

2 Grundlagen zur Privatsphäreforschung

Diese Arbeit baut auf verschiedenen Forschungsströmen wie der Forschung zu Social Apps Stereotypen und Geschäftsmodellen auf, die jedoch häufig nur für einzelne Kapitel relevant sind. Aus diesem Grund werden im Rahmen des aktuellen Kapitels nur die Grundlagen und Forschungsergebnisse vorgestellt, die alle der folgenden Studien betreffen. Dies sind insbesondere die Grundlagen zum Thema Privatsphäre. Auf studien-spezifische Literatur wird dann im jeweiligen Kapitel näher eingegangen. Kapitel 7 stellt außerdem die Ergebnisse einer strukturierten Literaturrecherche vor. Diese beschäftigt sich mit verschiedenen Erlösmodellen von Anbietern kostenloser Services. Da diese Studie die Anbieterperspektive einnimmt, wird sie im hinteren Teil der Arbeit, der sich auf diese Perspektive konzentriert, vorgestellt.

2.1 Privatsphäre – Definition und Abgrenzung

Privatsphäre ist ein vielschichtiges Konzept, das aus verschiedenen Perspektiven und Disziplinen untersucht wurde (Smith et al. 2011). Dies hat dazu geführt, dass keine einheitliche Definition des Begriffs existiert (Solove 2006) und der Versuch, eine einheitliche Definition zu finden, von führenden Forschern aus der Wirtschaftsinformatik als wenig zielführend angesehen wird (Mennecke et al. 2014). Daher soll hier zwar ein Überblick über bestehende Definition gegeben, aber keine allumfassende Definition abgeleitet werden.

In der Literatur wird zwischen physischer und informationeller Privatsphäre unterschieden. Dabei bezieht sich die physische Privatsphäre auf die Umwelt von und den direkten Zugang zu Personen, während sich die informationelle Privatsphäre auf den Zugang zu Informationen über das Individuum bezieht (Smith et al. 2011). Dabei umfasst die informationelle Privatsphäre zwei der vier von Clarke (1999) definierten Dimensionen: Die Privatsphäre der Kommunikation und die Privatsphäre der Daten (Bélanger & Crossler 2011). Wie der Großteil der Wirtschaftsinformatikforschung (Bélanger & Crossler 2011), legt diese Arbeit ihren Schwerpunkt auf die Betrachtung der informationellen Privatsphäre, die im Folgenden nur noch mit „Privatsphäre“ bezeichnet wird.

Sind sowohl die physische als auch die informationelle Privatsphäre gemeint, wird der Begriff „allgemeine Privatsphäre“ verwendet.

Die in der Literatur existierenden Definitionen lassen sich vier verschiedenen Gruppen zuordnen (Smith et al. 2011). Dabei wird allgemeine Privatsphäre als Gut, Zustand, Recht oder als Kontrolle angesehen (Smith et al. 2011). Die Betrachtung von Privatsphäre als Recht basiert auf der Definition von Warren & Brandeis (1890), die allgemeine Privatsphäre als „das Recht allein gelassen zu werden“ definieren. Bei dieser Sichtweise wird Privatsphäre als Menschenrecht angesehen, das einen integralen Bestandteil des Wertesystems einer Gesellschaft darstellt (Smith et al. 2011). Eine abgeschwächte Variante ist die Definition von Privatsphäre als Gut. In diesem Fall wird Privatsphäre immer noch als wichtiger Wert betrachtet, es wird ihr jedoch ein ökonomischer Wert zugeschrieben und sie kann somit im Rahmen einer Kosten-Nutzen-Analyse gegen andere Werte abgewogen werden (Smith et al. 2011). Diese Konzeptionalisierung berücksichtigt die Tatsache, dass Individuen ihre Informationen preisgeben, obwohl sie große Privatsphärebedenken haben (Norberg et al. 2007). Privatsphäre wird somit immer mehr als Gut betrachtet, das gegen andere Güter eingetauscht werden kann (z. B. Campbell & Carlson 2002; Davies 1997).

Neben diesen beiden wertbasierten Definitionen existieren Definitionen, die Privatsphäre als Zustand ansehen. Dabei führte Westin (1967) als Erster die Definition von allgemeiner Privatsphäre als Zustand ein. Informationelle Privatsphäre wird in diesem Zusammenhang als „Zustand mit eingeschränktem Zugriff auf Informationen“ definiert (Smith et al. 2011).

Die vierte Gruppe von Definitionen schließlich definiert allgemeine Privatsphäre als Kontrolle. So definiert Margulis (1977) Privatsphäre als die „Kontrolle von Transaktionen zwischen Personen und anderen, mit dem Ziel Autonomie zu verbessern und/oder Verletzlichkeit zu minimieren“. Neuere Forschung in diesem Feld definiert Privatsphäre allerdings nicht mehr mit Kontrolle an sich, sondern mit der Fähigkeit zur Kontrolle (Smith et al. 2011). Kontrolle spielt in vielen Definitionen eine wichtige Rolle. Allerdings wird in einigen Veröffentlichungen Privatsphäre mit Kontrolle gleichgesetzt, während in anderen Veröffentlichungen Kontrolle nur eine Dimension von allgemeiner Privatsphäre darstellt.

Da Privatsphäre fast unmöglich zu messen ist und die Einschätzung davon häufig auf Wahrnehmungen beruht, wird zu deren Operationalisierung häufig auf die Privatsphärebedenken von Individuen zurückgegriffen (Smith et al. 2011). Zur Messung dieser

Privatsphärebedenken wurden verschiedene Skalen, wie beispielsweise die Concern for Information Privacy (CFIP) Skala (Smith et al. 1996) und die Internet Users' Information Privacy Concerns Skala (Malhotra et al. 2004) entwickelt.

In der deutschen Sprache existiert neben dem Begriff Privatsphäre auch noch der Begriff Datenschutz. Dieser Begriff wird im Rahmen dieser Arbeit verwendet, wenn es darum geht, die Privatsphäre zu schützen. Das heißt, Privatsphäre ist ein Zustand und ein Gut, das durch Datenschutz gewährleistet wird.

2.2 Zentrale Erkenntnisse der Privatsphäreforschung

Wie bereits bei der Definition von Privatsphäre erwähnt, wird diese mit Hilfe von Privatsphärebedenken erfasst (Smith et al. 2011). Somit stehen Privatsphärebedenken häufig im Kern der Untersuchungen, die sich mit Privatsphäre und der Preisgabe von Informationen beschäftigen und repräsentieren somit eines der meist untersuchten Konstrukte in der Privatsphäreforschung (Bélanger & Crossler 2011). Es finden sich hierzu vielfältige Studien, welche die Einflussfaktoren und Effekte von Privatsphärebedenken untersuchen (z. B. Hong & Thong 2013; Xu et al. 2012b). Um diese Forschungsergebnisse zu konsolidieren, wurden verschiedene Makromodelle entwickelt (z. B. Li 2011; Smith et al. 2011). Im Folgenden wird ein Überblick über diese Makromodelle gegeben und kurz auf die wichtigsten Konstrukte eingegangen, um eine Basis für das Verständnis der später folgenden Ausführungen zu schaffen. Eine umfassende Beschreibung der Erkenntnisse aus der Privatsphäreforschung soll hier jedoch nicht gegeben werden, da ein solcher Überblick sehr gut in anderweitiger Literatur existiert (z. B. Bélanger & Crossler 2011; Li 2011; Smith et al. 2011).

Ein wichtiger Bestandteil vieler Studien ist das so genannte Privatsphärealkül (englisch: Privacy Calculus) (z. B. Dinev & Hart 2006; Laufer & Wolfe 1977; Milne & Gordon 1993). Dieses beschreibt, dass Nutzer häufig die aus der Informationspreisgabe resultierenden Vorteile gegen deren Kosten abwägen, wenn sie über die Preisgabe von Informationen entscheiden. Die Kosten entsprechen dabei meist den wahrgenommenen Risiken, die aus der Preisgabe der Informationen entstehen. Der Nutzen setzt sich aus verschiedenen möglichen Vorteilen zusammen. In der Literatur werden diesbezüglich beispielsweise Vorteile wie Kompensation (Hann et al. 2007), personalisierte Services (Awad & Krishnan 2006), Selbstdarstellung (Krasnova et al. 2010) und Bequemlichkeit (Bélanger et al. 2002) diskutiert.

Risiko allgemein setzt sich aus einer Eintrittswahrscheinlichkeit und der Höhe des potenziellen Schadens zusammen (Peter & Tarpey 1975). Dabei spielt bei Entscheidungen von Individuen nicht nur das tatsächliche, sondern insbesondere auch das wahrgenommene Risiko eine wichtige Rolle. Daher wird auch im Privatsphärenkontext meist das wahrgenommene Privatsphärenrisiko untersucht (z. B. Krasnova et al. 2010; Xu et al. 2011b). Dieses ist definiert als der Grad, zu dem ein Individuum glaubt, dass ein hoher, potenzieller Verlust mit der Preisgabe von Informationen an ein bestimmtes Unternehmen einhergeht (Malhotra et al. 2004). Steigt das wahrgenommene Privatsphärenrisiko, sinkt die Bereitschaft, Informationen preiszugeben (z. B. Dinev & Hart 2006; Krasnova et al. 2010) oder Online-Services zu verwenden (z. B. Featherman & Pavlou 2003; Xu et al. 2005).

Abhängige Variablen in existierenden Studien sind meist Verhaltensreaktionen von Individuen. Beispielsweise wird häufig die Informationspreisgabe untersucht oder ob bestimmte Transaktionen im Internet, die eine Informationspreisgabe beinhalten, getätigt werden (z. B. Dinev & Hart 2006; Krasnova et al. 2010). Aufbauend auf der Theorie des überlegten Handelns (Fishbein & Ajzen 1975) haben viele der existierenden Studien jedoch lediglich die Absicht, eine bestimmte Handlung durchzuführen, gemessen und von dieser Absicht auf das tatsächliche Verhalten geschlossen. Ein solches Vorgehen ist vor dem Hintergrund des Privatsphäre-Paradox jedoch kritisch zu sehen. Dieses besagt, dass die Verhaltensabsicht bei der Preisgabe von Informationen häufig von dem wahren Verhalten abweicht (Jensen et al. 2005; Norberg et al. 2007).

Neben den drei Konstrukten, wahrgenommene Vorteile, wahrgenommenes Risiko und Verhaltensreaktionen der Nutzer, die zum Privatsphärenkalkül gehören, wird in vielen Modellen außerdem das Vertrauen in einen Service oder in dessen Anbieter berücksichtigt (Dinev et al. 2006; Gefen et al. 2003; Pan & Zinkhan 2006). Im Privatsphärenkontext wird Vertrauen als der Grad definiert, zu dem ein Individuum davon ausgeht, dass ein Unternehmen in Bezug auf den Schutz der persönlichen Informationen seiner Kunden verlässlich ist (Malhotra et al. 2004). Das Vertrauenskonstrukt umfasst mehrere Dimensionen, die je nach Definition voneinander abweichen können. Häufig diskutierte Dimensionen in diesem Zusammenhang sind Integrität, Wohlwollen und Fähigkeit (Gefen et al. 2003).

Ein sehr bekanntes und weit verbreitetes Makromodell ist das „Antecedents-Privacy Concerns-Outcome“-Modell (APCO-Modell) (Smith et al. 2011), das in Abbildung 2

dargestellt ist. Es fasst die Erkenntnisse aus der Literatur in einem übergeordneten Modell zusammen. Neben den oben vorgestellten Konstrukten, wahrgenommenes Risiko, wahrgenommene Vorteile, Vertrauen und Verhaltensreaktionen, geht das Modell außerdem auf die Einflussfaktoren von Privatsphärebedenken ein und stellt den Zusammenhang zwischen Privatsphärebedenken und staatlicher Regulierung dar. Diese Beziehungen beruhen auf einer systematischen Literaturanalyse. Bei manchen Beziehungen wie der zwischen Privatsphärebedenken und Vertrauen konnte keine eindeutige Richtung im Sinne von Kausalität identifiziert werden, weil die Ergebnisse aus der Literatur widersprüchlich sind. Während einige Studien davon ausgehen, dass das Vertrauen die Privatsphärebedenken reduziert (Bélanger et al. 2002), zeigen andere, dass eine Reduktion der Privatsphärebedenken zu einem reduzierten Vertrauen führen kann (Metzger 2004). Außerdem sind die im Modell dargestellten Effekte auf die Verhaltensreaktionen kritisch zu hinterfragen, da in den untersuchten Studien häufig die Verhaltensintention und nicht das reale Verhalten abgefragt wurde. Wie oben erwähnt, ist dieser Zusammenhang problematisch zu sehen, da im Privatsphärekontext das bereits beschriebene Privatsphäre-Paradox zu beobachten ist.

Neben den Effekten von Privatsphärebedenken auf Vertrauen, Risiken und Verhaltensreaktionen werden auch Einflussfaktoren auf Privatsphärebedenken im APCO-Modell berücksichtigt. Dabei werden Privatsphärebedenken laut APCO-Modell insbesondere durch fünf Faktoren beeinflusst: privatsphärebezogene Erfahrungen, dem Bewusstsein für Privatsphäre, Persönlichkeitsmerkmale, demographische Faktoren und der kulturelle Hintergrund eines Nutzers (Smith et al. 2011).

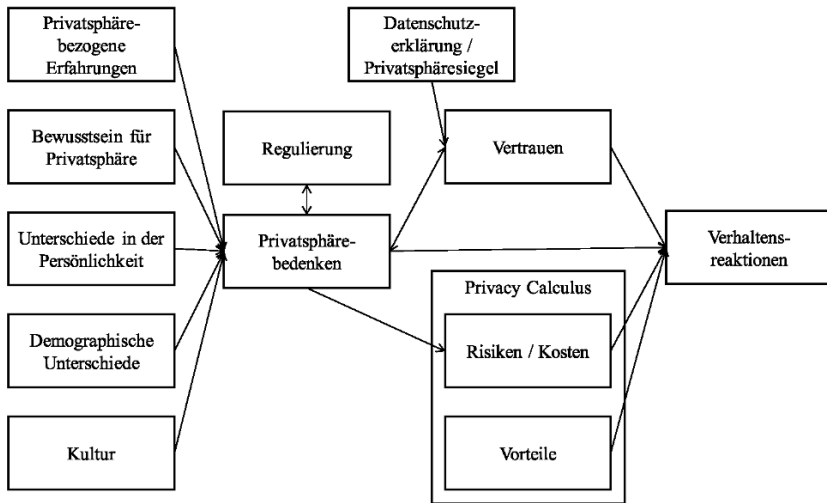


Abbildung 2: APCO-Modell nach Smith et al. (2011)

Neben dem APCO-Modell existieren zwei weitere Makromodelle, die in der Literatur diskutiert werden. Diese unterscheiden sich insbesondere hinsichtlich der Konzeptionalisierung von Privatsphärebedenken. Während im APCO-Modell nur das Konstrukt „Privatsphärebedenken“ vorkommt, werden diese bei den anderen Modellen weiter aufgeschlüsselt. So differenziert Li (2011) auf der individuellen Ebene zwischen allgemeinen und spezifischen Privatsphärebedenken. Allgemeine Privatsphärebedenken sind übergeordnete Bedenken, die Nutzer immer haben. Spezifische Privatsphärebedenken hingegen beziehen sich immer auf ein bestimmtes Unternehmen (Li 2011). Im Gegensatz zu Li (2011) gliedern Bélanger & Crossler (2011) die Privatsphärebedenken auf einer Ebene nicht weiter auf, sondern gehen davon aus, dass auf individueller, Gruppen-, Organisations- und gesellschaftlicher Ebene unterschiedliche Privatsphärebedenken vorliegen.

Ein weiterer Unterschied ist die Betrachtung von zusätzlichen Einflussfaktoren auf die Privatsphärebedenken. Neben personenbezogenen Unterschieden und kulturellen Faktoren werden in dem integrativen Framework von Li (2011) noch organisationale Faktoren wie die Reputation des anbietenden Unternehmens, soziale Faktoren und die Art der abgefragten Informationen mitberücksichtigt.

Das traditionelle APCO-Modell geht wie auch die anderen beiden Makromodelle davon aus, dass Individuen gezielt und aufwändig die verfügbaren Informationen verarbeiten

und basierend darauf eine rationale Entscheidung treffen (Dinev et al. 2015). Individuen verhalten sich jedoch häufig entgegen dieser Annahmen aus der klassischen Ökonomie. So haben erste Studien im Privatsphärenkontext gezeigt, dass Nutzer bestimmten kognitiven Verzerrungen unterliegen (Acquisti & Grossklags 2005; Acquisti et al. 2012) und dass auch Affekt einen Einfluss auf die Entscheidungen von Individuen hat (Li et al. 2011). Aufgrund dieser Einschränkungen wird zunehmend gefordert, dass aus der Verhaltensökonomie bekannte Verzerrungen bei der Untersuchung von Entscheidungsverhalten berücksichtigt werden (Ariely 2009).

Das klassische APCO-Modell wurde daher um Affekt und kognitive Verzerrungen erweitert (Dinev et al. 2015). So wird angenommen, dass der Aufwand, den ein Individuum bei der Informationsverarbeitung während einer privatsphärebezogenen Entscheidung betreibt, die Stärke der Beziehungen im APCO-Modell beeinflusst. Der Aufwand, den ein Individuum investiert, wird wiederum durch dessen aktuelle Emotionen, Motivation und Zeiteinschränkungen bestimmt. Neben diesen beiden Faktoren werden bei dem erweiterten Modell außerdem noch Verzerrungen und Heuristiken berücksichtigt (Dinev et al. 2015). Bei dem erweiterten Modell handelt es sich um ein konzeptionelles Modell, das als Ausgangspunkt für weitere Forschung mit Fokus auf kognitiven Verzerrungen und Emotionen dienen soll (Dinev et al. 2015). So sollen die hypothetisierten Zusammenhänge im Rahmen von empirischen Studien wie beispielsweise Experimenten näher untersucht werden (Dinev et al. 2015).

Nachdem in diesem Kapitel wichtige Begriffe und Konstrukte eingeführt wurden, wird im folgenden Kapitel die erste Studie zur Beantwortung der eingangs gestellten Forschungsfragen vorgestellt.

Der Wert von Nutzerinformationen aus Anbieter- und
Nutzerperspektive
Analyse des Trade-offs zwischen Datenverwendung und
Datenschutz
Eling, N.
2018, XXI, 245 S. 18 Abb., Softcover
ISBN: 978-3-658-19545-8