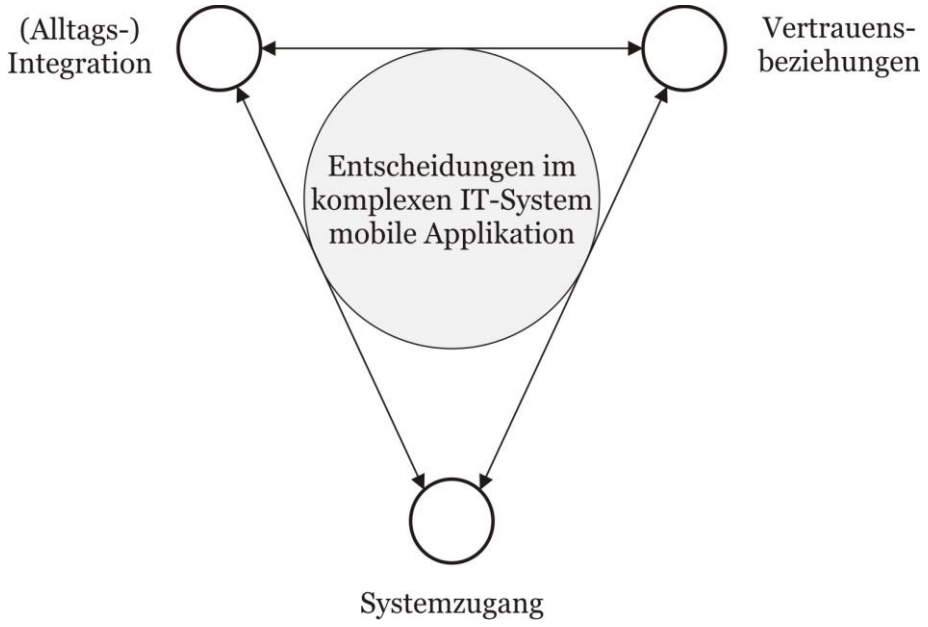

Abbildung 8. Entscheidungskontext mobiler Applikationen (Buck & Eymann, 2013, S. 1992).

Der Kontext von Apps wird maßgeblich beeinflusst vom Systemzugang, den wahrgenommenen Vertrauensbeziehungen und der vollzogenen Alltagsintegration des Systems. Unter Systemzugang wird die durch den Nutzer verwendete Hardware, das SMD, verstanden, welche zwingend in ein mobiles Ökosystem integriert ist. Darüber hinaus betrachtet der Systemzugang die Wahrnehmung des Informationssystems durch den Nutzer und seine Beziehung zum SMD. Unter Vertrauensbeziehungen werden die bestehenden Beziehungen der Akteure im Informationssystem, die damit verbundenen Informationsasymmetrien und mögliche Wahrnehmungen und Effekte subsumiert. Die Alltagsintegration beschreibt Verortung des Informationssystems im Nutzeralltag und die damit verbundene Wahrnehmung der Nutzer.

Titel der Publikation:

Das Privacy Paradox bei mobilen Applikationen: Kontextuale Besonderheiten mobiler Applikationen

Autoren:

Christoph Buck, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Torsten Eymann, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Eigenleistung von Christoph Buck an der Publikation:

Für die Publikation „Das Privacy Paradox bei mobilen Applikationen: Kontextuale Besonderheiten mobiler Applikationen“ habe ich mich als Lead-Autor im Rahmen der Entwicklung und Konzeption der zugrunde gelegten Fragestellung verantwortlich gezeichnet. Ich habe den theoretischen Bezugsrahmen und die aufgestellten Hypothesen entwickelt. Darüber hinaus habe ich den überwiegenden Teil des Textkörpers angefertigt und die Ergebnisse der Gutachten reflektiert, abgewogen und in die Publikation eingearbeitet.

Vollständige Zitation der Publikation:

Buck, C., & Eymann, T. (2013). Das Privacy Paradox bei mobilen Applikationen : Kontextuale Besonderheiten mobiler Applikationen. In M. Horbach (Ed.), GI Edition Proceedings: Vol. 220. Informatik 2013 - Informatik angepasst an Mensch, Organisation und Umwelt. Tagung vom 16. - 20. September 2013 in Koblenz, Germany (S. 1985–1999). Bonn: Ges. für Informatik.

Abrufbar von:

https://pdfs.semanticscholar.org/4053/4788a9f9b313f4511044337a14e42795f1cc.pdf

4.2.2 Der unbewusste App-Nutzer: Das Informations-Such-Verhalten von App-Nutzern (Buck, Horbel, Germelmann et al., 2014)

Das als Privatheitsparadox benannte widersprüchliche Verhalten von Nutzern (Norberg et al., 2007), nach welchem die Nutzer ihren Wunsch nach der Wahrung ihrer Privatheit ausdrücken aber trotzdem gegensätzlich handeln, kann in einer besonderen Ausprägung bei Apps beobachtet werden. In mobilen Ökosystemen beziehen Nutzer zahlreiche (monetär) kostenfreie Apps ohne sich über den Gegenwert ihrer persönlichen Daten bewusst zu sein. Trotz der tiefgreifenden Verankerung von Apps im Alltag und dem damit einhergehenden hohen monetären Gegenwert von persönlichen Daten geben Nutzer ihre Privatheit zunehmend gegen Apps mit teilweise nur geringem funktionalem Umfang auf.

In einem Markt mit vollständigen Informationen und einer rationalen Auswahl von Handlungsalternativen wären sich Nutzer dem Gegenwert ihrer persönlichen Daten bewusst und würden ihre Privatheit nur in gerechtfertigter Höhe preisgeben. Diese gerechtfertigte Höhe entspräche dem Gegenwert der Bedürfnisbefriedigung durch die Apps. Die Annahme der vollständigen Information muss bei Apps jedoch aufgegeben werden. Nach Darby und Karni (1973) können jegliche Güter in drei Eigenschaftstypen, nämlich Sucheigenschaften, Erfahrungseigenschaften und Vertrauenseigenschaften unterteilt werden (Darby & Karni, 1973). Weiber und Adler (1995) folgend verhalten sich die drei Eigenschaftstypen komplementär, jeder Kaufakt weist also immer einen Anteil an Sucheigenschaften, Erfahrungseigenschaften und Vertrauenseigenschaften auf (Weiber & Adler, 1995). Software im Allgemeinen und Apps im Speziellen weisen hiernach einen hohen Grad an Erfahrungs- und Vertrauenseigenschaften auf: Obwohl alle nötigen Informationen über die Apps vorab eingesehen werden können, kann die Funktionalität und die Qualität der App nur erfahren werden. Darüber hinaus ist es für Nutzer schwierig die Verarbeitungsbreite und -tiefe der genutzten persönlichen Daten nachzuvollziehen. Vor dem Hintergrund der bestehenden hohen Informationsasymmetrien müsste der App-Markt theoretisch zum Erliegen kommen (Hirshleifer, 1973). Im Gegensatz dazu zeigt der App-Markt steigende Wachstumszahlen, in dem Nutzer zunehmend Apps zu Befriedigung ihrer alltäglichen Bedürfnisse beziehen.

Um zu verstehen welche Informationen Nutzer für ihre Entscheidungsfindung des App-Downloads als wertvoll wahrnehmen, wurde der Kontext eines üblichen

Entscheidungsprozesses beim Download einer App entwickelt. Der in Abbildung 9 dargestellte Bezugsrahmen zeigt unterschiedliche Einflüsse auf die Entscheidungsfindung des Nutzers. Neben Informationen durch das mobile Ökosystem (App-Anbieter; Betriebssystem-Anbieter) können die anonyme Masse der App-Nutzer (beispielsweise durch Bewertungen und Kritiken), die soziale Gruppe des Nutzers sowie die Aufnahme externer und unabhängiger Informationen (beispielsweise unabhängige Testberichte) Einfluss auf das Entscheidungsverhalten des einzelnen Nutzers haben.

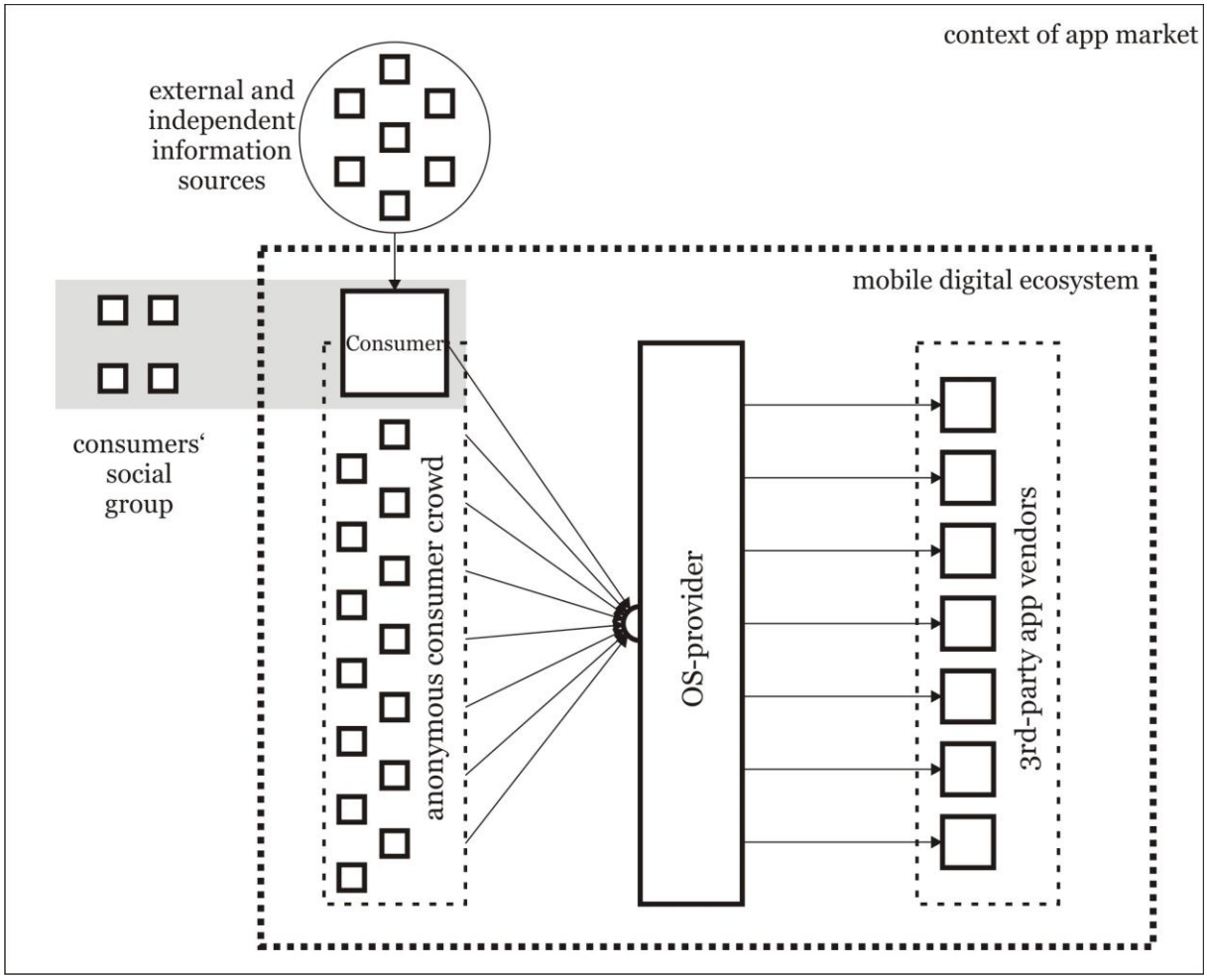

Abbildung 9. General framework of an app purchase decision-making process (Buck, Horbel, Germelmann et al., 2014, S. 5).

Entlang des Kaufprozesses, von der Wahrnehmung des Angebots der Apps bis hin zum Download der App, wurde ein quantitativ-empirischer Online-Fragebogen entwickelt. Der Fragebogen spiegelt die Chronologie wieder, welche den beim Informations- und Kaufprozess präsentierten Informationen entspricht. Die Chronologie wird durch die

Phasen Bekanntwerden, Suche im App-Store, Suchergebnisse und App-Information dargestellt und durch insgesamt 31 Variablen operationalisiert. 521 Probanden (N=521) nahmen an der Untersuchung teil, von welchen 42% weiblich (N=219) und 58% männlich (N=302) waren.

Im Rahmen einer Hauptkomponentenanalyse konnten sieben Faktoren extrahiert werden, welche 57,2% der Gesamtvarianz erklären. Durch Kalkulation der Mittelwerte kann gezeigt werden, dass der Faktor soziale Gruppe den höchsten Einfluss auf die Bezugsentscheidung einer App hat. Ebenfalls wichtige Faktoren stellen die App-Store-Informationen und die anonyme Reputation dar. Trotz der hohen Informationsasymmetrie spielen die Glaubwürdigkeit des App-Anbieters, das App Design und proaktive Informationspreisgabe nur eine untergeordnete Rolle.

Um ein tiefergreifendes Verständnis der Informationserfordernisse von Nutzern im Entscheidungsprozess des App-Downloads zu erlangen, konnten durch eine Clusteranalyse sechs Nutzertypen abgeleitet werden. Die Nutzertypen können beschrieben werden durch die Bezeichnungen *social prestige*, *co-creator*, *OS-associated*, *social group dependent*, *security seeker* und *egomaniac*. Die sechs Nutzertypen unterscheiden sich signifikant in den Bereichen Geschlecht, Tätigkeit, Einkommen, Betriebssystemzugehörigkeit und Erfahrung. Ebenfalls unterscheiden sich die Nutzertypen signifikant hinsichtlich ihrer Einstellung gegenüber unterschiedlicher Preis- und Monetarisierungsstrategien von Apps.

Die Ergebnisse der Studie zeigen auf, dass die Informationssuche und die von den Nutzern als relevant erachteten Informationen sehr stark auf soziale Komponenten sowie den Informationen des App-Stores fokussiert sind. Vor dem Hintergrund der Beschaffenheit von Apps und des bestehenden Privatheitsrisikos ist es jedoch fraglich, ob die bestehenden Informationsasymmetrien durch die bevorzugten Informationsquellen abgebaut werden können. Lediglich ein Nutzersegment (*security seeker*) legt großen Wert auf Informationen zu Privatheitseinstellungen, Sicherheit und der Vertrauenswürdigkeit der App.

Titel der Publikation:

The unconscious app consumer: Discovering and comparing the information-seeking patterns among mobile application consumers

Autoren:

Christoph Buck, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Chris Horbel, Department of Sociology, Environmental and Business Economics, University of Southern Denmark

Claas Christian Germelmann, Lehrstuhl für Marketing, Universität Bayreuth

Torsten Eymann, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Eigenleistung von Christoph Buck an der Publikation:

Für die Publikation „The unconscious app consumer: Discovering and comparing the information-seeking patterns among mobile application consumers“ habe ich mich als Lead-Autor verantwortlich gezeichnet. Ich habe die Forschungsfragen entwickelt und war maßgeblich am Studiendesign, der Datenaufnahme und der Datenauswertung für die Publikation beteiligt. An der Entwicklung und Anfertigung des Textkörpers, sowie die Reflektion und Einarbeitung der Gutachten war ich maßgeblich beteiligt.

Vollständige Zitation der Publikation:

Buck, C., Horbel, C., Germelmann, C. C., & Eymann, T. (2014). The Unconscious App Consumer: Discovering and Comparing the Information-Seeking Patterns among Mobile Application Consumers. ECIS 2014.

Abrufbar von:

http://aisel.aisnet.org/ecis2014/proceedings/track14/8/

4.2.3 Ein Kontextrahmenwerk für die Wahrnehmung mobiler Applikationen (Buck, Horbel et al., 2017)

Apps stellen, aufgrund der IT-Architektur mobiler Ökosysteme, ein konstituierendes Merkmal von SMD dar. Demnach sind Apps ein wesentlicher Bestandteil für die Funktionsfähigkeit von SMD ebenso wie für den Zugang von Nutzern zu digitalen Ökosystemen. Gemessen an der schieren Anzahl von Apps, stellen diese mittlerweile die meist benutzte Schnittstelle zwischen (privaten) Nutzern und digitalen Systemen dar – sie sind Schlüsselelemente für die Funktionalität von digitalen Systemen und deren Interface-Design. Die wachsende Relevanz und Popularität von Apps ist vorwiegend in der Alltagsintegration bei (privaten) Nutzern begründet. Durch die Nutzbarkeit von zahlreichen internen und externen Sensoren über das SMD, verbesserten Prozessoren, zunehmender Vernetzung und wachsender Speicherkapazitäten kann die Vision des *ubiquitous computing* von Weiser (1991) durch SMD und Apps als erreicht angesehen werden (Weiser, 1991). Hierdurch wird eine neue Sichtweise auf Nutzer von Informationssystemen von Nöten. Klassische Ansätze in der Forschungsdomäne der IS unterstellen einen organisationalen Hintergrund und eine aufgabenabhängige Nutzung von Informationssystemen. Die Publikation greift den Aufruf von Lamb und Kling (2003) auf und erweitert die Sichtweise auf die Nutzer von Informationssystemen um deren komplexe soziotechnische Nutzungssituation beschreiben zu können (Lamb & Kling, 2003).

Die Betrachtung von Nutzern von Informationssystemen als Individuen außerhalb von Organisationen wird unter dem Begriff des *experiential computing* subsumiert (Yoo, 2010). Die überwiegende Anzahl zielt auf die Bedürfnisbefriedigung von privaten Nutzern ab. In Abhängigkeit der Berechtigungen und Funktionalitäten verbindet eine App unterschiedliche Datenquellen, ermöglicht neue Wertversprechen und stellt effektive digitale Lösungen zu oftmals nicht-digitalen Bedürfnissen bereit. Die tiefgreifende Verankerung im Alltag wird von Apple Inc. treffend beworben als „There´s an app for that." (Apple Inc., 2017). Der Werbeslogan drückt in anschaulicher Art und Weise die breiten Anwendungsmöglichkeiten von Apps im Alltag der Nutzer aus.

Obwohl Apps aus einer technischen Perspektive komplexe Softwareprodukte darstellen und mit klassischer Desktop-Software vergleichbar sind, unterscheidet sich das Kauf-, Download- und Nutzungsverhalten. Trotz des erhöhten Privatheitsrisikos

agieren Nutzer beim Bezug und der Nutzung von Apps wesentlich unbedarfter. Diese vermeintlich leichtfertige Nutzung von Apps kann durch eine verzerrte Wahrnehmung des, auch aus technischer Perspektive, hochkomplexen Softwareguts begründet werden. Die Wahrnehmung der Nutzer von Apps und der daraus resultierende Entscheidungsprozess wird vom zugrundeliegenden Kontext stark beeinflusst (Dijksterhuis et al., 2005; Gerrig, 2012). Forschungsarbeiten zum *automativ goal-pursuit* implizieren, dass zielgerichtetes Handeln unbewusst und ausschließlich durch das vorliegende Umfeld bestimmt werden können (Aarts & Dijksterhuis, 2000).

Die hohe Akzeptanz von Apps resultiert aus der optimierten Zusammenführung von Nutzerinteressen und passgenauen Angeboten. Obwohl Apps in der Regel als Softwareprodukte von Drittparteien angeboten werden, wird dem Nutzer ein Bild eines einheitlichen App-Stores und dem Angebot *aus einer Hand* suggeriert. Diese verzerrte Angebotswahrnehmung kann mit dem Prinzip des *figure and ground* erklärt werden, nach welchen Stimuli nur wahrgenommen werden, wenn sie sich von ihrem Hintergrund absetzen (Schiffman et al., 2012). Folglich ist es für Nutzer schwerer wahrzunehmen, dass Apps von (unbekannten) Drittanbietern zum Download angeboten werden. Zusätzlich tendieren Nutzer zu *group stimuli* und dem *need to closure* (Schiffman et al., 2012). Dies kann dazu führen, dass Nutzer aufgrund ihrer Erfahrung und ihrem Vorwissen Apps unterbewusst falsch zuordnen (beispielsweise dem Ökosystemanbieter) und die vorhandenen Informationsasymmetrien unterbewusst durch Erfahrungen, Erwartungen und Motive abbauen. Aufgrund ihres hohen Fragmentierungsgrads verniedlichen Nutzer Apps als kleine Alltagshelfer. Dies kann zu einer Habitualisierung des App-Bezugs führen, welche generell einer Anpassung der Risikopräferenzen nach sich ziehen kann.

Obwohl Informationen bezüglich der Privatheit und der Informationssicherheit der Nutzer (beispielsweise die Vertrauenswürdigkeit des Anbieters, der Bezug und die Verwendung persönlicher Daten) höchste Priorität bei der Auswahl einer App haben sollten, scheinen derartige Informationen nur geringe Relevanz bei den Nutzern einzunehmen (Buck, Horbel, Germelmann et al., 2014). Diese selektive Wahrnehmung unterstützt die Wahrnehmungsorganisation durch das Prinzip des *figure and ground* und führt zu einer verzerrten Interpretation der Wahrnehmung.

Um das Nutzerverhalten hinsichtlich Apps und mobiler Ökosysteme besser verstehen zu können muss der relevante Kontext bestimmt und betrachtet werden. Hierbei

können im Hinblick auf die Wahrnehmung von Apps vier verschiedene Dimensionen identifiziert werden, welche in Abbildung 10 dargestellt sind.

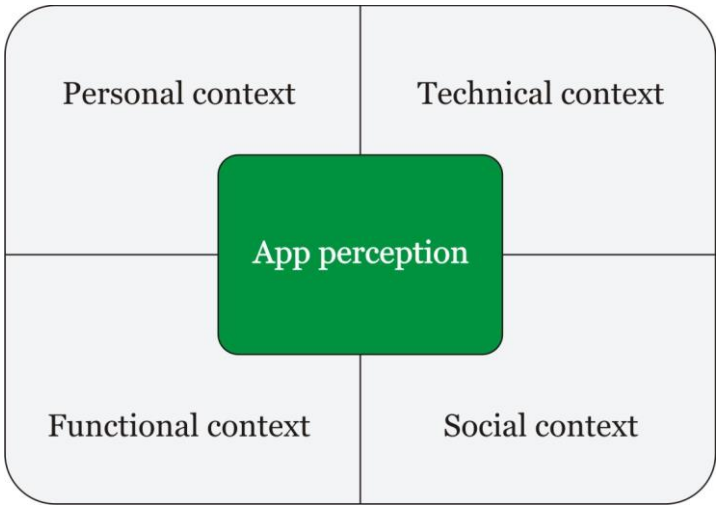

Abbildung 10. The context framework of app perception (Buck, Horbel et al., 2017).

Die Wahrnehmung von Apps wird beeinflusst durch den persönlichen, den technischen, den funktionalen und den sozialen Kontext. Der persönliche Kontext wird bestimmt durch die Verwendungsrichtung des Informationssystems. Durch die tiefgreifende Alltagsintegration von Apps muss deren Wahrnehmung nicht vor dem organisationalen, sondern vor dem Hintergrund der privaten Nutzung diskutiert werden. Beim technischen Kontext spielen die Einflüsse der genutzten Hardware sowie des zugrundeliegenden Ökosystems maßgebliche Rollen für die Wahrnehmung einer App. Der funktionale Kontext beinhaltet Elemente wie die Einfachheit der Bedienung, die unmittelbare Nutzung und die Individualisierung des Gesamtsystems durch den Bezug unterschiedlicher Apps. Der soziale Kontext beschreibt die Integration des Nutzers in sozialen Gruppen und Beziehungen zu anderen Individuen.

Titel der Publikation:

A four-factor framework of consumers' perception of mobile applications in context

Autoren:

Christoph Buck, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Chris Horbel, Department of Sociology, Environmental and Business Economics, University of Southern Denmark

Tim Kessler, Juniorprofessur Internationales Technologiemanagement, insbesondere industrielle Dienstleistungen, Universität Bayreuth

Eigenleistung von Christoph Buck an der Publikation:

An der Publikation „A four-factor framework of consumers' perception of mobile applications in context" war ich als Lead-Autor beteiligt. Ich habe mich für die Entwicklung der Forschungsfragen verantwortlich gezeichnet und war maßgeblich an der Konzeption, dem Aufbau und der Anfertigung des Forschungsbeitrags, sowie der kritischen Reflexion und Einarbeitung der Gutachten, beteiligt.

Vollständige Zitation der Publikation:

Buck, C., Horbel, C., & Kessler, T. (2017). A four-factor framework of consumers' perception of mobile applications in context. Bayreuther Arbeitspapiere zur Wirtschaftsinformatik. (64), 1–34.

Abrufbar von:

https://epub.uni-bayreuth.de/3420/

4.3 Privatheit als wahrgenommener Wert

Persönliche Daten und informationelle Privatheit werden als neue Güterklasse definiert. Durch persönliche Daten können beispielsweise neue Services angeboten und bestehende Kostenstrukturen verbessert werden (Spiekermann-Hoff et al., 2015). Vor dem Hintergrund der steigenden Bedeutung persönlicher Daten und einer zunehmenden *Unsichtbarkeit* von Informationssystemen gewinnen Fragestellungen bezüglich der Wahrnehmung der Nutzer hinsichtlich des Wertes ihrer Privatheit an Relevanz. Das in der Literatur vorherrschende Konstrukt, welches den ökonomischen Austausch bei der Preisgabe persönlicher Daten für den Bezug oder die Nutzung eines Services abbildet, wird als Privatheitskalkül bezeichnet (Dinev & Hart, 2006). In seiner ursprünglichen Ausformung unterstellt das Privatheitskalkül den Nutzern eine objektive Bewertung der Austauschsituation und damit eine objektive Bewertung ihrer preisgegebenen persönlichen Daten. Die beiden nachfolgend vorgestellten Forschungsbeiträge weichen von dieser Annahme ab und definieren in informationeller Privatheit einen abstrakten Wert.

Die Publikation „App-Privacy as an Abstract Value – Approaching Contingent Valuation for Investigating the Willingness to Pay for App Privacy“ untersucht die Zahlungsbereitschaft von Nutzern für ihre Privatheit (Buck, 2015). Aufbauend auf der Klassifikation von Privatheit als abstraktem Wert wird im Rahmen einer Contingent-Valuation-Studie die Zahlungsbereitschaft von Nutzern für den Erhalt ihrer Privatheit untersucht.

Die Publikation „Privacy as a Part of the Preference Structure of Users App Buying Decision” betrachtet Privatheit als kaufrelevantes Produktattribut bei mobilen Applikationen (Buck, Stadler et al., 2017). Im Rahmen der vorgestellten Forschungsstudie wird untersucht, ob Nutzer Privatheit als kaufrelevantes Produktattribut von mobilen Applikationen wahrnehmen. Im Rahmen einer Choice-Based-Conjointanalyse wird die Wahrnehmung von Privatheit als Produktattribut untersucht.

4.3.1 Privatheit als abstrakter Wert (Buck, 2015)

Informationssysteme sind in Wirtschaft und Gesellschaft allgegenwärtig. Durch technologische Errungenschaften wie beispielsweise die Miniaturisierung, steigende Prozessorleistungen, wachsende Speicherkapazitäten und eine zunehmende Vernetzung sind Informationssysteme in nahezu sämtliche Bereiche des alltäglichen Lebens vorgedrungen. Im Massenmarkt der privaten Nutzer stellen SMD und Apps die gängigste Schnittstelle zwischen Informationssystemen und Anwendern dar. Apps erfüllen, von Navigation und Kalendererinnerungen über Gaming, Informationen, Sportunterstützung und Einkaufslisten, bis hin zur Steuerung von Smart Homes, kleinstfragmentierte Aufgaben und sind tief im Alltag der Nutzer integriert.

Die praktischen, leicht integrierbaren und oft ohne direkte Bedienung im Hintergrund laufenden Anwendungen sind zwar meist ohne monetäre Kosten zu beziehen, verlangen im Gegenzug jedoch die Preisgabe persönlicher Daten. Beim Bezug und der Nutzung von Apps treten die Nutzer in eine ökonomische Austauschbeziehung ein, bei der die durch die App zu erbringende Dienstleistung gegen die Preisgabe persönlicher Daten getauscht wird. Zwar werden zur Erbringung der Funktionalität personalisierter Anwendungen persönliche Daten benötigt, doch zeigt sich bei Apps, dass die weitere Verwendung der Daten oft intransparent und der Umfang der bezogenen Daten oft nicht im Verhältnis zum Leistungsumfang der Applikationen steht.

In der Literatur wird die angesprochene Austauschsituation durch das sogenannte Privatheitskalkül ausgedrückt (Dinev & Hart, 2006). Dem Privatheitskalkül folgend, bewerten Nutzer die dargestellte Austauschsituation rational und treffen ihre Entscheidung zum Bezug einer App auf Basis vollständiger Informationen. Demzufolge stellt die Preisgabe persönlicher Daten beim Bezug und bei der Nutzung einer App das Ergebnis einer bewussten Entscheidung, nach einer rationalen Abwägung zwischen Kosten und Nutzen, dar. In Anbetracht der zugrundeliegenden Annahmen, des Kontexts der Entscheidungssituation beim Download und der Nutzung von Apps und der Beschaffenheit von digitalen Informationen muss von der objektiven beziehungsweise objektivierten Bewertung der Preisgabe persönlicher Daten durch den Nutzer abgerückt werden. Persönliche Daten, und damit die Privatheit in digitalen Systemen, werden als abstrakter Wert definiert.

Doch welche Zahlungsbereitschaft besteht bei Nutzern für den Erhalt ihrer Privatheit?

Aufgrund der Wertbeschaffenheit von persönlichen Daten in digitalen Systemen

nimmt der vorliegende Artikel Abstand von klassischen Messmethoden zur Zahlungsbereitschaft. Um die Zahlungsbereitschaft ermitteln zu können, muss entweder ein maximaler Preis oder ein Reservationspreis als Referenzwert festgelegt werden. Da im Bereich persönlicher Daten jedoch keinerlei alternative Güter oder Services, keine Marktpreise und keine monetären Kompensationswerte vorliegen, können klassische Messmethoden (Willingness-To-Pay; Willingness-To-Accept) nicht angewendet werden. Aufgrund der nicht vorhandenen transparenten und vertrauenswürdigen Marktpreise wurde eine *Contingent Valuation Method* (CVM) zur Bestimmung der Zahlungsbereitschaft für den Erhalt der Privatheit bei Apps entwickelt. Im Rahmen der CVM wird versucht den individuellen Wert für ein Gut zu bestimmen. Die CVM wurde in Anlehnung an Carson (2012) in einem mehrstufigen Online-Fragebogen entwickelt. Abbildung 11 zeigt den Aufbau der Studie.

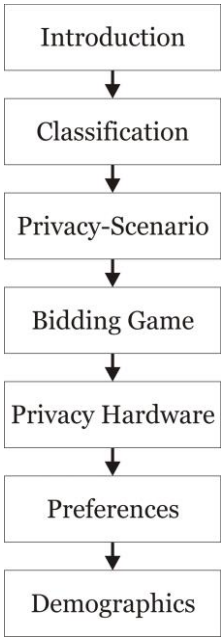

Abbildung 11. Setup of the Study (Buck, 2015, S. 109).

An der CVM-Studie haben insgesamt 1171 Probanden (N=1171) teilgenommen. 998 Datensätze konnten für die Datenanalyse verwendet werden. Die Ergebnisse zeigen signifikante Unterschiede in der Zahlungsbereitschaft in unterschiedlichen Gruppen. Hiernach haben Nutzer unterschiedliche Zahlungsbereitschaften in Abhängigkeit der bezogenen App.

Titel der Publikation:

App-Privacy as an Abstract Value - Approaching Contingent Valuation for Investigating the Willingness to Pay for App Privacy

Autor:

Christoph Buck, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Vollständige Zitation der Publikation:

Buck, C. (2015). App-Privacy as an Abstract Value - Approaching Contingent Valuation for Investigating the Willingness to Pay for App Privacy. Proceedings of The Fifteenth International Conference on Electronic Business, S. 105–115.

Abrufbar von:

http://iceb.nccu.edu.tw/proceedings/2015/

4.3.2 Privatheit als kaufrelevantes Produktattribut von mobilen Applikationen (Buck, Stadler et al., 2017)

In digitalen Systemen haben sich persönliche Daten zu einem eigenen Gut entwickelt. Gerade in mobilen Ökosystemen können persönliche Daten einen enormen ökonomischen Wert einnehmen (Spiekermann-Hoff et al., 2015). Durch die IT-Architektur mobiler Ökosysteme, der zugrundeliegenden Betriebssystemstruktur und der beliebigen Erweiterbarkeit durch Apps dringen die Informationssysteme tief in den Alltag von Nutzern ein. Die hierdurch gewonnenen persönlichen Daten können zu einem ganzheitlichen Nutzerprofil aggregiert und weiterverwendet werden (Buck, Horbel, Kessler et al., 2014). Dem Weltwirtschaftsforum folgend, stellen persönliche Daten eine neue Klasse an Wirtschaftsgütern dar (Schwab et al., 2011). Somit sind persönliche Daten eine Handelsware und können als werthaltiges Gut gehandelt werden. In der Literatur wird der Austausch von persönlichen Daten gegen die Nutzung einer App als Privatheitskalkül beschrieben (Dinev & Hart, 2006).

Im Rahmen des Forschungsbeitrags wird das Privatheitskalkül, welches der Annahme von vollständiger Information und einem rationalen Abwägen des Nutzers hinsichtlich der Kosten und Nutzen der Preisgabe persönlicher Daten folgt, kritisiert. Die verwendeten Annahmen erweisen sich in mobilen Ökosystemen als fragwürdig. Apps sind datenzentrische Dienste, wodurch der Wert der persönlichen Daten nicht nur im Moment der Datenaufnahme, sondern vielmehr durch Weiterverarbeitung, Aggregation, Verknüpfung und Auswertung generiert wird. Diese werthaltigen Verarbeitungsschritte, bedingt durch die Beschaffenheit digitaler Informationen, können vom Nutzer weder wahrgenommen noch eingeschätzt werden. Demnach stellt der Erhalt der Privatheit für Nutzer keinen monetär messbaren, sondern vielmehr einen abstrakten Wert dar.

Dieser Perspektivenwechsel ermöglicht es, das Verhalten von Nutzern besser verstehen zu können und nicht als paradox zu bewerten. In der gängigen Literatur wird unter dem sogenannten Privatheitsparadox subsumiert, dass Nutzer hohe Bedenken bezüglich ihrer Privatheit formulieren, in der Entscheidungssituation (beispielsweise Download einer App) aber dann doch gegensätzlich handeln (Norberg et al., 2007). Dieser Widerspruch kann zu Teilen dadurch erklärt werden, dass Nutzer den tatsächlichen Wert ihrer Daten nicht bewerten können und somit in der Entscheidungssituation von fehlgeleiteten Annahmen ausgehen. In Anbetracht des

Privatheitsparadox muss demnach die Frage gestellt werden, ob Nutzer im Erhalt ihrer Privatheit einen Wert sehen.

Im Kontext von mobilen Ökosystemen und Apps lautet die Forschungsfrage der vorgestellten Publikation: Stellt der Schutz der Privatheit beim Download einer App eine kaufrelevante Produkteigenschaft dar?

Zur Beantwortung der Forschungsfrage wurde mit der *Choice-Based-Conjointanalyse* (CBC) ein dekompositionelles Verfahren zur Untersuchung der Präferenzstruktur von Nutzern verwendet. Die CBC stellt eine Mischung aus der *Discrete Choice Analysis* (DCA) und der *Traditional Conjoint Analysis* (TCA) dar und misst die Nutzenwerte der Probanden. Den Teilnehmern der Studie wurden jeweils zehn randomisierte *Choice Sets* vorgelegt, in welchen sie sich für die für sie attraktivste Variante einer App entscheiden mussten. Im Rahmen eines *Choice-Sets* wurden den Probanden vier Varianten einer App mit unterschiedlichen Ausprägungen der einzelnen Produktattribute vorgelegt. Als Produktattribute wurden die durchschnittlichen Bewertungen, Privatheitseinstellungen, der benötigte Speicherplatz und der Kaufpreis in jeweils drei Stufen verwendet. Unter der Annahme, dass die Teilnehmer immer die Produktvariante mit dem höchsten individuellen Wert auswählen, konnten individuelle Nutzenwerte generiert werden.

Insgesamt nahmen 221 Probanden (N=221) an der Studie teil, woraus 111 verwertbare Datensätze generiert werden konnten. Die Auswertung der CBC zeigt auf, dass Privatheit im Rahmen der Studie als das wichtigste Produktattribut beim Download von Apps angesehen wird. Demnach kann im Schutz der Privatheit beim Bezug einer App ein kaufrelevantes Produktattribut gesehen werden.

Titel der Publikation:

Privacy as a Part of the Preference Structure of Users App Buying Decision

Autoren:

Christoph Buck, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Florian Stadler, zeb -360° Consulting for Financial Services

Kristin Suckau, Lehrstuhl für Innovations- und Dialogmarketing, Universität Bayreuth

Torsten Eymann, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Eigenleistung von Christoph Buck an der Publikation:

Für die Publikation „Privacy as a Part of the Preference Structure of Users App Buying Decision“ habe ich mich als Lead-Autor verantwortlich gezeichnet. Ich habe den Forschungsbedarf identifiziert und die Forschungsfrage federführend entwickelt. Bei der Entwicklung des Studiendesigns, der Datenaufnahme und der Datenauswertung war ich maßgeblich beteiligt. Ich habe den überwiegenden Teil des Textkörpers verfasst und die Ergebnisse der Gutachten reflektiert, abgewogen und in die Publikation eingearbeitet.

Vollständige Zitation der Publikation:

Buck, C., Stadler, F., Suckau, K., & Eymann, T. (2017). Privacy as a Part of the Preference Structure of Users App Buying Decision. In J. M. Leimeister und W. Brenner (Eds.), Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017) (S. 792–806). St. Gallen.

Abrufbar von:

http://aisel.aisnet.org/wi2017/track08/paper/1/

4.4 Privatheitsbedenken bei mobilen Applikationen

Mit der fortschreitenden Alltagsintegration von Informationssystemen nehmen auch die Privatheitsbedenken der Nutzer zu (Kokolakis, 2017). Privatheitsbedenken stellen das zentrale Konstrukt der Privatheitsforschung dar und werden in der Literatur als gängiger Proxy zur Messung von Privatheit benannt (Bélanger & Crossler, 2011; Li, 2011; Smith et al., 2011). Privatheitsbedenken sind vom jeweiligen Kontext abhängig (Nissenbaum, 2010). Verschiedene Autoren identifizieren in der Erforschung des Kontexts von Privatheitsentscheidungen und in den Privatheitsbedenken beeinflussenden Faktoren (Antecedents) großen Forschungsbedarf (Dinev et al., 2015; Smith et al., 2011).

Die Publikation „App Information Privacy Concerns“ beinhaltet die Entwicklung eines (für Apps) spezifischen Messinstruments für Privatheitsbedenken (Buck & Burster, 2017). Auf Basis der bestehenden Literatur wurde der *App Information Privacy Concern* (AIPC) entwickelt. Der AIPC wurde im Rahmen einer empirischen Studie durch eine Hauptachsenanalyse evaluiert.

Die Publikation „Priming App Information Privacy Concerns in Mobile Ecosystems“ untersucht den Zusammenhang zwischen unterschiedlichen Priming-Stimuli und Privatheitsbedenken (Buck, Burster et al., 2017). Im Rahmen einer Experiment-Serie werden sechs unterschiedliche Online-Experimente und deren Einfluss auf Privatheitsbedenken vorgestellt.

Die Publikation „Stop Disclosing Personal Data about Your Future Self“ untersucht den Zusammenhang zwischen Privatheitsbedenken und der Beziehung von Nutzern zu ihrem zukünftigen Selbst (Buck, 2017). Hierbei wird die grundlegende Hypothese untersucht, ob Nutzer, die sich stärker mit ihrem zukünftigen Selbst identifizieren, höhere Bedenken bezüglich ihrer Privatheit haben.

4.4.1 Privatheitsbedenken bei mobilen Applikationen (Buck & Burster, 2017)

Apps stellen ein Schlüsselelement für die Anwendbarkeit, Funktionalität und den Erfolg von mobilen Ökosystemen dar. Für zahlreiche webbasierte oder technologiebasierte Angebote und Wertversprechen stellen Apps die vom Nutzer gemeinhin akzeptierte Nutzeroberfläche dar. Aufgrund der tiefgreifenden Alltagsintegration stellen durch Apps und mobile Ökosysteme erhobene persönliche Daten wertvolle Wirtschaftsgüter dar, gegen deren Preisgabe die meisten Apps bezogen werden können. Demnach riskieren Nutzer beim Bezug von Apps ihre Privatheit auf einem sehr hohen Level.

Da Privatheit auf individuellen Erkenntnissen, Einstellungen und Wahrnehmungen beruht und als solche nicht gemessen werden kann, haben sich in der Literatur stellvertretend die sogenannten Privatheitsbedenken herauskristallisiert. Obwohl keine einheitliche Definition vorhanden ist, werden Privatheitsbedenken unter dem Grad subsumiert, unter welchem ein Nutzer einen Schaden in Verbindung mit persönlichen Daten wahrnimmt. In unterschiedlichen Studien wurden mehrere Messinstrumente für Privatheitsbedenken erstellt. Ausgehend vom *Concern For Information Privacy* (CFIP) von Smith et al (1996) wurden die *Internet Users' Information Privacy Concerns* (IUIPC) und der *Mobile Users' Information Privacy Concern* (MUIPC) entwickelt. Um den Kontext von Apps zu berücksichtigen wurden die bestehenden Konstrukte und Variablen untersucht, konsolidiert und zu einem *App Information Privacy Concern* (AIPC) weiterentwickelt. Die Weiterentwicklung der bestehenden und empirisch validierten Messinstrumente für Privatheitsbedenken zum AIPC erfolgte über ein dreistufiges Verfahren. Im ersten Schritt wurde der IUIPC als Basis für den AIPC identifiziert und im zweiten Schritt durch den MUIPC ergänzt. Im dritten Schritt wurde der finale AIPC definiert.

Der theoretisch hergeleitete AIPC verfügt über 17 Variablen in fünf Dimensionen (*Collection*, *Perceived Control*, *Awareness*, *Secondary Use of Information*, *Global Information Privacy Concern*). Tabelle 3 zeigt die 17 für den Kontext von Apps entwickelten Variablen.

Table 3. Items of the AIPC (Buck & Burster, 2017, S. 6–7).

Abkürzung	Formulierung der Variablen
MaPeCo1	Mobile app privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
MaPeCo2	(Mobile app user) control of personal information lies at the heart of mobile app users' privacy.
XuPeIn2	I believe that as a result of my using mobile apps, information about me that I consider private is now more readily available to others than I would want.
XuPeIn3	I feel that as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy.
MaAw1	Mobile app providers seeking information online should disclose the way the data are collected, processed, and used.
MaAw2	A good privacy policy for mobile app users should have a clear and conspicuous disclosure.
MaAw3	It is very important to me that I am aware and knowledgeable about how my personal information will be used.
MaColl1	It usually bothers me when mobile apps ask me for personal information.
MaColl2	When mobile apps ask me for personal information, I sometimes think twice before providing it.
XuPeSu2	I am concerned that mobile apps may monitor my activities on my mobile device.
XuPeSu3	I am concerned that mobile apps are collecting too much information about me.
XuSeUPI1	I am concerned that mobile apps may use my personal information for other purposes without notifying me or getting my authorization.
XuSeUPI2	When I give personal information to use mobile apps, I am concerned that apps may use my information for other purposes.
XuSeUPI3	I am concerned that mobile apps may share my personal information with other entities without getting my authorization.
MaGIPC2	Compared to others, I am more sensitive about the way mobile app providers handle my personal information.
MaGIPC3	To me, it is the most important thing to keep my privacy intact from app providers.
MaGIPC6	I am concerned about threats to my personal privacy today.

Um das neue Konstrukt des AIPC evaluieren zu können wurde eine Online-Befragung mit 355 Teilnehmern (N=355) in Deutschland durchgeführt. Im Rahmen einer Hauptachsenanalyse (Promax) konnten die drei Faktoren *Anxiety* (acht Variablen), *Personal attitude* (vier Variablen) und *Requirements*" (fünf Variablen) extrahiert werden. Die drei Faktoren erklären eine Gesamtvarianz von 60,64%.

Der entwickelte AIPC ermöglicht es Forschern bei zukünftigen Untersuchungen kontext-spezifische Variablen zur Untersuchung von Privatheitsbedenken bei Apps zu verwenden.

Titel der Publikation:

App Information Privacy Concerns

Autoren:

Christoph Buck, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Simone Burster, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Eigenleistung von Christoph Buck an der Publikation:

Für die Publikation „App Information Privacy Concerns“ habe ich mich als Lead-Autor verantwortlich gezeichnet. Ich habe den Forschungsbedarf identifiziert und die Forschungsfrage für das Anwendungsgebiet entwickelt. Bei der Entwicklung des Studiendesigns, der Datenaufnahme und der Datenauswertung war ich maßgeblich beteiligt. Ich habe den überwiegenden Teil des Textkörpers verfasst und die Ergebnisse der Gutachten reflektiert, abgewogen und in die Publikation eingearbeitet.

Vollständige Zitation der Publikation:

Buck, C., & Burster, S. (2017). App Information Privacy Concerns. AMCIS 2017.

Abrufbar von:

http://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/17/

4.4.2 Der Zusammenhang zwischen kognitiven Verzerrungen und Privatheitsbedenken (Buck, Burster et al., 2017)

Die fortschreitende Integration von Informationssystemen in den Alltag von privaten Nutzern impliziert neben zahlreichen Vorteilen für die Anwender auch einschneidende Konsequenzen. Vor allem im Bereich der Privatheit der Nutzer entstehen durch das *experiential computing* und durch für den Anwender zunehmend unsichtbare Systeme große Herausforderungen. Beim Bezug der meist (monetär) kostenlosen Apps treten die Nutzer explizit in eine ökonomische Austauschbeziehung ein. Für die Nutzung und Funktionalität des Informationssystems geben Nutzer ihre persönlichen Daten preis. Die Bewertung des Werts der persönlichen Daten im Moment des Downloads der App und hinsichtlich der zukünftigen Nutzung kann von Nutzern jedoch nicht eingeschätzt werden. Dadurch bedrohen Apps und mobile Ökosysteme zu einem hohen Grad die Privatheit der Nutzer.

Aufgrund der bestehenden hohen Informationsasymmetrie, welche durch die Nutzer nur mit sehr großem Aufwand reduziert werden könnten, müssten App-Märkte und mobile Ökosysteme nach der ökonomischen Theorie zum Erliegen kommen (Akerlof, 1970; Hirshleifer, 1973). In der Realität ist jedoch das Gegenteil der Fall. Trotz wachsender Bedenken hinsichtlich der Privatheit der Nutzer ist die Nachfrage nach Apps ungebrochen. Dieses vermeintlich widersprüchliche Verhalten wird in der Literatur unter dem Privatheitsparadox diskutiert, welches die Inkonsistenzen zwischen den Einstellungen von Nutzern hinsichtlich ihrer Privatheit und ihrem tatsächlichen Verhalten betrachtet. Während die benannten Inkonsistenzen in der Literatur oft als paradoxes Verhalten der Nutzer definiert werden, folgt der vorliegende Beitrag dem Aufruf von Dinev et al. (2015) zur Einbeziehung von sozialpsychologischen Effekten und Erkenntnissen aus der Verhaltensökonomie. Demnach wirken sich beispielsweise kognitive Verzerrungen oder instabile Präferenzen auf das Entscheidungsverhalten von Individuen in digitalen Systemen aus, wonach ihr Verhalten nicht mehr als paradox bezeichnet werden kann.

Die Alltagsintegration und die Funktionalität von Smartphones deuten darauf hin, dass sich Individuen in einem *low-effort*-Prozess befinden, wenn sie ihr Smartphone nutzen. Es ist davon auszugehen, dass die erforschten Effekte aus dem Bereich der Verhaltensökonomie und Sozialpsychologie auch starken Einfluss auf das Nutzungsverhalten in Informationssystemen und das Privatsphäre-Verhalten von

Nutzern haben (Acquisti & Grossklags, 2008; Dinev et al., 2015; Grossklags & Acquisti, 2007). Durch äußere Beeinflussungen entscheidet der Nutzer nicht zwingend auf Basis einer rationalen Kosten-Nutzen-Abwägung, sondern trifft Entscheidungen unter Zuhilfenahme des unterbewussten Systems. Dies impliziert, dass er sich über die Konsequenzen eines App-Downloads nicht bewusst ist und die Auswirkungen auf seine informationelle Privatsphäre unterschätzt.

Um mögliche Faktoren der Einflussnahme auf das Privatsphäre-Verhalten von Nutzern zu untersuchen wurde eine Serie von sechs Experimenten durchgeführt. Als unabhängige Variablengruppe wurden Priming Stimuli gewählt. Priming fällt unter die äußeren Beeinflussungen und kann durch eine Form der kognitiven Verzerrung beschrieben werden, die Individuen dahingehend beeinflusst, wie sie Informationen wahrnehmen und verarbeiten (Kahneman, 2012; Tulving et al., 1982). Priming Effekte treten in Situationen mit geringer kognitiver Anstrengung auf, die sowohl Handlungen als auch Emotionen beeinflussen können (Tulving et al. 1982; Dinev et al. 2015). Die direkte Messung der Kontrolle oder der Verletzung der informationellen Privatsphäre ist nahezu unmöglich, da Privatsphäre auf Kognition und subjektiver Wahrnehmung beruht und nicht auf rationalem Entscheidungsverhalten. Aus diesem Grund wurde der *App Information Privacy Concern* (AIPC) als abhängige Variable verwendet.

Die empirische Studie basiert auf sechs unterschiedlichen Experimenten bei denen insgesamt 1599 Probanden (N=1599) teilgenommen haben. Ziel der Experimente ist es aufzuzeigen, dass sich bereits durch das Einsetzen unterschiedlicher Priming Stimuli (beispielsweise *scrambled sentences* und *order of information*) Bedenken bezüglich informationeller Privatsphäre verändern.

Die Ergebnisse der Studie zeigen signifikante Unterschiede in unterschiedlichen Experimenten und auf Ebene verschiedener Gruppen. Die Ergebnisse der Experiment-Serie zeigen auf, dass mit einfachen Stimuli Anreize gesetzt werden können, die Nutzer zu veränderten Privatsphäre-Bedenken bewegen. Hohe Privatheitsbedenken können zu einer verantwortungsbewussten Preisgabe persönlicher Daten führen. Dies könnte implizieren, dass es in digitalen Systemen mit einfachen und unterbewusst wahrgenommenen Eingriffen möglich ist, das Verhalten hinsichtlich der Preisgabe persönlicher Daten zu beeinflussen.

Title:

Priming App Information Privacy Concerns in Mobile Ecosystems

Author:

Christoph Buck, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Simone Burster, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Torsten Eymann, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Eigenleistung von Christoph Buck an der Publikation:

Für die Publikation „Priming App Information Privacy Concerns in Mobile Ecosystems“ habe ich mich als Lead-Autor verantwortlich gezeichnet. Ich habe die Forschungsidee, die Forschungsfragen und das grundlegende Forschungsdesign entwickelt. Bei der Datenaufnahme und der Datenauswertung war ich maßgeblich beteiligt. Ich war federführend für die Erstellung und Überarbeitung des Forschungsbeitrags verantwortlich.

Vollständige Zitation der Publikation:

Buck, C., Burster, S., & Eymann, T. (2017). Priming App Information Privacy Concerns in Mobile Ecosystems. Bayreuther Arbeitspapiere zur Wirtschaftsinformatik. (63), 1–18.

Abrufbar von:

https://epub.uni-bayreuth.de/3419/

4.4.3 Der Zusammenhang zwischen der Identifikation mit dem zukünftigen Selbst und Privatheitsbedenken (Buck, 2017)

Der Einzug von Informationssystemen in den Massenmarkt privater Anwender führt zu spürbaren Veränderungen im Hinblick auf die Integration, den Umgang und die Wahrnehmung von digitalen Systemen. Apps sind mittlerweile in nahezu jeden Bereich des alltäglichen Lebens von privaten Nutzern eingezogen und erfüllen zahlreiche Bedürfnisse. Durch die immer tiefer greifende Integration von Apps im Alltag steigen mögliche Anwendungsbereiche durch die Informationssysteme und somit der wahrgenommene Mehrwert für die Nutzer. Dieser höhere Mehrwert wird generiert durch das Speisen der Informationssysteme mit persönlichen Daten, um auf deren Basis weiterführende Services anzubieten. Dementsprechend werden Informationssysteme mit dem Grad ihrer *Unsichtbarkeit* auf funktionaler Ebene zunehmend wertstiftender. Ein höherer Grad an *Unsichtbarkeit* impliziert einen geringeren Grad der aktiven Partizipation der Nutzer und somit eine höhere Anwenderfreundlichkeit. Diese tiefgreifende Integration erfordert in ihrer Konsequenz die Verwendung sensibler und intimer persönlicher Daten.

Die durch SMD und Apps erhobenen und verwendeten Daten weisen somit einen sehr hohen ökonomischen Mehrwert auf. Durch die tiefgreifende Integration der Informationssysteme geben Anwender, um die Funktionalität der Systeme nutzen zu können, hochgradig sensible Daten preis. Über die Aggregation der unterschiedlichen Datenfragmente der einzelnen Apps lassen sich im Umkehrschluss ganzheitliche Datenprofile erstellen, aus welchen Interessen, Bedürfnisse, Motive und Neigungen der Nutzer abgeleitet werden können (Mai, 2016). Demnach riskieren Nutzer ihre Privatheit durch den Bezug von Apps ohne die zukünftigen (möglicherweise negativen) Auswirkungen abschätzen zu können.

Trotz steigender Privatheitsbedenken in der Gesellschaft hinsichtlich digitaler Systeme steigt die Nutzung der *Alltagshelfer*. Mit, allein im Jahr 2016, über 180 Milliarden bezogenen Apps, ist die Nachfrage ungebrochen (Statistic Brain, 2016). Doch warum geben Nutzer ihre Privatheit für derart geringfügige Gegenleistungen preis?

Im Bereich der Gesundheitsvorsorge und der finanziellen Vorsorge existieren zahlreiche Erkenntnisse aus der Sozialpsychologie und der Verhaltensökonomie, inwiefern Individuen heutige Handlungen mit ihren zukünftigen Auswirkungen in Einklang bringen. Im Bereich des hyperbolischen Diskontierens bewerten Individuen

den kurzfristigen Nutzen höher als die langfristigen Schäden (beispielsweise durch das Rauchen). Im Hinblick auf die Preisgabe persönlicher Daten können die Auswirkungen auf die zukünftige Lebenssituation von Nutzern nicht abgeschätzt werden. Demnach müssten Nutzer im Hinblick auf ihre Zukunft vorsichtig mit ihren persönlichen Daten umgehen.

Um diesen Zusammenhang untersuchen zu können, wird das psychometrische Messinstrument der *Future Self-Continuity* (FSC) in die Forschungsdomäne der IS eingeführt. Das von Ersner-Hershfield et al. (2009) entwickelte Messinstrument untersucht, inwiefern sich Individuen mit ihrem zukünftigen Selbst identifizieren und ob sie in Abhängigkeit dieser Beziehung bei heutigen Entscheidungen Rücksicht auf ihr zukünftiges Selbst nehmen (Ersner-Hershfield et al., 2009). Demzufolge nehmen Individuen keine Rücksicht auf ihr zukünftiges Selbst, wenn sie sich nicht mit diesem identifizieren – sie behandeln ihr dieses wie einen Fremden.

Auf die Preisgabe persönlicher Daten projiziert bedeutet dies, dass Nutzer, welche sich mit ihrem zukünftigen Selbst stärker identifizieren, auch sensibler mit ihren persönlichen Daten umgehen. Da Privatheit als solche nicht gemessen werden kann, muss eine positive Beziehung zwischen der Identifikation mit dem zukünftigen Selbst und Privatheitsbedenken bestehen. In Anlehnung an die Arbeit von Ersner-Hershfield et al. (2009) wurde ein Online-Fragebogen entwickelt, welcher den Zusammenhang zwischen der FSC und dem *App Information Privacy Concern* (AIPC) untersucht.

Die Ergebnisse der Studie zeigen einen signifikanten Zusammenhang zwischen dem Konstrukt der FSC und dem AIPC. Demnach weisen Nutzer, die sich mit ihrem zukünftigen Selbst mehr identifizieren, höhere Privatheitsbedenken auf. Diesen Nutzern kann ein vorrausschauender Umgang mit ihren persönlichen Daten unterstellt werden.

Titel der Publikation:

Stop Disclosing Personal Data about Your Future Self

Autor:

Christoph Buck, Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth

Vollständige Zitation der Publikation:

Buck, C. (2017). Stop Disclosing Personal Data about Your Future Self. AMCIS 2017.

Abrufbar von:

http://aisel.aisnet.org/amcis2017/HumanCI/Presentations/14/

5 Kritische Reflexion und zukünftige Forschung

Mit der zunehmenden Vernetzung von Sensoren und Alltagsgeräten nehmen die Möglichkeiten zur Aufnahme, Speicherung und Verarbeitung von persönlichen Daten rapide zu. Durch die Integration von Informationssystemen in den Alltag und deren Zurücktreten in den Hintergrund geben Nutzer zunehmend ihre persönlichen Daten im Austausch für digitale Services preis, ohne die dahinter liegenden Transaktionen verstehen und nachvollziehen zu können. Das hierauf fußende Privatheitsparadox attestiert den Nutzern ein widersprüchliches Verhalten: Ihre Verhaltensabsichten stehen in Kontrast zu ihren tatsächlichen Handlungen.

Die vorliegende Dissertation hat zum Ziel, Ansätze zur Erklärung des Privatheitsparadox zu entwickeln und Forschungsergebnisse zu der nachfolgend formulierten übergeordneten Forschungsfrage zu erzielen: Welche Einflussvariablen bedingen Privatheitsentscheidungen in mobilen Ökosystemen?

Mit den drei in Unterkapitel 4.2 vorgestellten Forschungsbeiträgen kann ein Beitrag zum Verständnis der Kontextvariablen für Entscheidungen in mobilen Ökosystemen geleistet werden. In mobilen Ökosystemen existieren zahlreiche Einflussfaktoren welche die Wahrnehmung der digitalen Services verzerren können. Hierdurch kann in direkter und indirekter Art und Weise auch die Wahrnehmung auf die Entscheidungssituation bezüglich der Preisgabe persönlicher Daten beeinflusst werden. Dies kann gestützt werden durch das Informationsverhalten der Nutzer im App-Download-Prozess: Diese hinterfragen nur selten das tatsächliche technische Angebot der App, den App-Anbieter oder Vereinbarungen zu den preiszugebenden persönlichen Daten.

Die beiden in Unterkapitel 4.3 vorgestellten Forschungsbeiträge untersuchen den durch die Nutzer wahrgenommenen Wert ihrer persönlichen Informationen. Nutzer messen ihren persönlichen Daten zwar einen Wert zu, können diesen jedoch ob seiner abstrakten Natur nicht fundiert monetär benennen. Die Forschungsergebnisse lassen darauf schließen, dass Nutzer, abhängig von der thematischen Ausrichtung der App, ihrer Privatheit Wert zumessen und im Erhalt dieser ein kaufrelevantes Produktattribut von Apps sehen.

Darüber hinaus können im Rahmen der drei in Unterkapitel 4.4 vorgestellten Forschungsbeiträge weitere Ansätze zur Erklärung des Privatheitsverhaltens aufgezeigt werden. Neben der Entwicklung eines für den Kontext von Apps

spezifischen Messinstruments für Privatheitsbedenken konnten Anhaltspunkte aus der Sozialpsychologie identifiziert werden, die möglicherweise Einfluss auf das Privatheitsverhalten von Nutzern haben.

Die im Rahmen der Dissertation zusammengetragenen Forschungsbeiträge stellen, jeder Beitrag für sich, punktuelle Betrachtungen eines breit gefächerten Phänomens dar. Jeder der acht Beiträge weist Limitationen hinsichtlich der Methodik, des Betrachtungsgegenstands, der Perspektive oder der erhobenen Daten auf. Die vorliegende Arbeit kann kein ganzheitliches Bild bezüglich des Privatheitsverhaltens von Nutzern in mobilen Ökosystemen zeichnen. Zwar können einzelne Forschungsbeiträge in Beziehung zueinander gebracht werden, doch fehlt ein allumfassendes Bild um das Nutzerverhalten in seiner bestehenden Tiefe und Komplexität verstehen zu können. Die Beiträge können jedoch, wenn auch mit nur eingeschränkter Generalisierbarkeit für alle Informationssysteme und Nutzer, im Bereich von mobilen Ökosystemen und Apps einen Beitrag zum wissenschaftlichen Diskurs leisten. Die Forschungsbeiträge sollen als initiale Arbeiten verstanden werden, welche zahlreiche Bedarfe für zukünftige Forschungsarbeiten identifizieren.

Zukünftige Forschung muss den Entscheidungskontext detaillierter untersuchen um das Nutzerverhalten besser verstehen zu können, um das Privatheitsparadox erklären und abbauen zu können und um dem Ziel der informationellen Selbstbestimmung der Nutzer näher zu kommen. Hierfür sollten Forschungsarbeiten versuchen mobile Ökosysteme ganzheitlich zu verstehen und das Nutzungsverhalten in Verbindung mit beispielsweise den verwendeten Geräten mit dem genutzten Betriebs- oder Ökosystem und vorhandenen Vertrauensstrukturen untersuchen. Eine wichtige und in der Literatur bisher vernachlässigte Kontextvariable stellt die *Literacy* dar. Um das Verhalten von Nutzern in mobilen Ökosystemen besser verstehen zu können, sollte ein Hauptaugenmerk auf die App- und Privacy-*Literacy* gelegt werden, da diese Aufschluss über das spezifische Wissen der Nutzer und somit über einen wichtigen Faktor im Entscheidungsprozess gibt.

Mit dem Perspektivenwechsel hin zum *experiential computing* geht auch die Aufforderung einher, das Verhalten von Nutzern als menschlichen Individuen in und mit Informationssystemen zu untersuchen. Demnach sollte sich die IS-Domäne im Allgemeinen und die Privacy-Forschung im Speziellen, Erkenntnissen und Forschungsrichtungen von verwandten Disziplinen wie beispielsweise der

Sozialpsychologie, der Soziologie oder der Verhaltensökonomie öffnen.

Vor dem Hintergrund von Privatheit und persönlichen Daten als neue Güterklasse bestehen darüber hinaus große Forschungsbedarfe hinsichtlich des Wertbeitrags der Nutzer in digitalen Systemen. Zukünftige Forschungsarbeiten sollten sich der Benennung, Definition und Transparenz des Wertbeitrags durch Nutzer widmen und Implikationen auf zukünftige Serviceangebote und Geschäftsmodelle beachten. Hierbei sollte immer die Selbstbestimmung der Nutzer bei der Nutzung von Informationssystemen im Vordergrund stehen. Auch regulatorische Konsequenzen aus bestehenden Forschungsergebnissen müssen in Betracht gezogen und kritisch geprüft werden. So sollte informationelle Privatheit zunehmende Relevanz im Bereich des Verbraucherschutzes und angrenzenden Gebieten erfahren.

Mit der Betrachtung von Privatheit und persönlichen Daten über die bestehenden Grenzen von Forschungsdisziplinen hinaus geht auch der Bedarf nach Methodenvielfalt einher. Eine zu starke Fokussierung auf quantitative Untersuchungen, durch beispielswiese Fragebogenforschung, sollte, aufgrund der hohen Kontextabhängigkeit von Privatheit, kritisch hinterfragt werden. Privatheit dringt in sämtliche Bereiche der Gesellschaft ein und sollte aus diesem Grund auch, je nach Perspektive und Fokus, mit den bestehenden mannigfaltigen Methoden untersucht werden.

Privatheit, vor allem informationelle Privatheit, ist ein wertvolles Gut, dass es für die Nutzer zu bewahren gilt. In modernen Informationssystemen kann einmal aufgegebene Privatheit nur schwerlich wieder hergestellt werden. Ein selbstbestimmter Umgang mit der eigenen Privatheit sollte jedem Nutzer möglich sein.

„Privatsphäre ist wie Sauerstoff – man schätzt sie erst, wenn sie fehlt."

John Emontspool

6 Literaturverzeichnis

Aarts, H., & Dijksterhuis, A. (2000). Habits as knowledge structures: Automaticity in goal-directed behavior. *Journal of Personality and Social Psychology*, *78*(1), 53–63.

Abowd, G. D., Iftode, L, & Mitchell, H. (2005). Guest editors' introduction: The smart phone--a first platform for pervasive computing. *IEEE Pervasive Computing*, *4*(2), 18–19.

Achten, O. M., & Pohlmann, N. (2012). Sichere Apps. *Datenschutz und Datensicherheit*, *36*(3), 161–164.

Ackerman, M. S. (2004). Privacy in pervasive environments: Next generation labeling protocols. *Personal and Ubiquitous Computing*, *8*(6), 430–439.

Acquisti, A., & Grossklags, J. (2003). Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior. *2nd Annual Workshop on Economics and Information Security-WEIS*. (1-27).

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26–33.

Acquisti, A., & Grossklags, J. (2008). What can behavioral economics teach us about privacy. In A. Acquisti (Ed.), *Digital privacy. Theory, technologies, and practices* (S. 363–377). New York: Auerbach Publications.

Akerlof, G. A. (1970). The market for "lemons": Quality uncertainty and the market mechanism. *The quarterly journal of economics*, *84*(3), 488–500.

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*.

Apple Inc. (2017). Apple Trademark List. Retrieved from https://www.apple.com/legal/intellectual-property/trademark/appletmlist.html

Avital, M., & Germonprez, M. (2003). Ubiquitous computing: surfing the trend in a balanced act. *Sprouts: Working Papers on*, *3*(19). Retrieved from https://www.researchgate.net/profile/Matt_Germonprez/publication/238619898_Ubiquitous_computing_surfing_the_trend_in_a_balanced_act/links/55e85b6a08ae65b638997d2b.pdf

Bansal, G., Zahedi, F. M.et al. Gefen, D. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. *ICIS 2008*.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS quarterly*, *35*(4), 1017–1041. Retrieved from http://www.jstor.org/stable/41409971

Bennett, C. J. (1995). The political economy of privacy: a review of the literature. *Center for Social and Legal Research*.

Bettencourt, L. A., Lusch, R. F., & Vargo, S. L. (2014). A service lens on value creation. *California management review*, *57*(1), 44–66.

Borriello, G. (2000). The challenges to invisible computing. *Computer*, *33*(11), 123–125.

Borriello, G. (2008). Invisible computing: automatically using the many bits of data we create. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, *366*(1881), 3669–3683.

Buck, C. (2015). App-Privacy as an Abstract Value - Approaching Contingent Valuation for Investigating the Willingness to Pay for App Privacy. *Proceedings of The Fifteenth International Conference on Electronic Business*, 105–115. Retrieved from http://iceb.nccu.edu.tw/proceedings/2015/

Buck, C. (2017). Stop Disclosing Personal Data about Your Future Self. *AMCIS 2017*.

Buck, C., & Burster, S. (2017). App Information Privacy Concerns. *AMCIS 2017*.

Buck, C., Burster, S., & Eymann, T. (2017). Priming App Information Privacy Concerns in Mobile Ecosystems. *Bayreuther Arbeitspapiere zur Wirtschaftsinformatik*. (63), 1–18.

Buck, C., Dettweiler, C., & Eymann, T. (2014). Informationsökonomische Einordnung von mobilen Applikationen. *HMD Praxis der Wirtschaftsinformatik*, *51*(2), 188–198.

Buck, C., & Eymann, T. (2013). Das Privacy Paradox bei mobilen Applikationen : Kontextuale Besonderheiten mobiler Applikationen. In M. Horbach (Ed.), *GI Edition Proceedings: Vol. 220. Informatik 2013 - Informatik angepasst an Mensch, Organisation und Umwelt. Tagung vom 16. - 20. September 2013 in Koblenz, Germany* (S. 1985–1999). Bonn: Ges. für Informatik. Retrieved from https://pdfs.semanticscholar.org/4053/4788a9f9b313f4511044337a14e42795f1cc.pdf

Buck, C., & Eymann, T. (2014). Risikofaktor Mensch in mobilen Ökosystemen. *HMD Praxis der Wirtschaftsinformatik*, *51*(1), 75–83.

Buck, C., Eymann, T., & Kaubisch, D. (2016). Wer weiß was? – Digitale Privatsphäre und App-Literacy aus Nutzerperspektive. In V. Nissen, D. Stelzer, S. Straßburger, & D. Fischer (Eds.), *Multikonferenz Wirtschaftsinformatik (MKWI) 2016. Technische Universität Ilmenau, 09. - 11. März 2016* (S. 391–402). Ilmenau: Universitätsverlag Ilmenau.

Buck, C., Germelmann, C. C., & Eymann, T. (2016). Datenweitergabe als Bedrohung? Konsumentenwahrnehmung am Beispiel mobiler Applikationen. In M. Schmidt-Kessel & C. Langhanke (Eds.), *Schriften zu Verbraucherrecht und Verbraucherwissenschaften: Band 6. Datenschutz als Verbraucherschutz* (S. 49–67). Jena: JWV Jenaer Wissenschaftliche Verlagsgesellschaft.

Buck, C., Horbel, C., & Eymann, T. (2014). The Unconscious App Consumer: Discovering and Comparing the Information-Seeking Patterns among Mobile Application Consumers. *ECIS 2014*. Retrieved from http://s3.amazonaws.com/academia.edu.documents/46318665/THE_UNCONSCIOUS_APP_CONSUMER_DISCOVERING20160607-18717-20cfkl.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1492092838&Signature=K4FNA3td%2B9BWEtQksXOG7SFz%2FIM%3D&response-content-disposition=inline%3B%20filename%3DThe_Unconscious_App_Consumer_Discovering.pdf

Buck, C., Horbel, C., & Kessler, T. (2017). A four-factor framework of consumers' perception of mobile applications in context. *Bayreuther Arbeitspapiere zur Wirtschaftsinformatik*. (64), 1–34.

Buck, C., Horbel, C., & Germelmann, C. C. (2014). Mobile Consumer Apps: Big Data Brother is Watching You. *Marketing Review St. Gallen*, *31*(1), 26–35.

Buck, C., Kessler, T., & Eymann, T. (2015). Nutzerverhalten als Teil der IT-Security: ein IS-Literaturüberblick. In O. Thomas & F. Teuteberg (Eds.), *Smart enterprise engineering. 12. Internationale Tagung Wirtschaftsinformatik (WI 2015) : Tagungsband* (S. 1115–1130). Osnabrück: Universität Osnabrück.

Buck, C., Stadler, F., & Eymann, T. (2017). Privacy as a Part of the Preference Structure of Users App Buying Decision. In J. M. Leimeister & W. Brenner (Eds.), *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)* (S. 792–806). St. Gallen. Retrieved from https://eref.uni-bayreuth.de/36125/

Campbell, J. E., & Carlson, M. (2002). Panopticon. com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media*, *46*(4), 586–606.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60–67.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Darby, M. R., & Karni, E. (1973). Free Competition and the Optimal Amount of Fraud. *The Journal of Law and Economics*, *16*(1), 67–88.

Dewey, J. (1934). *Art as experience*.

Dhawan, S. M., Gupta, B. M., & Gupta, R. (2016). Global pervasive and ubiquitous computing during 2005-14. *Annals of Library and Information Studies*, *63*(2), 117–125.

Dijksterhuis, A., Smith, P. K., & Wigboldus, D. H. (2005). The Unconscious Consumer: Effects of Environment on Consumer Behavior. *Journal of Consumer Psychology*, *15*(3), 193–202.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research*, *26*(4), 639–655.

Ersner-Hershfield, H., Garton, M. T., & Knutson, B. (2009). Don't stop thinking about tomorrow: Individual differences in future self-continuity account for saving. *Judgment and Decision Making*, *4*(4), 280–286.

Ferstl, O. K., & Sinz, E. J. (2013). *Grundlagen der Wirtschaftsinformatik* (7th ed.). Berlin/Boston: De Gruyter.

Geminn, C., & Roßnagel, A. (2015). „Privatheit" und „Privatsphäre" aus der Perspektive des Rechts – ein Überblick. *JuristenZeitung*, *70*(14), 703–708.

Gerrig, R. J. (2012). *Psychology and life* (2nd Australasian ed.). Frenchs Forest, N.S.W.: Pearson Australia.

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS quarterly*, *30*(3), 611–642.

Grochla, E. (1975). *Betriebliche Planung und Informationssysteme: Entwicklung und aktuelle Aspekte*. *Rowohlts deutsche Enzyklopädie: Vol. 373*. Reinbek b. Hamburg: Rowohlt.

Grossklags, J., & Acquisti, A. (2007). When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. *WEIS 2007*. Retrieved from http://weis07.infosecon.net/papers/66.pdf

Hansen, H. R., Neumann, G., & Mendling, J. (2015). *Wirtschaftsinformatik: Grundlagen und Anwendungen* (11. völlig neu bearbeitete Auflage). Berlin, Germany, Munich, Germany, Boston, Massachusetts: De Gruyter.

Hayes, G. R., Poole, E. S., & Truong Khai N. (2007). Physical, social, and experiential knowledge in pervasive computing environments. *IEEE Pervasive Computing*, *6*(4), 56–63.

Heinrich, L. J., Heinzl, A., & Riedl, R. (2011). *Wirtschaftsinformatik: Einführung und Grundlegung* (4., überarb. und erw. Aufl.). *Springer-Lehrbuch*. Berlin: Springer.

Hirshleifer, J. (1973). Where are we in the theory of information? *The American Economic Review*, *63*(2), 31–39.

Holzer, A., & Ondrus, J. (2011). Mobile application market: A developer's perspective. *Telematics and Informatics*, *28*(1), 22–31.

Hotter, M. (2011). *Privatsphäre: Der Wandel eines liberalen Rechts im Zeitalter des Internets* (1. Aufl.). *Campus Forschung: Vol. 951*. Frankfurt am Main: Campus Verlag GmbH.

Ihde, D. (2010). *Technology and the lifeworld: From garden to earth*. *Indiana series in the philosophy of technology*. Bloomington: Indiana University Press.

Kahneman, D. (2012). *Thinking, fast and slow*. London: Penguin Books.

Kessler, T., & Buck, C. (2017). How Digitization Affects Mobility and the Business Models of Automotive OEMs. In A. Khare, B. Stewart, & R. Schatz (Eds.), *Phantom Ex Machina. Digital Disruption's Role in Business Model Transformation* (S. 107–118). Cham, s.l.: Springer International Publishing.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–

Kovacs, G. (2012). *We are being watched. It's now time for us to watch the watchers.* Retrieved from https://www.ted.com/talks/gary_kovacs_tracking_the_trackers/transcript?language=de#t-380691

Krasnova, H., & Kift, P. (2012). Online privacy concerns and legal assurance: a user perspective. *AIS SIGSEC WISP Workshop on Information Security and Privacy*.

Lamb, R., & Kling, R. (2003). Lamb, Roberta, and Rob Kling. "Reconceptualizing users as social actors in information systems research. *MIS quarterly*, *27*(2), 197–235.

Laudon, K. C., Laudon, J. P., & Schoder, D. (2010). *Wirtschaftsinformatik: Eine Einführung* (2., aktualisierte Aufl.). *IT*. München: Pearson Deutschland.

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for information systems*, *28*(28), 453–496.

Lusch, R. F., & Vargo, S. L. (2014). *Service-dominant logic: Premises, perspectives, possibilities*. Cambridge: Cambridge University Press.

Lyytinen, K., Yoo, Y., & Sorensen, C. (2004). Surfing the next wave: design and implementation challenges of ubiquitous computing. *Communications of the Association for information systems*, *13*(1), 40.

Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society*, *32*(3), 192–199.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of social issues*, *33*(3), 5–21.

Merleau-Ponty, M. (1962). *Phenomenology of perception*. New York: Routledge.

Merli, G. (2013). The transformation of the business model: business modelling. In L. Cinquini, A. Di Minin, & R. Varaldo (Eds.), *Sxi - Springer per l'innovazione = Sxi - Springer for innovation: Vol. 8. New business models and value creation. A service science perspective* (S. 67–86). Milan: Springer.

Mertens, P. (2013). *Operative Systeme in der Industrie* (18., überarb. und aktualisierte Aufl.). *Lehrbuch: ; 1*. Wiesbaden: Springer Gabler.

Müller, G., Flender, C., & Peters, M. (2012). Vertrauensinfrastruktur und Privatheit als Ökonomische Fragestellung. In J. Buchmann (Ed.), *acatech Studie. Internet privacy. Eine multidisziplinäre Bestandsaufnahme ; a multidisciplinary analysis* (S. 143–188). Berlin: Springer Vieweg.

Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, California: Stanford Law Books an imprit of Standford University Press.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Olson, N., Nolin, J. M., & Nelhans, G. (2015). Semantic web, ubiquitous computing, or internet of things? A macro-analysis of scholarly publications. *Journal of Documentation*, *71*(5), 884–916.

Pearlson, K. E., Saunders, C. S., & Galletta, D. F. (2016). *Managing and using information systems: A strategic approach* (Sixth edition). Hoboken, NJ: Wiley.

Peter, J. P., & Tarpey, Sr., Lawrence X. (1975). A Comparative Analysis of Three Consumer Decision Strategies. *Journal of Consumer Research*, *2*(1), 29.

Prensky, M. (2001). Digital natives, digital immigrants part 1. *On the horizon*, *9*(5), 1–6.

Rössler, B. (2001). *Der Wert des Privaten* (1. Aufl., Orig.-Ausg). *Suhrkamp-Taschenbuch Wissenschaft: Vol. 1530*. Frankfurt am Main: Suhrkamp.

Saha, D., & Mukherjee, A. (2003). Pervasive computing: a paradigm for the 21st century. *Computer*, *36*(3), 25–31.

Satyanarayanan, M. (2001). Pervasive computing: Vision and challenges. *IEEE Personal communications*, *8*(4), 10–17.

Scheer, A.-W. (1998). *Wirtschaftsinformatik: Referenzmodelle für industrielle Geschäftsprozesse* (Studienausg., 2., durchges. Aufl.). Berlin: Springer.

Schiffman, L. G., Kanuk, L. L., & Hansen, H. (2012). *Consumer behaviour: A European outlook* (2. ed.). Harlow: Financial Times Prentice Hall.

Schmidt-Kessel, M., & Grimm, A. (2017). Unentgeltlich oder entgeltlich? - Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten. *ZfPW Zeitschrift für die gesamte Privatrechtswissenschaft*, 84–108.

Schoeman, F. (1984). Privacy: philosophical dimensions. *American Philosophical Quarterly*, *21*(3), 199–213.

Schwab, K., Marcus, A., & Hoffman, W. (2011). Personal data: The emergence of a new asset class. *An Initiative of the World Economic Forum*.

Segura, A. S., & Thiesse, F. (2015). Extending UTAUT2 to Explore Pervasive Information Systems. *ECIS 2015*. (Paper 154).

Silva, J. L., Campos, J. C., & Harrison, M. D. (2014). Prototyping and analysing ubiquitous computing environments using multiple layers. *International Journal of Human-Computer Studies*, *72*(5), 488–506.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, *35*(4), 989–1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, *20*(2), 167–196.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564.

Spiekermann, S., & Korunovska, J. (2017). Towards a value theory for personal data. *Journal of Information Technology*, *32*(1), 62–84.

Spiekermann-Hoff, S., Böhme, R., & Hui, K.-L. (2015). The Challenges of Personal Data Markets and Privacy. *Electronic Markets (em)*, *25*(2), 161–167.

Statistic Brain. (2016). Mobile Phone App Store Statistics. Retrieved from http://www.statisticbrain.com/mobile-phone-app-store-statistics/

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*(1), 36–49.

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in personnel and human resources management*, *8*(3), 349–411.

Sullivan, J., Scheepers, R., & Meddleton, C. (2009). Conceptualizing User Satisfaction in the Ubiquitous Computing Era. *ICIS 2009*. (Paper 103).

Thompson, M. J. (2005). DATA MINE-A story best told with numbers-Invisible Computing is Hard to Miss-The integration of technology into our business and personal lives is upon us. *Technology Review*, *108*(2), 86–87.

Tripathi, A. K. (2005). Reflections on challenges to the goal of invisible computing. *ACM Ubiquity*, *6*(17), 1.

Tulving, E., Schacter, D. L., & Stark, H. A. (1982). Priming effects in word-fragment completion are independent of recognition memory. *Journal of experimental psychology: learning, memory, and cognition*, *8*(4), 336–342.

Vargo, S. L., & Lusch, R. F. (2004). Evolving to a New Dominant Logic for Marketing. *Journal of Marketing*, *68*(1), 1–17. h

Vargo, S. L., Lusch, R. F., & Wieland, H. (2011). Alternative logics for service (s): From hybrid systems to service ecosystems. In D. Spath (Ed.), *Taking the pulse of economic development. Service trends* (S. 123–135). München: Hanser.

Varian, H. R. (2009). Economic Aspects of Personal Privacy. In L. M. Pupillo & W. H. Lehr (Eds.), *Internet Policy and Economics* (2nd ed., S. 101–109). Dordrecht: Springer.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193–220.

Weiber, R., & Adler, J. (1995). Informationsökonomisch begründete Typologisierung von Kaufprozessen. *Zeitschrift für betriebswirtschaftliche Forschung*, *47*(1), 43–65.

Weiser, M. (1991). The Computer for the 21st Century. *Scientific American*, *265*(3), 94–104.

Weiser, M. (1993). Some Computer Science Issues in Ubiquitous Computing. *Communications of the ACM*, *36*(7), 75–84.

Weiser, M. (1996). Ubiquitous Computing. Retrieved from http://www.ubiq.com/hypertext/weiser/UbiHome.html

Westin, A. F. (1968). Privacy and Freedom. *Washington and Lee Law Review*, *25*(1), 166.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of social issues*, *59*(2), 431–453.

Xu, H., Gupta, S., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. *ICIS 2012*.

Yoo, Y. (2010). Computing in everyday life: A call for research on experiential computing. *MIS quarterly*, *34*(2), 213–231.

Zhao, R., & Wang, J. (2011). Visualizing the research on pervasive and ubiquitous computing. *Scientometrics*, *86*(3), 593–612.