Morlok, Tina; Matt, Christian; Hess, Thomas

Working Paper

Privatheitsforschung in den Wirtschaftswissenschaften: Entwicklung, Stand und Perspektiven

Arbeitsbericht, No. 1/2017

Provided in Cooperation with:
University of Munich, Munich School of Management, Institute for Information Systems and New Media

Suggested Citation: Morlok, Tina; Matt, Christian; Hess, Thomas (2017) : Privatheitsforschung in den Wirtschaftswissenschaften: Entwicklung, Stand und Perspektiven, Arbeitsbericht, No. 1/2017, Ludwig-Maximilians-Universität München, Institut für Wirtschaftsinformatik und Neue Medien (WIM), München

This Version is available at:
https://hdl.handle.net/10419/170499

Privatheitsforschung in den Wirtschaftswissenschaften: Entwicklung, Stand und Perspektiven

Technical Report · September 2017

CITATIONS
0

3 authors, including:

Tina Morlok
Ludwig-Maximilians-University of Munich
8 PUBLICATIONS **1** CITATION

SEE PROFILE

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
FAKULTÄT FÜR BETRIEBSWIRTSCHAFT
INSTITUT FÜR WIRTSCHAFTSINFORMATIK UND NEUE MEDIEN
PROF. DR. THOMAS HESS
WIM

ARBEITSBERICHT 1/2017

Privatheitsforschung in den Wirtschaftswissenschaften: Entwicklung, Stand und Perspektiven

Tina Morlok, Christian Matt, Thomas Hess

Herausgeber

Prof. Dr. Thomas Hess

Ludwig-Maximilians-Universität München

Fakultät für Betriebswirtschaft

Institut für Wirtschaftsinformatik und Neue Medien

www.wim.bwl.lmu.de

Inhaltsverzeichnis

1 Einleitung

In den letzten Jahren ist das Konzept der Privatheit zu einem prominenten Thema der gesellschaftlichen, politischen und wissenschaftlichen Debatte geworden, auch in Deutschland. Durch den verstärkten und zugleich vernetzten Einsatz digitaler Technologien wird Privatheit, wie wir sie bisher kennen, vermehrt in Frage gestellt. Beispielsweise hat sich das Internet in den letzten 20 Jahren zu einer universalen Kommunikationsplattform entwickelt, die für Milliarden von Nutzern nicht mehr wegzudenken ist. Technologische Innovationen wie das „Internet der Dinge“ und „Pervasive Computing“ lassen die physische und die digitale Welt zunehmend verschmelzen. Soziale Netzwerke, intelligente Suchmaschinen, Web-Tracking sowie Technologien für die zunehmende Analyse und Vorhersagbarkeit von Vorlieben und Verhalten stellen ebenfalls die klassischen Konzepte der Privatheit mehr und mehr in Frage. Gleichzeitig gibt es auch interessante Ansätze, die helfen sollen, Privatheit im Internet wieder zurückzugewinnen.

Dabei ist die Verwendung persönlicher Nutzerdaten zentraler Kern der Diskussion, da immer mehr Konsumenten digitale Technologien und Online-Dienste für alltägliche Zwecke nutzen (Yoo 2010). Nicht nur, dass hierdurch immer mehr Nutzerdaten generiert werden, auch entwickeln sich die Analysemöglichkeiten für daraus resultierende Datenbestände stets weiter. Heutzutage stehen vermehrt leistungsfähige, computergestützte Verfahren zur Verfügung, die eine Aggregation von Daten sowie eine darauf basierende Prognose des Verhaltens deutlich vereinfachen. Es ist möglich, Daten aus unterschiedlichen Quellen miteinander zu verknüpfen und auszuwerten — unabhängig von deren Menge und deren Datenformat. Auch können die Daten immer schneller ausgewertet werden und eröffnen somit Unternehmen zahlreiche neue Potentiale, etwa bessere Einblicke in das Konsumentenverhalten, die Erfassung von deren Interessen oder auch den Verkauf von Daten. Konsumenten haben die Chance Güter schneller zu finden, müssen aber ggf. mit personenbezogenen Daten „zahlen“. Edward Snowden hat 2013 auch deutlich gemacht, dass nicht nur Unternehmen vermehrt Zugriff auf Konsumentendaten haben, sondern auch Regierungsbehörden u.U darauf zugreifen können.

Etablierte gesellschaftliche und rechtliche Normen als auch ethische Prinzipien bezüglich Privatheit greifen vor dem Hintergrund der skizzierten technologischen Entwicklung daher wahrscheinlich zu kurz. Gleichfalls soll und muss die Digitalisierung so gestaltet werden, dass sie den Grundstrukturen und -werten einer Demokratie gerecht wird. Der Umgang mit Privatheit ist dabei ein wichtiger Aspekt. Bislang ist unklar, wie Privatheit in einer digitalisierten Welt ethisch, rechtlich, normativ, politisch und technisch sichergestellt werden kann und welche wirtschaftlichen Chancen damit einhergehen (Forum Privatheit 2017).

Ökonomische Aspekte sind sowohl auf individueller als auch auf gesellschaftlicher Ebene von höchster Bedeutung. Bei seiner Entscheidung über den Umgang mit Privatheit berücksichtigt ein

Individuum auch ein ökonomisches Kalkül. Unternehmen erproben zur Zeit Erlösmodelle, die auf der verstärkten Verwertung personenbezogener Daten beruhen. Zudem entstehen neue Unternehmen, die sich ganz auf die Sammlung und Aggregation von personenbezogenen Daten spezialisieren. Es ist daher wesentlich, das Konzept Privatheit auch aus ökonomischer Perspektive zu betrachten. Daher setzt sich dieser Beitrag zum Ziel, das wirtschaftswissenschaftliche Verständnis von Privatheit und die Bearbeitung des Konzepts in den Wirtschaftswissenschaften (WiWi) übersichtlich darzustellen. Für die Analyse der wirtschaftswissenschaftlichen Literatur ziehen wir Quellen aus Betriebswirtschaftslehre (BWL) und Volkswirtschaftslehre (VWL) zu Rate. In der BWL dominieren definitionsgemäß die Individual- bzw. Anbieterperspektive (z.B. Dinev und Hart 2006; Li und Sarkar 2011). Die VWL adressiert grundsätzlich die Anbieter- und Marktebene sowie alle Typen von Akteuren (Konsument, Unternehmen, Staat), typischerweise aber abstrakter als die BWL.

Bei marktlicher Koordination, wie sie auch in Deutschland vorherrscht, tauschen Anbieter und Nachfrager Leistungen über einen Markt aus. Verfügt ein Anbieter über mehr Informationen über seinen (potentiellen) Kunden, dann kann er ein besseres, sprich gewinnoptimales Angebot aufstellen (etwa indem er für den einzelnen Kunden passendere Produkte empfiehlt), komplementäre Güter anbieten (z.B. mit Hilfe von auf das Verhalten oder die Präferenzen des Kunden zugeschnittener Werbung) oder aber gewonnene Daten verkaufen – alles natürlich nur im Rahmen des gegebenen gesetzlichen Rahmens und ggf. getroffener einzelvertraglicher Vereinbarungen. Gleichwohl wird der (potentielle) Kunde abwägen, ob er der Verwendung von Daten zustimmt, sofern für ihn die Intention des Anbieters transparent ist. Beides wird durch die technologischen Möglichkeiten determiniert. Abbildung 1 verdeutlicht den Zusammenhang zwischen technologischem Treiber und den verschiedenen Akteuren im Markt.

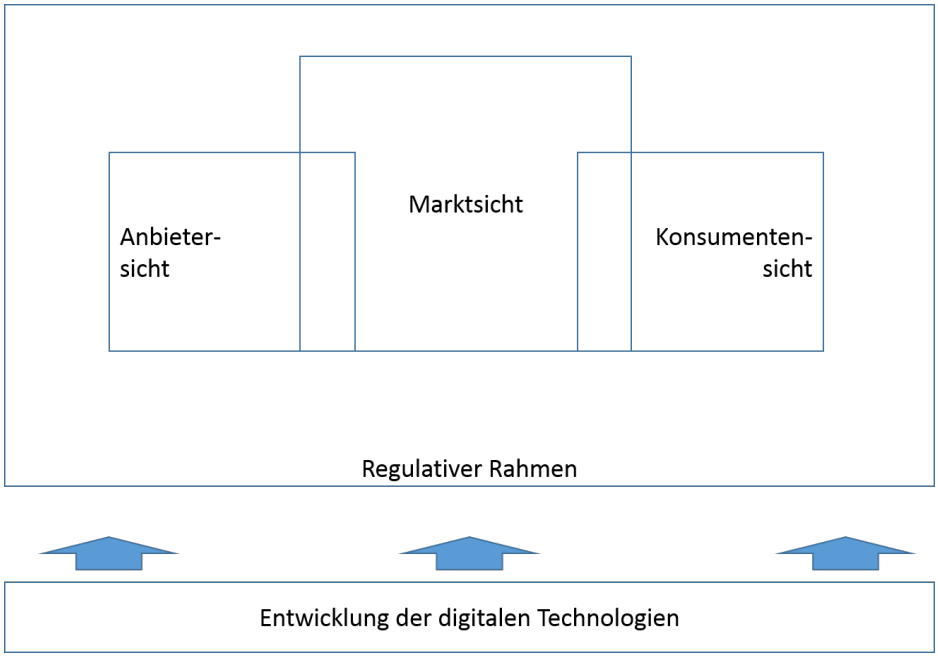

Abbildung 1 Ebenen der wirtschaftswissenschaftlichen Betrachtung des Themas Privatheit

Wirtschaftswissenschaftlich ebenfalls relevant ist die aggregierte Betrachtung des Handels der Wirtschaftssubjekte. Dabei geht es insbesondere um den Zusammenhang zwischen dem Umgang staatlichen Schutzes informationeller Privatheit und der volkswirtschaftlichen Leistung, gerade auch im Vergleich der erkennbaren Unterschiede zwischen Kontinentaleuropa und Nordamerika. Entscheidend dafür ist der regulative Rahmen.

Dieser Beitrag zielt darauf ab, auf Basis einer systematischen Literaturanalyse einen Überblick über die wesentlichen Forschungsstränge zum Konzept Privatheit in der WiWi-Literatur zu geben. Dabei steht im Vordergrund zu beantworten, was das Privatheitsverständnis in den WiWi ist und welche zentralen Forschungsfelder sich — auf Basis der drei wesentlichen Perspektiven der WiWi — unterscheiden lassen. In einer detaillierteren Darstellung stellen wir zudem die Ergebnisse aus der Literaturanalyse aus Konsumenten-, Anbieter- und Marktperspektive bereit. Der Beitrag führt zudem auf, welche Forschungslücken aktuell noch in den WiWi bestehen und welche Themen künftig stärker adressiert werden (sollten).

Der vorliegende Beitrag ist wie folgt strukturiert: In Kapitel 2 beschreiben wir, wie wir die systematische Literaturanalyse durchgeführt haben. In Kapitel 3 stellen wir, ebenfalls noch einleitend, das Privatheitsverständnis in den WiWi vor. Die Kapitel 4 bis 6 liefern die Ergebnisse der Literaturanalyse und umfassen die wesentlichen Forschungsstränge in den WiWi. Der Beitrag schließt mit einem Fazit und einem Ausblick für künftige Forschungsthemen in den WiWi (Kapitel 7).

Die Arbeit ist im Rahmen des „Forum Privatheit“ in der ersten Förderphase entstanden. Die vom Bundesministerium für Bildung und Forschung (BMBF) über einen Zeitraum von 3 Jahren geförderte erste Phase des Verbundprojekts verfolgte das Ziel, das Verständnis von Privatheit in der digitalen Welt sowie individuelle und gesamtgesellschaftliche Herausforderungen interdisziplinär herauszuarbeiten und darauf aufbauend mögliche Lösungskonzepte für die Wahrung informationeller Selbstbestimmung abzuleiten (www.forum-privatheit.de).

2 Methodik

2.1 Zweistufiges Vorgehen

Die WiWi-Literatur, die wir für die systematische Analyse berücksichtigt haben, umfasst einen Zeitraum von 1971-2017 und deckt somit die wesentlichen Wellen der Privatheitsforschung in den WiWi ab (Acquisti et al. 2016). Auf Basis des mehrstufigen Ansatzes von Webster und Watson (2002) haben wir relevante Publikationen innerhalb der BWL (inkl. Wirtschaftsinformatik) und VWL auf Basis von drei Stufen identifiziert. Für die Auswahl relevanter Publikationen haben wir uns an den Rankings für BWL und VWL orientiert. Zur Identifikation der relevanten Literatur in der BWL haben wir das VHB-Jourqual 3 Ranking herangezogen (VHB-JOURQUAL3 2017). Um die relevante Literatur in der VWL zu identifizieren, haben wir auf Basis des Handelsblatt-VWL-Rankings eine Auswahl an relevanten Zeitschriften getroffen (Handelsblatt 2013). Dabei berücksichtigt haben wir: MIS

Quarterly, Information Systems Research, European Journal of Information Systems, Journal of Management Information Systems, Journal of the Association for Information Systems, Journal of Information Technology, Journal of Strategic Information Systems American Economic Review, Organization Science, Management Science, American Economic Journal: Microeconomics, Communications of the ACM, Information & Management, Electronic Markets, Decision Support Systems, Economics Letters, International Journal of Industrial Organization, Journal of Business Ethics, Journal of Economic Behavior & Organization, Journal of Marketing Research, Marketing Science und The RAND Journal of Economics.

Neben Artikeln aus hochgerankten wissenschaftlichen Zeitschriften haben wir Konferenzbeiträge berücksichtigt, um auch aktuelleren Themen Rechnung zu tragen. Hierfür haben wir Konferenzbeiträge der relevanten Konferenzen in der Wirtschaftsinformatik – wo Konferenzen traditionell eine wichtige Rolle zukommt – analysiert und relevante Papiere ausgewählt. Berücksichtigt haben wir hierfür Tagungsbände der folgenden Konferenzen: International Conference on Information Systems (ICIS), European Conference on Information Systems (ECIS) und Hawaii International Conference on System Sciences (HICSS).

Zur Identifikation der Studien haben wir eine Stichwortsuche über wissenschaftliche Suchmaschinen (Google Scholar) und verschiedene wissenschaftliche Datenbanken (EBSCO, JSTOR archive) mit den Stichwörtern „Economics“, „Privacy“, „Advertising“, “Marketing”, “Social Welfare”, „Welfare“, „Personalization“, „Regulation“, „Willingness to Pay“, „Value of Privacy“, „Data Markets“, „Privacy Policies“, “Property Rights”, “Privacy Concerns”, “Privacy Calculus”, “Privacy Paradox”, und “Privacy at Work” durchgeführt. Wir haben die Titel und die Abstracts von jedem Artikel überprüft, um zu bewerten, ob eine Einbeziehung der Publikation angebracht ist. In Summe ergaben sich insgesamt 290 Artikel, die wir dann in der Tiefe überprüft haben.

Im zweiten Schritt haben wir die Zitationen der identifizierten Artikel analysiert sowie auf Google Scholar die „zitiert von“-Funktion herangezogen. Auf diese Weise haben wir weitere Artikel identifiziert, die wir in der Literaturanalyse berücksichtigt haben. Zudem haben wir auf die Zitationshäufigkeit geachtet, um die Bedeutung einer Studie zu approximieren. Die systematische und umfassende Suche führte zu einer Anzahl von insgesamt 407 Artikeln. In Abbildung 2 ist eine Übersicht über die Verteilung der Artikel im Zeitverlauf dargestellt. Insgesamt 162 Artikel nehmen die Individualperspektive ein. 122 Artikel adressieren die Anbieter- und 99 die Marktperspektive. Insgesamt 14 Artikel bilden eine Mischform aus den 3 Perspektiven und bei 10 Artikeln handelte es sich um Literatur-Reviews. Diese sind nicht in die Grafik miteingeflossen.

Die ersten Publikationen aus Marktperspektive wurden bereits in den 70er und 80er Jahren publiziert (Akerlof 1970, Hirshleifer 1971; Hirshleifer 1980; Posner 1981; Stigler 1980). Die erste kleinere Welle zur Forschung aus Individual- und Anbieterperspektive in den WiWi findet sich jedoch erst zu Beginn der 90er Jahre (z.B. Culnan 1993; Milne und Gordon 1993). Erst zur Jahrhundertwende haben die

Anbieter- und Individualperspektive den Schwerpunkt der Arbeiten in den WiWi ausgemacht. Nach einer zweiten Welle zu Beginn der 2000er Jahre (z.B. Milberg et al. 2000; Bélanger et al. 2002; Chan und Greenaway 2005) gab es seit 2011 wieder eine deutliche Zunahme an Studien zur Privatheit über alle drei Perspektiven hinweg. Insbesondere aus der Individualperspektive hat die Literatur hier wieder stark zugenommen, während die Literatur aus Anbietersicht seit Mitte der 2000er Jahre relativ gleichstark vertreten ist. 2015 sticht in der Verteilung besonders hervor, da hier nicht nur insgesamt eine deutlich höhere Anzahl an Publikationen vorliegt, sondern insbesondere aus Anbieter- und Marktperspektive eine deutlich höhere Zahl an Publikationen vorzufinden ist. Das Jahr 2017 ist noch nicht abgeschlossen, wir haben daher Publikationen berücksichtigt, die bis Frühjahr 2017 publiziert wurden.

Abbildung 2 Verteilung der Publikationen im Zeitraum von 1970-2017

2.2 Abgrenzung zu vorliegenden Literaturanalysen

Bereits in der Vergangenheit wurden verschiedene Literaturanalysen zum Thema Privatheit durchgeführt. Während einige Literaturanalysen aus einer interdisziplinären Perspektive durchgeführt wurden, um den interdisziplinären Charakter des Konzepts Privatheit Rechnung zu tragen (Bélanger und Crossler 2011; Li 2011; Li 2012; Smith et al. 2011), so gibt es auch verschiedene Literaturübersichten aus dem VWL-Bereich (Acquisti et al. 2016; Hui und Png 2005; Jentzsch 2016).

Eine der ersten Literaturanalysen zur Privatheitsforschung in der VWL stammt von Hui und Png (2005). Die Autoren thematisieren den sogenannten freien Marktansatz der VWL aus den 80er Jahren sowie indirekte und direkte Externalitäten, welche aus der Nutzung persönlicher Informationen entstehen. Die Autoren diskutieren verschiedene Lösungen für die optimale Allokation von persönlichen Informationen durch Eigentumsrechte und Regularien und argumentieren gegen den freien Marktansatz, da diese Sichtweise nicht zu einem ökonomisch effizienten Ergebnis führe (Hui und Png 2005). Acquisti et al. (2016) analysieren in ihrer Studie

theoretische und empirische VWL-Studien zum Thema „Ökonomie der Privatheit“. Dabei untersuchen die Autoren den ökonomischen Wert von Privatheit, die Konsequenzen von Privatheitsschutz und des Teilens persönlicher Informationen auf die gesamtwirtschaftliche Wohlfahrt. Ein weiterer Bestandteil des Artikels ist das Verständnis und Entscheidungsverhalten von Konsumenten in Bezug auf den Trade-Off zwischen dem Schutz und Teilen persönlicher Informationen. Die Autoren kommen zu dem Schluss, dass es nicht lediglich eine singuläre ökonomische Theorie von Privatheit gibt, da das Thema in verschiedenen Kontexten relevant ist. Die Autoren postulieren jedoch, dass in den jeweiligen Kontexten robuste theoretische Erkenntnisse identifizierbar seien (Acquisti et al. 2016). Ebenfalls aus einer VWL-Perspektive haben sich Cecere et al. (2017) mit dem Thema „Ökonomie der Privatheit“ befasst. Die Autoren argumentieren (ähnlich wie Acquisti et al. (2016)), dass aufgrund der Digitalisierung der Ökonomie und der Fortschritte in der Datenverarbeitung Ökonomen immer stärker auf die Rolle von persönlichen Daten in Märkten aufmerksam geworden sind (Cecere et al. 2017, S. 1). Die Autoren untersuchen die WiWi-Literatur und heben hervor, wie wichtig es ist, die komplexen Interaktionen zwischen den verschiedenen ökonomischen Akteuren zu berücksichtigen. Die Autoren heben zudem spezifische Strategien hervor, die sich mit Privatheitsproblemen befassen.

Eine weitere Literaturanalyse zur „Ökonomie der Privatheit“ hat Jentzsch (2016) durchgeführt. Die Autorin untersucht die Literatur zu den beiden Themenfeldern Ökonomie der Cyber-Security und Privatheit. Diese Literaturanalyse untersucht die bisherige Forschung anhand angewandter Methoden und thematisiert Marktversagen und identifizierte Probleme. Ebenso stellt diese Literaturanalyse praxisnahe und konkrete Handlungsempfehlungen für Firmen, politische Entscheidungsträger und Forscher bereit und ist somit als praxisorientiertes Gegenstück zu der recht abstrakten und breiten Übersicht von Acquisti et al. (2016) einzuordnen.

Obwohl bereits verschiedene Literaturübersichten aus interdisziplinärer und aus volkswirtschaftlicher Perspektive bestehen, fehlt bislang eine Übersicht, die die WiWi-Forschung und deren drei zentrale Perspektiven holistisch zusammenfasst. Insbesondere die BWL wurde in den bestehenden Literaturübersichten vernachlässigt. Einzig Cecere et al. (2017) hat zuletzt eine Analyse der WiWi durchgeführt. Ähnlich wie unser Ansatz unterscheiden die Autoren die Konsumentenperspektive, die Anbieterperspektive und die Marktperspektive. Die Autoren kommen zu dem Schluss, dass es schwierig ist, die richtige Balance zwischen dem Teilen und dem Schutz persönlicher Informationen zu finden. Die Autoren postulieren, dass Privatheitsschutz auch als Differenzierungskriterium für Unternehmen gesehen werden kann, welche sich so von Wettbewerbern abheben können, das ist allerdings abhängig von individuellen Präferenzen. Die Analyse von Cecere et al. (2017) konzentriert sich auf drei besondere Teilaspekte: Individuelles Verhalten, Verwertung von persönlichen Daten durch Unternehmen und staatliche Eingriffe durch Regulierung. Unsere Literaturanalyse verfolgt einen holistischeren Ansatz. Auf Basis der drei

zentralen Perspektiven leiten wir zu Beginn ein Privatheitsverständnis für die WiWi ab. Anschließend stellen wir aus der Individualperspektive die zentralen Konzepte der Privatheitsliteratur vor. Aus Anbieterperspektive umfasst unsere Analyse die Teilaspekte Personalisierung, Preisdiskriminierung und Privatheit in der Arbeitswelt. Im Rahmen der Marktperspektive betrachten wir nicht nur Regulierung, sondern auch die Themen Privatheitsschutz und Wohlfahrt sowie Märkte für personenbezogene Daten.

3 Privatheit und die Wirtschaftswissenschaften

3.1 Privatheitsverständnis in der Literatur

Verschiedene Disziplinen wie Philosophie, Sozial- und Politikwissenschaften, Recht, Psychologie, Wirtschaftswissenschaften sowie Informatik haben sich in der Vergangenheit mit dem Konzept der Privatheit befasst (Child et al. 2009; Raij et al. 2011; Saeri et al. 2014). Die Privatheitsforschung war daher durch ein hohes Maß an unterschiedlichen Zugängen gekennzeichnet. Im Laufe der Zeit hatten sich aufgrund dessen — anstelle eines einheitlichen Verständnisses — eine Vielzahl von meist disziplinspezifischen Konzeptualisierungen und Definitionen entwickelt (Smith et al. 2011). Zu Beginn der Privatheitsforschung wurde das Konzept häufig als *physische Privatheit* verstanden. Diese umfasst den physischen Zugang zu einem Individuum und/oder dessen räumlicher Umgebung und dem Privatraum. Daraus resultierte die im Rechtsbereich häufig angewandte Definition von Privatheit als das „Recht, alleine gelassen zu werden“ (Warren und Brandeis 1890). Andere Disziplinen, wie etwa die Philosophie und die Psychologie, beschreiben Privatheit als einen „Zustand des begrenzten Zugangs oder der Isolation“ (Schoeman 1984). In den Sozialwissenschaften wird Privatheit als ein soziales Problem und Verhaltenskonzept verstanden (Margulis 2003).

Die Konzepte, Definitionen und Beziehungen waren bis dato häufig inkonsistent und schwer ineinander überführbar. (Bélanger und Crossler 2011; Solove 2006). In der Fachliteratur dominiert das Konzept der *informationellen Privatheit* (Bélanger und Crossler 2011). Diese umfasst den Zugang zu persönlichen Daten, die gesammelt, verarbeitet und analysiert werden können (Smith et al. 2011).

In den Wirtschaftswissenschaften sind zwei Definitionen von Privatheit besonders stark vertreten. Eine zentrale Definition beschreibt Privatheit als ein *ökonomisches, handelbares Gut*, das im Austausch mit anderen Gütern oder Dienstleistungen getauscht werden kann (Dinev 2014; Smith et al. 2011). Privatheit wird aus wirtschaftswissenschaftlicher Sicht somit häufig als Ware definiert (Campbell und Carlson 2002; Davies 1998). Aus dieser ökonomischen(-philosophischen) Perspektive ist "Privatheit ein individueller und gesellschaftlicher Wert, aber sie ist nicht absolut, da man ihr einen ökonomischen Wert zuweisen und sie in einer Kosten-Nutzen-Berechnung berücksichtigen kann" (Smith et al. 2011, S. 993). Nach einer liberalen ökonomischen Perspektive schlagen Aaken et al. (2014) vor, dass das Konzept Privatheit als eine spezifische Form von Freiheit verstanden werden sollte. Obwohl die Autoren folgern, dass die Privatheit auf dem Markt gehandelt werden kann,

argumentieren sie, dass die Menschen ihre Freiheit und damit ihre Privatheit nicht unwiderruflich aufgeben können (Aaken et al. 2014).

Aus diesem Grundverständnis lässt sich das in den Wirtschaftswissenschaften dominierende Verständnis von Privatheit als *Kontrolle* oder als *Fähigkeit zur Kontrolle* erklären. Die Definition von Privatheit als *Kontrolle* wurde von Westin (1967) eingeführt. Westin (1967) definiert Privatheit als den Anspruch von Individuen, Institutionen und Gruppen, für sich selbst zu bestimmen, wann, wie und in welchem Ausmaß Informationen über sie an Dritte kommuniziert werden. Altman (1975) definierte Privatheit als die „selektive Kontrolle über den Zugang zu einem Selbst oder einer Gruppe“ (Altman 1975, S. 18). In der Forschung zur informationellen Privatheit wird diese Definition bevorzugt, da dieses Konzept einen nicht-normativen Charakter aufweist und eine empirische Untersuchung des Gegenstands ermöglicht (Smith et al. 2011).

Während die ursprüngliche Definition Privatheit als Kontrolle per se beschreibt, haben neuere Definitionen Privatheit vielmehr als die *Fähigkeit zur Kontrolle* (Smith et al. 2011, S. 995) beschrieben. Zum Beispiel definieren Culnan und Bies (2003) die Privatheit als "die Fähigkeit des Individuums, zu kontrollieren, unter welchen Bedingungen ihre personenbezogenen Daten erworben und verwendet werden" (S. 326). Dabei kommt es darauf an, inwieweit der Nutzer das Gefühl hat, über seine eigenen Informationen bestimmen zu können. Die Kontrolle kann zum einen in vollem Maße so bestehen, wie der Nutzer es wahrnimmt oder andererseits dem Nutzer nur das Gefühl geben, dass er die Datenpreisgabe kontrollieren kann.

Bezüglich der informationellen Privatheit kann zudem zwischen zwei Arten der Kontrolle unterschieden werden (Krasnova et al. 2010). Die Kontrolle über die *Informationspreisgabe* und die Kontrolle über die *Informationsverwendung* (Awad und Krishnan 2006; Hann et al. 2007). Li et al. (2010) definieren informationelle Privatheit als die Kontrollmöglichkeit für Individuen, Zeitpunkt, Art und Umfang, in welchen persönliche Informationen mit anderen ausgetauscht und genutzt werden, zu bestimmen. Wenn ein Individuum persönliche Informationen offenlegt, um zum Beispiel einen Online-Dienst zu nutzen, könnten diese Informationen an Dritte weitergeleitet werden. Die Datenverwendung und -verbreitung liegt dann außerhalb des Einflussbereiches der Nutzer (Chau und Clemons 2011). Der Kontrollverlust beschreibt somit, dass ein Individuum nach der Preisgabe von Informationen keine Kontrolle mehr über die Verwendung seiner Daten hat.

Neben dem grundlegenden Verständnis von Privatheit ist auch der Betrachtungsfokus entscheidend. Ein Großteil der Privatheitsforschung hat sich dem Konzept Privatheit aus der Perspektive des *Betroffenen* genähert. Jedoch hat in den letzten Jahren die Forschung zur sogenannten *Interdependenten Privatheit* deutlich zugenommen (Biczók und Chia 2013; Pu und Grossklags 2015). Dieser Perspektivenwechsel basiert auf technischen Entwicklungen, die dazu geführt haben, dass persönliche Informationen zunehmend miteinander vernetzt sind (Marwick und Boyd 2014). Vielmehr können Entscheidungen eines Individuums die Privatheit eines anderen gefährden (Biczók

und Chia 2013), da es in einer vernetzten Welt zunehmend schwieriger wird, persönliche Daten zu kontrollieren, die online preisgegeben oder mit anderen geteilt werden (James et al. 2017). Sendet etwa ein Nutzer Bilder oder Videos über den Kurznachrichtendienst WhatsApp an andere, werden diese Daten per Standardeinstellung der Applikation auf dem mobilen Gerät des Empfängers gespeichert (WhatsApp 2017). Nutzer können persönliche Daten von Dritten mit (1) einer großen Anzahl an anderen Nutzern (z.B. bei der Nutzung von Sozialen Netzwerken) teilen und (2) mit einem Klick große Mengen an persönlichen Daten Dritter teilen (z.B. bei der Installation von Apps). Aus diesem Grund hat sich die Privatheitsforschung von dem Untersuchungsgegenstand der persönlichen Privatheit hin zu einem differenzierten Spektrum von Konzeptualisierungen weiterentwickelt (James et al. 2017). Forscher aus verschiedenen Fachbereichen haben Konzepte vorgeschlagen, um die Idee von Privatheit auf einer interpersonellen Ebene abzubilden (Jia und Xu 2016; Koohikamali et al. 2017; Pu und Grossklags 2015). Zu diesen neuen Konzepten zählen zum Beispiel die Konzepte der *vernetzten Privatheit* (Boyd 2012), *kollektive* (Jia und Xu 2016) und *interpersonelle Privatheitsbedenken* (Shi et al. 2012).

3.2 Privatheit im Kontext der fortschreitenden Digitalisierung

Durch den Einsatz digitaler Technologien wird Privatheit, wie wir sie bisher kennen, zunehmend in Frage gestellt. Dies ist der Fall, da zum einen immer mehr Nutzerdaten automatisiert generiert und gesammelt und zum anderen die Analysemöglichkeiten dafür deutlich verbessert wurden. So trägt die Verbreitung von mobilen Endgeräten wesentlich zur Zunahme an Nutzerdaten bei. Zum Beispiel tauschen Nutzer auf Sozialen Netzwerken (z.B. Facebook oder Snapchat) Informationen aus, um mit anderen Nutzern sozial zu interagieren. Alleine auf der Plattform Snapchat, einer mobilen Chat-App, versenden Nutzer täglich mehr als eine Million Fotos (Aslam 2017). Über andere Dienste, wie den Facebook Messenger und WhatsApp, werden täglich mehr als 60 Milliarden Nachrichten verschickt (Goode 2016). Es wird immer alltäglicher, unterschiedliche Lebensbereiche online zu verwalten. Beispielsweise tätigen Nutzer immer häufiger Einkäufe online (sog. E-Commerce) und verwalten ihre Gesundheitsdaten zunehmend elektronisch (sog. E-Health). Bei der Nutzung von Online-Diensten, wie Suchmaschinen, Sozialen Netzwerken und Kommunikationsdiensten, hinterlassen Verbraucher jedoch persönliche Datenspuren (Hess und Scheiner 2012). Dadurch wächst das Gesamtvolumen der einer Person zurechenbaren Daten (die sogenannten personenbezogenen Daten) sehr stark an.

Informationspreisgabe kann freiwillig oder obligatorisch erfolgen. Individuen geben ihre persönlichen Daten zum einen auf freiwilliger Basis preis, etwa bei der Verwendung von Online-Diensten (z.B. Soziale Netzwerke). Andererseits können Individuen und ihr Nutzungsverhalten (z.B. Suchanfragen oder Kaufintentionen) im Internet auch über einzelne Websites hinaus nachverfolgt werden (Stichwort: Tracking) — und geben somit unfreiwillig ihre persönlichen Daten preis. Hierzu werden unterschiedliche Verfahren zur webseitenübergreifenden Identifikation eingesetzt, wie etwa klassische HTTP-Cookies oder auch neuere Methoden wie das sogenannte Browser-Fingerprinting.

Zusätzlich werden auch unabhängig von der aktiven Internetnutzung digitale Daten durch Tracking erhoben, z.B. durch Werbe-IDs im Kontext von mobilen Endgeräten und Applikationen (Bründl et al. 2015).

Diese Zunahme an Daten wird von technologischen Fortschritten getrieben, wie z.B. der Anstieg der verfügbaren Rechenleistung, der Kapazitäten zur Datenspeicherung sowie der Bandbreite von Netzwerken, welche zu neuen Möglichkeiten der Speicherung, Aggregation, Verknüpfung und Analyse von Daten führen. Die gesammelten Daten werden dann etwa mittels Data Mining und Machine Learning Methoden ausgewertet. So werden dann beispielsweise personenbezogene Daten (z.B. Geschlecht, Alter, Einkommen, Interessen) extrahiert und daraus Nutzerprofile abgeleitet. Dabei hilft, dass personenbezogene Daten immer stärker miteinander vernetzt sind. So sehen sich Nutzer Entscheidungssituationen gegenüber, bei denen sie nicht nur über die Preisgabe eigener Daten entscheiden (müssen), sondern auch Daten von Dritten preisgeben (Biczók und Chia 2013). So müssen Nutzer etwa bei der Installation von Apps häufig ihre Kontaktlisten preisgeben, um die App überhaupt erst nutzen zu können (Pu und Grossklags 2015). Mit dieser Preisgabe können Nutzer die Privatheit Dritter (ungewollt) gefährden. Anbieter wiederum können diese Daten nutzen und auf Basis von Machine Learning Algorithmen Rückschlüsse auf andere Individuen, deren Verhaltensweisen und Interessen ziehen (Boyd 2012). Ein anderes Beispiel für die Interkonnektivität der Privatheit ist die Nutzung von sozialen Netzwerken. Hier teilen Nutzer beispielsweise häufig Bilder, Videos oder Standortdaten, die Informationen von Dritten beinhalten (Olteanu et al. 2016).

Digitale Technologien sind damit *Enabler* neuer Möglichkeiten der Beschaffung und Verarbeitung personenbezogener Daten und somit der Fähigkeit des Anbieters, personenbezogene Daten zu kontrollieren. Daneben liefern digitale Technologien aber auch diverse Ansatzpunkte um die Fähigkeit zur Kontrolle für Individuen wiederherzustellen. Typische Beispiele für *Privacy Enhancing Technologies* sind beispielsweise Cookie-Blocker oder Verschlüsselungen, die eine anonymisierte Kommunikation ermöglichen.

4 Forschungsstrang 1: die Konsumentenperspektive

Innerhalb der Konsumentenperspektive lassen sich vier Teilaspekte identifizieren: die Privatheitsbedenken, das Privatheitskalkül, das Privatheitsparadox und die Zahlungsbereitschaft für Privatheit. In den folgenden Abschnitten folgt eine detaillierte Darstellung dieser Teilaspekte.

4.1 Privatheitsbedenken

Da das Konzept *Privatheit* ein latentes Konzept darstellt und daher nicht direkt gemessen werden kann, wird in der Literatur häufig das Konzept der *Privatheitsbedenken* (engl: Privacy Concerns) stellvertretend für Privatheit verwendet (Smith et al. 2011). In den letzten Jahren wurde das Konzept der Privatheitsbedenken zu einem zentralen Forschungsgegenstand. Privatheitsbedenken sind eines der wichtigsten Konzepte in der Privatheitsforschung, nicht nur in den WiWi, sondern auch in

anderen Disziplinen wie der Psychologie und den Kommunikationswissenschaften (Dinev et al. 2015). Sie spielen eine wichtige Rolle bei Privatheitsentscheidungen von Individuen, da sie einen Einfluss auf die Verhaltensabsichten und das tatsächliche Verhalten haben (Ajzen 1991). Die Forschung hat sich intensiv mit der Erfassung und den Konsequenzen von Privatheitsbedenken befasst (Smith et al. 2011). Die bisherigen Studien konzentrierten sich daher auf die Privatheitsbedenken als abhängige (Xu et al. 2008), moderierende (Bansal et al. 2016) und als unabhängige Variable (Dinev und Hart 2006).

Trotz verschiedener Bestrebungen um die Vereinheitlichung des Konzepts werden auch weiterhin unterschiedliche Definitionen, Konzeptualisierungen und Messmethoden angewandt. In der Literatur herrscht jedoch zumindest Konsens darüber, dass Privatheitsbedenken ein multidimensionales Konstrukt sind (Hong und Thong 2013). Zwei Konzeptualisierungen werden dabei besonders häufig herangezogen. Zum einen die *Concerns for Information Privacy*-Skala nach Smith et al. (1996) und zum anderen die *Internet User Information Privacy Concerns*-Skala nach Malhotra et al. (2004). Das Messinstrument von Smith et al. (1996) beschreibt die individuellen Bedenken darüber, dass (1) eine große Menge an persönlichen Daten gesammelt wird, (2) persönliche Daten fehlerhaft sind, (3) Anbieter, die Daten sammeln, diese für heimliche Zwecke nutzen, und (4) Anbieter daran scheitern, persönliche Daten zu schützen. Die Skala von Malhotra et al. (2004) basiert auf dieser Konzeptualisierung und überträgt das Konstrukt auf den Online-Kontext. Das Instrument umfasst insgesamt drei Dimensionen: (1) Sammlung, (2) Kontrolle und (3) Bewusstsein.

Zahlreiche Studien in den WiWi haben das Konzept der Privatheitsbedenken in unterschiedlichen Kontexten angewandt, wie etwa im Bereich Marketing, E-Commerce, E-Health und Soziale Netzwerke (Anderson und Agarwal 2011; Jia und Xu 2016; Malhotra et al. 2004). Studien zur Privatheit haben das Konzept vorwiegend verwendet, um zu untersuchen, ob Individuen Bedenken gegenüber Website-Anbietern haben, deren Praktiken ihre Privatheit einschränken könnten. Diese Studien haben u.a. nachgewiesen, dass die Privatheitsbedenken die Absicht der Nutzer beeinflussen, persönliche Daten preiszugeben, E-Commerce-Transaktionen durchzuführen, sowie personalisierte und standortbezogene Internetdienste zu nutzen. In ihrer Studie bestätigen Xu et al. (2011a), dass es einen negativen Zusammenhang zwischen der Kontrolle über die Verbreitung von persönlichen Daten und Privatheitsbedenken gibt. Haben Individuen das Gefühl, keine Kontrolle über ihre persönlichen Daten zu haben, so erhöhen sich – nicht wirklich überraschend – ihre Privatheitsbedenken. Zudem wurde in der Literatur gezeigt, dass Privatheitsbedenken dazu führen, dass Individuen vorsichtiger mit ihren persönlichen Daten umgehen. So haben etwa Son und Kim (2008) festgestellt, dass Nutzer, die sich Sorgen über einen möglichen Informationsmissbrauch machen, bei Online-Transaktionen häufiger ihre persönlichen Daten zurückhalten. Ebenso untersuchten Stewart und Segars (2002) die Privatheitsbedenken im Kontext von Direktmarketing. Die Autoren stellten fest, dass Verbraucher sich weigerten, ihre Finanzinformationen an

Versicherungsgesellschaften preiszugeben, wenn sie Bedenken darüber haben, wie Anbieter mit ihren Informationen umgehen könnten.

Schränken Verbraucher ihre Nutzung von Online-Diensten aufgrund von Privatheitsbedenken ein oder beenden die Nutzung der Dienste gänzlich, so gefährden sie damit unter Umständen sogar den Erfolg des Unternehmens (Krasnova et al. 2010). Beispielsweise sind Anbieter von Sozialen Netzwerken davon abhängig, dass Nutzer möglichst viele und persönliche Daten von sich teilen. Werden die Nutzer zunehmend passiv oder löschen ggf. sogar ihr Nutzerkonto, so ist das Erlösmodell vieler Plattformanbieter gefährdet. Ein Verständnis darüber, was bei Nutzern Bedenken auslöst und Lösungsansätze, wie man diese als Unternehmen adressieren kann oder privatheitsfreundliche Funktionen bzw. Dienste entwickeln kann, bietet neue Möglichkeiten für Erlösmodelle. Diese können letztlich die Akzeptanz und Nutzung von Diensten und Plattformen erhöhen (Schreiner 2016).

4.2 Das Privatheitskalkül

Ein weiterer wesentlicher Teilaspekt in den Wirtschaftswissenschaften bildet das sogenannte *Privatheitskalkül*. Laufer und Wolfe (1977) haben den Ansatz des Privatheitskalküls unter dem Begriff *Privacy Calculu*s in der Privatheitsliteratur eingeführt und beschreiben diesen als den bewussten kognitiven Prozess, der die Entscheidung der Informationspreisgabe erklärt.

Das Privatheitskalkül basiert auf dem ökonomischen Ansatz der Kosten-Nutzen-Analyse (Hann et al. 2002) und hat in der Privatheitsforschung vielfach Anwendung gefunden. In den WiWi ist die Kosten-Nutzen-Analyse ein fest etablierter Ansatz zur Erklärung von individuellem Entscheidungsverhalten. Das Privatheitskalkül folgt dieser ökonomischen Sicht (Pavlou 2011). Häufig wird das Privatheitskalkül daher in Verbindung mit ökonomischen Theorien wie der Nutzenmaximierungstheorie und der Erwartungswert-Theorie angewandt (Li 2012). Li argumentiert, dass das Privatheitskalkül als ein privatheitsspezifisches Beispiel von ökonomischen Entscheidungsfindungstheorien angesehen werden kann (Awad und Krishnan 2006, Rust et al. 2002). Die Erwartungswert-Theorie besagt, dass Individuen Informationen über verschiedene Aspekte jeder Wahl-Möglichkeit sammeln und jedem dieser Aspekte einen Wert zuordnen (Ajzen und Fishbein 1975). Nutzenmaximierung wiederum beschreibt, dass Individuen die verschiedenen Aspekte gegeneinander abwägen und dann die Option wählen, die ihren Nutzen maximiert (Mas-Colell 1995). Es wird davon ausgegangen, dass Individuen eine bewusste Entscheidung über eine Informationspreisgabe treffen. Der Ansatz beschreibt, dass Individuen eine Kosten-Nutzen-Analyse durchführen und dabei Privatheitsbedenken als Nachteile interpretieren, welche sie gegenüber möglichen Vorteilen einer Informationspreisgabe abwägen. Mit anderen Worten wägen Individuen einen möglichen Verlust der Privatheit gegen einen potentiellen Nutzen, der mit der Informationspreisgabe einhergeht, ab. Überwiegt der wahrgenommene Nutzen, so entscheidet sich das Individuum zur Informationspreisgabe (Chellappa und Sin 2005).

Individuen bewerten insbesondere dann ihre persönlichen Daten als wertvoll, wenn sie sich bewusst sind, dass Dritte daran interessiert sind (Spiekermann 2012). Häufig sind sie aber bereit, etwas von ihrer Privatheit aufzugeben, um monetäre Vorteile zu erhalten, wie Rabatte oder Coupons (Caudill und Murphy 2000). Beispielsweise „tauschen" Nutzer bei der Verwendung von Online-Diensten ihre persönlichen Daten gegen die kostenlose Nutzung des Dienstes (Wenninger et al. 2012). Ein anderer Vorteil ist die Personalisierung von Diensten und Produkten. Chellappa und Sin (2005) beschreiben Personalisierung als „die Anpassung von Produkten und des Einkaufserlebnisses an die Interessen der Konsumenten, basierend auf deren persönlichen Informationen und Präferenzen" (Chellappa und Sin 2005, S. 181). Für Nutzer entsteht dadurch ein Mehrwert. So können etwa personalisierte Content-Dienste den sog. „Information Overload" verringern und somit die Benutzerzufriedenheit steigern (Liang et al. 2006). Jedoch erfordert die Personalisierung von Angeboten und Produkten, dass die Nutzer ihre persönlichen Daten preisgeben.

Das Privatheitskalkül wurde ausführlich in verschiedenen Kontexten untersucht, etwa im E-Commerce (Dinev und Hart 2006), bei mobilen Apps (Xu et al. 2009) und der Nutzung von Sozialen Netzwerken (Wilson et al. 2014). Zum Beispiel stellen Dinev und Hart (2006) ein erweitertes Privatheitskalkül für Online-Transaktionen vor. Im Kontext von Personalisierung schlagen Chellappa und Sin (2005) ein Forschungsmodell vor, das die Nutzung der Online-Personalisierung durch die Kompatibilität zwischen dem Wert für die Personalisierung und Privatheitsbedenken voraussagt. Ein weiterer Strang der Privatheitskalkül-Literatur konzentriert sich auf Soziale Netzwerke. So haben etwa Krasnova et al. (2012) die Rolle der Kultur bei der Entscheidung, persönliche Daten auf sozialen Netzwerken preiszugeben, untersucht. Sipior et al. (2013) haben das Calculus-Modell von Dinev und Hart (2006) erweitert und auf den Sozialen Netzwerk-Kontext adaptiert. Damit haben sie Informationspreisgabeverhalten auf Sozialen Netzwerken erklärt. Xu et al. (2009) haben das Privatheitskalkül im Kontext von standortbezogenen Diensten untersucht und herausgefunden, dass Nutzer zwischen Privatheitsbedenken und monetären Anreizen abwägen, wenn sie darüber entscheiden, einen standortbezogenen Dienst zu nutzen. Während Privatheitsbedenken sie von der Nutzung abhalten können und einen negativen Einfluss auf die Verhaltensabsicht zeigen, so wirken sich monetäre Anreize positiv auf die Entscheidung der Nutzer aus. Ebenfalls auf Basis des Privatheitskalküls haben Milne und Gordon (1993) festgestellt, dass auch im Kontext von Direktmarketing ein Privatheitskalkül zugrunde liegt und dabei das potentielle Risiko einer Informationspreisgabe gegenüber der Höhe der Entschädigung, also den Nutzen, abgewogen wird.

Die Privatheitsforschung hat privatheitsbezogene Entscheidungen lange vorrangig als einen rationalen Entscheidungsprozess verstanden, der von einer kognitiven Bewertung der (1) angenommenen Kosten und (2) wahrgenommenen Vorteile, die mit der Preisgabe persönlicher Daten einhergehen, ausgeht (Culnan und Armstrong 1999; Dinev und Hart 2006). Typischerweise ist die Literatur also davon ausgegangen, dass Individuen eine rationale Abwägung zwischen Risiken und

Vorteilen treffen, wenn sie mit einer Entscheidung über die Preisgabe persönlicher Informationen konfrontiert sind (Malhotra et al. 2004; Xu et al. 2009) wie etwa bei der Durchführung von internetbasierten Transaktionen (Pavlou und Gefen 2004). Jedoch hat die entscheidungstheoretische Forschung in den WiWi in den letzten Jahren verstärkt gezeigt, dass nicht immer ein rationales Kalkül vorliegt, sondern Individuen in bestimmten Situationen irrationale Entscheidungen treffen, etwa in Situationen mit Unsicherheit, asymmetrischer Informationen oder bei Vorliegen von Heuristiken (Acquisti et al. 2016). Eine wachsende Anzahl an Studien argumentiert, dass die rationalen Überlegungen des Privatsphärekalküls durch psychologische Beschränkungen begrenzt sein könnten, etwa durch die Unfähigkeit alle relevanten Informationen zu verarbeiten (Acquisti 2009; Acquisti und Grossklags 2005) oder durch die stärkere Gewichtung sofortiger Vorteile gegenüber langfristig auftretender negativer Konsequenzen (Acquisti 2004; Wilson und Valacich 2012). Zudem wurde gezeigt, dass Emotionen und die Stimmung einen wesentlichen Einfluss auf das Privatheitskalkül und schlussendlich auf die Informationspreisgabe haben (Kehr et al. 2015).

4.3 Das Privatheitsparadox

Ein weiteres wesentliches Themenfeld in der Privatsphäreforschung ist das sogenannte *Privatheitsparadox*. Dieses beschreibt, dass das individuelle Informationspreisgabeverhalten nicht unbedingt den geäußerten Absichten entspricht (Norberg et al. 2007). So geben Individuen etwa häufig deutlich mehr persönliche Daten an Vermarkter und Anbieter preis als sie es in ihren Absichten geäußert haben. Aus dieser Beobachtung haben Forscher abgeleitet, dass Verhaltensabsichten in Bezug auf die Privatheit nicht immer ein genauer Prädiktor des tatsächlichen Verhaltens sind (Norberg et al. 2007).

Das Privatheitsparadox wurde ebenfalls in verschiedenen Kontexten untersucht. So wurde das Paradox etwa im Kontext von E-Commerce (Beresford et al. 2012), mobilen Apps (Sutanto et al. 2013), und Sozialen Netzwerken (Alashoor und Baskerville 2015) untersucht. Im E-Commerce Kontext haben etwa Beresford et al. (2012) gezeigt, dass Kunden von Online-Shops trotz Privatheitsrisiken nicht dazu bereit sind, für den Erhalt ihrer Privatheit zu bezahlen.

Zahlreiche Studien haben sich auch auf das sogenannte Privatheitsparadox im Kontext von Personalisierung konzentriert. Hierbei wurde untersucht, inwieweit Nutzer trotz Privatheitsrisiken für den Erhalt von Personalisierungsvorteilen ihre persönlichen Daten an Online-Anbieter preisgeben (Awad und Krishnan 2006; Sheng et al. 2008; Sutanto et al. 2013). Sutanto et al. (2013) haben das Paradox etwa im Kontext mobiler Apps untersucht. Als Ergebnis ihrer Studie schlagen sie eine sogenannte „personalisierte, privatheitssichere App“ vor, welche Daten lokal auf dem Smartphone des Nutzers speichert und verarbeitet, diese aber nicht an Vermarkter weiterleitet, so dass zwar personalisierte Produktinformationen (Werbung) bereitgestellt werden können, jedoch ohne die Privatheit der Nutzer zu gefährden (Sutanto et al. 2013, S. 1143).

Auch im Kontext von Sozialen Netzwerken wurde das Paradox untersucht, da Nutzer Sozialer Netzwerke, wie etwa Facebook oder Instagram, freiwillig große Mengen an persönlichen Informationen preisgeben. So zeigen etwa Gross und Acquisti (2005), dass Facebooknutzer trotz bestehender Privatheitsrisiken freiwillig große Mengen an persönlichen Daten auf der Plattform preisgeben, wohingegen restriktive Privatheitseinstellungen kaum genutzt werden. Die meisten Nutzer verbleiben bei den Standard-Privatheitseinstellungen, die von Facebook voreingestellt sind. Alashoor und Baskerville (2015) haben in ihrer Studie kognitive Absorption als eine Erklärung für das Privatheitsparadox auf Sozialen Netzwerken identifiziert. In ihrer Studie zeigen sie, dass durch kognitive Absorption die wahrgenommenen Vorteile einer Informationspreisgabe gegenüber den Privatheitsrisiken deutlich verstärkt werden und somit Nutzer eher gewillt sind, persönliche Daten auf der Plattform preiszugeben.

Das Privatheitsparadox lässt sich aus psychologischer Sicht weitgehend erklären (Acquisti und Grossklags 2005). Individuen unterschätzen häufig langfristige Risiken, wenn die Aussicht auf kurzfristige Vorteile besteht (Acquisti und Grossklags 2005). Vorteile werden folglich häufig überschätzt und ihr Einfluss wiegt stärker auf die Entscheidung als mögliche Risiken (Lee et al. 2011). Yoo et al (2012) haben gezeigt, dass wenn Individuen Privatheitsverletzungen ohne tatsächlichen Schaden erlebt haben, dies auch die wahrgenommene Wahrscheinlichkeit für einen tatsächlichen Schaden reduziert.

4.4 Zahlungsbereitschaft für Privatheit

Jentzsch (2014) definiert den Begriff der Monetarisierung der Privatheit als „die Kompensation für den Verzicht auf Privatheit, also die Preisgabe von persönlichen Informationen gegen Bezahlung“ (Jentzsch 2014, S. 793). Unternehmen versuchen mit unterschiedlichen Mitteln Kunden dazu zu bewegen, persönliche Informationen von sich preiszugeben, sei es über Rabatte oder die kostenlose Nutzung von Online-Angeboten. Aus praktischer Sicht ist dieser Austausch von Daten gegen persönliche Vorteile von großer Bedeutung für Anbieter. Jedoch ist das Entscheidungsverhalten der Individuen sehr komplex und die bisherige Forschung zeigt auf, dass der Wert der Privatheit sehr stark kontextspezifisch ist (Acquisti et al. 2016; Nissenbaum 2009).

In den WiWi ist das Themenfeld Zahlungsbereitschaft für Privatheit ein wesentlicher Teilaspekt. Zum einen soll ein besseres Verständnis geschaffen werden, wie Anbieter Privatheit monetarisieren können und ebenso über das Verhalten und Präferenzen der Nutzer. Ein wichtiges Ziel in diesem Feld ist es, ein möglichst wahrheitsgetreues Bild vom Wert der Privatheit zu ermitteln (Jentzsch 2014). Aus einer marktorientierten Perspektive würde dies auf Basis von Angebot und Nachfrage abzuleiten sein, was zu einer effizienten Allokation von persönlichen Informationen, also der Preisgabe von Informationen gegenüber Unternehmen führen sollte. Aufgrund von Externalitäten ist dies in der Realität jedoch so nicht umzusetzen (Jentzsch 2014).

In diesem Bereich befassen sich Forscher mit der Fragestellung, welchen (monetären) Wert Individuen ihrer Privatheit zuordnen und unter welchen Bedingungen sie bereit sind, für ihre Privatheit etwas zu bezahlen. Im Wesentlichen zeigen auch hier die Studien, dass die Bewertung von Privatheit stark kontextabhängig ist (Acquisti 2010). Egelmann et al. (2013) haben in ihrer Studie zwei Experimente durchgeführt, um zu untersuchen, welche Zahlungsbereitschaft für Privatheit Nutzer bei der Installation neuer Apps haben. Für die Experimente wurden drei Arten von Zugriffserlaubnissen variiert: Internetzugang, GPS-Daten, Audiodaten. Die Autoren fanden heraus, dass Nutzer bei der Wahl zwischen verschiedenen Apps mit ähnlichen Funktionalitäten bereit sind, 1,50 US-Dollar für die App zu bezahlen, die am wenigsten Zugriffserlaubnisse anfordert. Dieses Ergebnis liegt jedoch der Bedingung zugrunde, dass die Teilnehmer die verschiedenen Erlaubnisanfragen jeder App miteinander vergleichen können. Die Autoren kommen zu dem Schluss, dass viele Smartphonenutzer um ihre Privatheit besorgt und bereit sind, einen Aufschlag für Apps zu bezahlen, die weniger persönliche Daten anfordern. Die Autoren schlagen Verbesserungen im Aufbau der Wahl für Apps vor, die es erlauben, dass Nutzer Zugriffserlaubnisanfragen von ähnlichen Apps besser vergleichen können, da dies privatheitsschützendes Verhalten motiviert.

Huberman et al. (2005) haben eine „Second-Price“ Auktion angewandt, um den Preis zu ermitteln, bei dem Individuen bereit sind, persönliche Informationen (z.B. ihr Gewicht) öffentlich preiszugeben. Haben Individuen das Gefühl, das ihre Informationen weniger erstrebenswert sind und von der Norm der restlichen Gruppe abweichen, bewerten sie ihre Informationen höher. Wathieu und Friedman (2005) stellten fest, dass Umfrageteilnehmer es eher akzeptieren, dass eine Organisation ihre persönlichen Daten teilt, wenn das Unternehmen zuvor den wirtschaftlichen Nutzen dafür erklärt hat. Hann et al. (2007) konzentrierten sich in ihrer Studie auf Online-Privatheit. Auf Basis einer Conjoint-Analyse fanden sie heraus, dass der Schutz vor Fehlern, unsachgemäßen Zugriff und sekundäre Nutzung von persönlichen Informationen für US-Teilnehmer einen Wert zwischen 30,49 und 44,62 US-Dollar hat. Ebenfalls auf Basis einer Conjoint-Analyse haben Pu und Grossklags (2015) im Kontext der Adoption von Social Apps untersucht, welchen monetären Wert Technologienutzer den persönlichen Informationen ihrer Freunde zuordnen. Die Autoren kommen zu dem Schluss, dass die Privatheit der Freude für Nutzer den drittwichtigsten Faktor darstellt. Nutzer bewerten die vollständigen Profilinformationen ihrer Freunde mit 1,56 US-Dollar, wenn die Informationen relevant für die Funktionalität der App sind bzw. mit 0,98 US-Dollar, wenn sie es nicht sind. Schreiner und Hess (2015) konnten zudem zeigen, dass Facebook-Nutzer bereit sind, auf Basis eines Freemium-Modells für den Erhalt der Privatheit zu bezahlen. Voraussetzung hierfür ist jedoch, dass die Nutzer die Premium-Version als wertsteigernd und vertrauenswürdig bewerten. Im Kontext von Telemarketing haben Varian et al. (2005) sowie Png (2007) untersucht, inwieweit sich US-Konsumenten vor Telemarketing schützen. Dafür haben sie Daten der sogenannten „Do Not Call“-Liste herangezogen. Diese Liste umfasst eine Datenbank mit Haushalten, die darum gebeten haben,

nicht von Telemarketern kontaktiert zu werden. Die beiden Studien zeigen jedoch sehr unterschiedliche Werte, die zwischen wenigen Cents und bis zu 30 US-Dollar reichen. Schließlich haben Tsai et al. (2011) festgestellt, dass Teilnehmer eher bereit sind, einen Preisaufschlag von etwa 0,50 US-Dollar zu bezahlen, um bei einem privatheitsfreundlicheren Verkäufer einzukaufen, wenn die Informationen über Datenschutzregelungen auf eine kompakte und markante Art zugänglich sind.

Es wird deutlich, dass eine monetäre Bewertung der Privatheit bisher nicht zu einheitlichen Ergebnissen geführt hat. Konkrete Hinweise für die Praxis, etwa zur Preisgestaltung von Online-Anbietern, lassen sich bisher daher nicht ableiten. Jentzsch (2014) stellt etwa in Frage, ob es bisher überhaupt robuste Methoden gibt, um den ökonomischen Wert von Daten zu erheben. Frik und Gaudeul (2016) kritisieren ebenfalls die klassischen Ansätze zur Messung der Zahlungsbereitschaft für Privatheit. Sie argumentieren, dass die Abfrage der Zahlungsbereitschaft über Experimente und Umfragen nicht den realen Entscheidungssituationen entsprechen und somit zu verzerrten Ergebnissen führen (Frik und Gaudeul 2016, S. 2). In einem Laborexperiment baten die Autoren stattdessen Teilnehmer, einen Fragebogen zu kontroversen, heiklen sowie sozial relevanten Themen zu beantworten. Anschließend nahmen die Teilnehmer an einem Experiment teil, in welchem Risikoeinstellungen und die Bereitschaft an einer Privatheits-Lotterie teilzunehmen untersucht wurden. Die Autoren zeigen, dass die Entscheidung, Privatheitsrisiken einzugehen mit der Entscheidung, monetäre Risiken einzugehen, korreliert. Der mittlere implizite monetäre Wert von Privatheit ist in etwa gleich zur durchschnittlichen Zahlungsbereitschaft für den Schutz von privater Information, jedoch korrelieren diese zwei Maße nicht auf einem individuellen Level. Sie zeigen, dass wenn man den Teilnehmern teilweise die Kontrolle über die Preisgabe persönlicher Informationen entzieht, dies nicht dazu führt, dass sie das Interesse am Schutz der persönlichen Informationen verlieren. Die Autoren zeigen auch, dass die Aversion vor Privatheitsrisiken reduziert wird, wenn die Teilnehmer nach finanziellen Entscheidungen über Privatheitsentscheidungen nachdenken sollen (Frik und Gaudeul 2016). Feri et al. (2016) argumentieren, dass für Nutzer die ökonomische Bewertung der Informationspreisgabe kontextabhängig sei und nicht einer nutzenmaximierenden Entscheidung unter vollständigen Informationen sondern eher einer riskanten Lotterie gleiche.

5 Forschungsstrang 2: die Anbieterperspektive

Die Literatur aus Anbieterperspektive befasst sich im Wesentlichen damit, wie Unternehmen persönliche Daten der Kunden verwenden und davon profitieren können, sei es durch die Personalisierung von Werbung und Produkten bis hin zu neuen Erlös- und Geschäftsmodellen (Hess und Scheiner 2012; Tucker 2014). Unternehmen können heutzutage Daten in den verschiedensten Kotexten und für unterschiedlichste Zwecke sammeln und analysieren. Wichtige Verwendungszwecke sind die Verwertung von Daten für Angebote, für eine verbesserte Preisdiskriminierung, für

den Verkauf personenbezogener Daten sowie die Verwertung von persönlichen Informationen durch Arbeitgeber (Cecere et al. 2017). Auf diese vier Themenfelder gehen wir im Folgenden näher ein.

5.1 Personalisierte Ansprache durch personenbezogene Daten

Die Idee einer personalisierten Ansprache besteht nicht erst seit es das Internet gibt. Jedoch haben es die Fortschritte in der IT möglich gemacht, Konsumenten mit wirksamen und nützlichen individuellen Produkt- und Dienstempfehlungen zu versorgen (Li und Unger 2012, S. 623) bzw. sogar die Produkte und Dienste selber anzupassen. Auf Basis von Konsumentendaten können Unternehmen Verhaltensweisen und Präferenzen erkennen und so ihr Angebote entsprechend personalisieren.

Die Personalisierungsforschung hat sich mit einer großen Bandbreite an unterschiedlichen Themen beschäftigt. Unternehmen möchten möglichst viele Daten auswerten, um ihre Kunden bestmöglich zu verstehen und optimal anzusprechen. Kunden wissen die Vorteile häufig zu schätzen, verspüren jedoch Privatheitsbedenken aufgrund der personalisierten Angebote, die auf Basis einer Analyse ihrer persönlichen Daten erst zustande gekommen sind. Im Forschungsfeld der Personalisierung wird daher häufig auch der Begriff „Personalization Privacy Paradox“ verwendet (z.B. Sutanto et al. 2013, Xu et al. 2011). Dieser Begriff beschreibt die Spannung zwischen Vorteilen für Nutzer durch die Personalisierung von Produkten und Dienstleistungen einerseits und den Privatheitsbedenken andererseits (Sutanto 2013) — wie wir sie auch schon aus dem Privatheitskalkül kennen.

Fühlen sich Konsumenten für die Preisgabe ihrer persönlichen Informationen ausreichend entlohnt, sind sie — dieser Logik entsprechend — eher bereit, persönliche Informationen offenzulegen (Rayna et al. 2015). Acquisti und Varian (2005) zeigen beispielsweise, dass verbesserte personalisierte Dienste Konsumenten dazu veranlassen können, persönliche Informationen preiszugeben. Auch die Reputation des Unternehmens ist wesentlich, damit Konsumenten dazu bereit sind, persönliche Daten, die dann für Personalisierungszwecke herangezogen werden, überhaupt erst preiszugeben. Die Forschung untersucht daher, unter welchen Bedingungen und zu welchem Grad Unternehmen Personalisierungssysteme einsetzen können, sodass Privatheitsbedenken der Konsumenten die möglichen Vorteile nicht überwiegen bzw. Konsumenten die Personalisierungssysteme akzeptieren. Je mehr Konsumenten einem Unternehmen vertrauen, desto eher sind sie bereit, persönliche Informationen zu teilen (Chellappa und Sin 2005). Auf Basis eines theoretischen Modells haben beispielsweise Chellappa und Sin (2005) untersucht, ob Konsumenten Online-Personalisierungs-angebote nutzen. Das Modell basiert auf einem Trade-Off-Ansatz, also einem Privatheitskalkül, bei dem Konsumenten die Vorteile der Personalisierung gegenüber ihren Privatheitsbedenken abwägen. Die Autoren zeigen, dass sich das Vertrauen der Konsumenten in den Anbieter positiv auf die Intention der Konsumenten auswirkt, Personalisierungsdienste des Anbieters zu nutzen. Die Autoren schlagen vor, dass Online-Anbieter vertrauensbildende Maßnahmen umsetzen sollten, um Konsumentendaten entsprechend sammeln und nutzen zu können. Anbieter sollten zudem

verstehen, welchen Wert Konsumenten auf unterschiedliche Arten von Personalisierung legen (Chellappa und Sin 2005, S. 181), um die Konsumenten adäquat zu adressieren.

Eine andere Lösung zur Steigerung der Akzeptanz schlagen Lee et al. (2011) vor. In ihrer Studie zeigen sie, dass Unternehmen die Privatheit der Konsumenten schützen und Privatheitsbedenken reduzieren können, indem sie faire Informationspraktiken implementieren. So kann zum Beispiel eine Reihe an Standards, die die Sammlung und die Nutzung von persönlichen Informationen regulieren, dabei helfen, Privatheitsbedenken auf Seiten der Konsumenten zu verringern (Lee et al. 2011).

Die Studie von Awad und Krishnan (2006) widmet sich der Frage, ob die wahrgenommene Informationstransparenz mit der Bereitschaft, ein Online-Profil zu erstellen, verknüpft ist. Mit ihren Ergebnissen zeigen die Autoren das Dilemma für Unternehmen auf. Die Konsumenten, die die Informationstransparenz von Unternehmen besonders schätzen, sind weniger dazu bereit, ein Profil zu erstellen (Awad und Krishnan 2006). Auch in anderen Kontexten wurde dieses Konzept untersucht. Im Kontext von standortabhängigem Marketing haben Xu et al. (2011) auf Basis eines erweiterten Privatheitskalküls das Paradox anhand von zwei unterschiedlichen Personalisierungs-ansätzen untersucht. Die Autoren zeigen, dass der Einfluss der Personalisierung auf die wahrgenommenen Risiken und Vorteile je nach Personalisierungssystem (verdeckt vs. offen) unterschiedlich ist. Während bei ersterem das Verhalten der Nutzer durch Trackingmethoden „beobachtet“ wird und die Nutzer automatisch standortspezifische Inhalte erhalten, so werden bei letzterem nur dann Informationen an Nutzer geschickt, wenn diese Informationen anfragen (z.B. Sehenswürdigkeiten in der Umgebung). Die Autoren konnten zeigen, dass der verdeckte Ansatz dazu führt, dass die Konsumenten mehr Spontaneinkäufe tätigen. Zudem zeigen die Ergebnisse, dass beide Formen der Personalisierung Privatheitsbedenken außer Kraft setzen können. Zu einem ähnlichen Ergebnis kommen Sutanto et al. (2013), die in ihrer Studie zeigen konnten, dass eine privatheitsfreundliche App die Sorge der Nutzer vor einer Privatheitsverletzung verringern kann.

Personalisierung spielt auch bei der Werbung eine zunehmend wichtige Rolle. Für eine Reihe von Internetunternehmen sind die Erlöse aus personalisierter Werbung eine der Haupteinnahmequellen (Martin und Murphy 2017). Jedoch sind die Ergebnisse zu den Effekten von personalisierter Werbung überraschend widersprüchlich. Beispielsweise zeigt Tucker (2014) in einem Feldexperiment am Beispiel von Facebook, dass die Effektivität von Werbung steigt, wenn Individuen mehr Kontrolle über ihre persönlichen Informationen haben. In einem weiteren Feldexperiment zeigen Lambrecht und Tucker (2013) jedoch, dass dynamisches Retargeting, also Werbung mit Bildern von genau den Produkten, die Konsumenten zuvor auf einer Website angesehen haben, im Durchschnitt weniger effizient ist als generische Werbung. Haben Individuen mehr Informationen über Produkte, an denen sie interessiert sind, steigt wiederum die Wirksamkeit von dynamischen Retargeting. Goldfarb und Tucker (2011a) untersuchen in ihrer Studie die Einflussfaktoren auf die Wirksamkeit von

personalisierter Online-Werbung und zeigen auf Basis eines Feldexperiments, dass Privatheitsbedenken die Wirksamkeit von verschiedenen Online-Werbetechniken beeinflussen können. Dies deckt sich mit anderen Ergebnissen der oben bereits erwähnten WiWi-Literatur zu den Effekten von Privatheitsbedenken auf das Verhalten der Konsumenten.

5.2 Perfektionierte Preisdiskriminierung mittels personenbezogener Daten

Die enorme Menge an persönlichen Daten, die durch die Nutzung von internetbasierten Diensten und dem Surfen im Internet generiert werden, erlauben es Anbietern, die Zahlungsbereitschaft der Konsumenten präziser als bisher zu bestimmen. Diese Fähigkeit ermöglicht wiederum ein Mehr an Preisdiskriminierung. Aus Anbietersicht ist die Preisdiskriminierung von Konsumenten prinzipiell vorteilhaft. Die Verwertung von persönlichen Informationen kann Preisdiskriminierung erleichtern, da die Analyse von personenbezogenen Daten es dem Unternehmen erlaubt, den individuellen Reservationspreis zu identifizieren (Cecere et al. 2017).

In der Literatur wurden über lange Zeit Preisdiskriminierung der zweiten und dritten Ordnung besonders stark untersucht. Mit Aufkommen des Internets ist auch die Preisdiskriminierung der ersten Ordnung und damit die Anpassung an den Reservationspreis wieder in den Fokus der Aufmerksamkeit gerückt (Rayna et al. 2015). Dies liegt daran, dass es digitale Technologien nun möglich machen, präzise das Verhalten von Konsumenten zu beobachten und daraus deren Zahlungsbereitschaft abzuleiten — wenn nicht sogar genau zu bestimmen (Acquisti und Varian 2005; Taylor 2004). Während zu Beginn die Informationen noch mit Cookies gesammelt wurden (Villas-Boas 2004), ermöglichen es neuere technische Entwicklungen, wie Big Data durch die Kombination von einer großen Menge an persönlichen Daten aus unterschiedlichen Quellen, das Konsumentenverhalten und die Zahlungsbereitschaft noch genauer zu erfassen (Rayna et al. 2015). Jedoch lässt sich das nicht immer umsetzen (Rayna et al. 2015). Amazon hat auf Basis von Schätzungen der Zahlungsbereitschaft der Konsumenten unterschiedliche Preise für die gleichen Produkte verlangt. Nachdem die Konsumenten auf diese Form der Preisdiskriminierung aufmerksam geworden sind, musste Amazon die Strategie rückgängig machen, um langfristige Reputationsschäden zu vermeiden (Rayna et al. 2015). Dieses Beispiel zeigt, dass Konsumenten, die sich über Preisdiskriminierung bewusst sind, häufig nicht dazu bereit sind, diese zu akzeptieren. Als Grund hierfür lässt sich nennen, dass Konsumenten befürchten, dass sie am Ende mehr für das gleiche Produkt oder die gleiche Dienstleistung zahlen müssen (Rayna et al. 2015).

Wie das Beispiel illustriert, geht die Preisdiskriminierung — im Gegensatz zur Personalisierung — zumeist mit konkreten monetären Nachteilen für die Konsumenten einher (Acquisti et al. 2016). Belleflamme und Vergote (2016) argumentieren, dass die verbesserten Möglichkeiten für Unternehmen zur Preisdiskriminierung eine Verringerung der Konsumentenrente mit sich bringen. Da die monetären Kosten zumeist erst zu einem deutlich späteren Zeitpunkt auftreten, vernachlässigen Individuen diese Kosten häufig bei ihrer Entscheidung der Informationspreisgabe

gegenüber einem Anbieter. Zum Beispiel sammeln Anbieter persönliche Informationen über Konsumenten und verwenden diese zu einem späteren Zeitpunkt für Preisdiskriminierung, wenn diese das nächste Mal den Online-Shop besuchen (Acquisti et al. 2016, S. 6). Individuen können den Zusammenhang zwischen Nutzungsverhalten und späterer Preisdiskriminierung nur schwer — wenn überhaupt — nachvollziehen. Aufgrund dessen geben Nutzer häufig (unfreiwillig) Informationen preis, welche später in konkreten monetären Nachteilen resultieren können. Konsumenten geben häufig persönliche Informationen preis, da sie sich einen konkreten Nutzen von dem Austausch versprechen. Jedoch haben Konsumenten häufig kaum die Kontrolle darüber wie und von wem die Daten später verwendet werden (Varian 1996). Zusätzlich kann Preisdiskriminierung auch erfolgen, wenn Unternehmen persönliche Informationen der Nutzer an Dritte verkaufen, wodurch auch andere Anbieter die Preisgestaltung gegenüber einzelnen Konsumenten für diese nachteilig anpassen können (Acquisti et al. 2016). Odlyzko (2003) stellt fest, dass es für den Konflikt zwischen den Anreizen für Anbieter, die Möglichkeiten für Preisdiskriminierung zu nutzen und dem Widerstand der Käufer keine einfache Lösung gibt.

Preisdiskriminierung kann sich jedoch auch negativ für Unternehmen auswirken. Insbesondere wenn Wettbewerb zwischen Unternehmen vorliegt, haben verschiedene WiWi-Studien gezeigt, dass Preisdiskriminierung zu Nachteilen führen kann. Unter Wettbewerb führt die Anwendung von Personalisierung und Preisdiskriminierung zu einem Gefangenendilemma, in welchem alle Unternehmen letztlich benachteiligt sind (Chen et al. 2001; Choudhary et al. 2005; Dewan et al. 2003; Shaffer and Zhang 2002; Thisse and Vives 1988). Dieses Dilemma ist damit zu erklären, dass Preisflexibilität es den Unternehmen erlaubt, Konsumenten mit einem personalisierten Angebot zu adressieren. Aus dem Wettbewerb resultiert, dass Unternehmen versuchen, jeden Konsumenten für sich zu gewinnen. Dafür senken sie beispielsweise wetteifernd die Preise für die Konsumenten (Lee et al. 2011). Choudhary et al. (2005) untersuchen beispielsweise ein vertikal differenziertes Duopol und zeigen, dass das Unternehmen mit der höheren Qualität durch personalisierte Preisgestaltung benachteiligt ist. Neuere Studien in diesem Gebiet haben jedoch verschiedene Kriterien identifiziert, welche es Unternehmen erlauben, das Gefangenendilemma zu vermeiden, wie etwa Größenunterschiede zwischen den Unternehmen. Shaffer und Zhang (2002) zeigen in diesem Kontext ein Beispiel für diesen Mechanismus. Sie untersuchen die Auswirkungen von Preisdiskriminierung bei Unternehmen, die sich in der Menge der loyalen Konsumenten unterscheiden. Die Studie zeigt, dass größere Unternehmen von personalisierter Preisgestaltung profitieren können, da dies ihren Marktanteil erhöht. Dewan et al. (2003) untersuchen Preisdiskriminierung über verschiedene Perioden. Sie zeigen, dass bei der Anwendung von Preisdiskriminierung durch mehrere konkurrierende Unternehmen der Erstanwender einen Vorteil genießt und den Markteintritt von möglichen Wettbewerbern durch strategische Investitionen in die Preisdiskriminierung behindern kann. Ein anderes Kriterium ist die Marktabdeckung. Ist der Markt nicht voll abgedeckt, können

Unternehmen ihren Marktanteil erhöhen und somit die Gewinne durch Preisdiskriminierung steigern (Choudhary et al. 2005).

Preisdiskriminierung der ersten Ordnung kann sich aber auch positiv für Konsumenten auswirken. Zu diesem Ergebnis kommen Rayna et al. (2015) in ihrer Studie. Anhand eines ökonomischen Modells zeigen die Autoren, dass die Belohnung von Konsumenten für die Preisgabe von persönlichen Informationen zu einer Situation führen kann, welche für Konsumenten und Anbieter vorteilhaft ist und somit beide von der Akzeptanz eines derartigen Preismodells profitieren können. Rayna et al. (2015) argumentieren, dass die enorme Zunahme an Nutzerdaten und Möglichkeiten für deren Analyse Preisdiskriminierung der ersten Ordnung nicht nur möglich gemacht hat, sondern auch sozial wünschenswert. Die Autoren argumentieren, dass digitale Güter sich wie öffentliche Güter verhalten und somit in Marktversagen resultieren (Rayna et al. 2015). Öffentliche Güter müssen folglich entsprechend der Zahlungsbereitschaft der einzelnen Konsumenten bepreist werden, damit ökonomische Effizienz vorliegen kann (Foley 1970).

5.3 Privatheit in der Arbeitswelt

Während in den Kommunikations-, Ethik- und Rechtswissenschaften das Thema Privatheit und Informationspreisgabe im Arbeitskontext recht intensiv untersucht wurde (Allen et al. 2007; Hartman 2001), so sind es in der WiWi-Forschung noch recht wenige Studien, die sich dem Thema aus ökonomischer Sicht gewidmet haben (Acquisti und Fong 2015; Morlok et al. 2016; Schmitz 2005). Das Themenfeld Privatheit in der Arbeitswelt lässt sich in zwei Teilaspekte untergliedern: Zum einen hat die WiWi-Literatur sich mit dem Aspekt der Privatheit von Mitarbeitern in Unternehmen befasst (Lugaresi 2010; Snyder 2010). Zum anderen gibt es Studien zu dem Aspekt, dass Arbeitgeber persönliche Informationen von Bewerbern analysieren, etwa auf Sozialen Netzwerken (Acquisti und Fong 2015).

Unternehmen sind zunehmend in der Lage das Verhalten ihrer Mitarbeiter mit relativ wenig Aufwand zu beobachten. So können Unternehmen etwa spezielle Überwachungssoftware einsetzen, um die Aktivitäten der Mitarbeiter an Computern und Smartphones zu überwachen (Gürtler und Höffler 2015). Derartige Softwares können etwa ableiten, wie produktiv einzelne Mitarbeiter sind, ob diese gestresst sind oder beispielsweise während der Arbeitszeit privat im Internet surfen. Zudem lassen sich vermehrt auch die exakten Standorte der Mitarbeiter bestimmen. Diese Standortbestimmung setzen etwa Logistikunternehmen ein, um die Bewegungsmuster ihrer Mitarbeiter und das Pausenverhalten zu analysieren. In den USA ist es beispielsweise rechtlich erlaubt, dass Unternehmen die E-Mails ihrer Mitarbeiter prüfen und Büroräume mit Videoüberwachung ausstatten. Dieser zunehmende Einsatz von Überwachungstechnologien in Unternehmen, aber auch von Technologien, die für Überwachungszwecke zweckentfremdet werden können (z.B. Wearables mit GPS-Tracker), hat zu einer Debatte darüber geführt, inwieweit Arbeitgeber das Verhalten ihrer Mitarbeiter überwachen dürfen. Zudem ist eine Diskussion darüber entstanden, ob der Staat

eingreifen sollte (wenn nicht sogar muss), um die Privatheit der Mitarbeiter zu schützen. Während in den USA beispielsweise der Privatheitsschutz für Mitarbeiter eher schwach ausgeprägt ist, so ist dieser in der EU deutlich stärker verankert (Gürtler und Höffler 2015). Unabhängig von der rechtlichen Situation ergeben sich ökonomische Fragestellungen in Bezug auf die Privatheit von Mitarbeitern.

Rein ökonomisch und stark abstrahiert betrachtet wäre die Überwachung von Mitarbeitern vorteilhaft, wenn dies zu einer Steigerung der Produktivität führt (Gürtler und Höffler 2015). Andererseits stellen sich jedoch ethische und rechtliche Fragen, etwa, inwieweit Mitarbeiter ein Recht auf Privatheit am Arbeitsplatz haben. Schmitz (2005) zeigt mittels eines vertragstheoretischen Modells, dass ein Gesetz zum Schutz der Privatheit der Mitarbeiter, welches Überwachung am Arbeitsplatz verbietet, die Gesamtwohlfahrt steigern kann. Der Autor erklärt dieses Ergebnis damit, dass ein derartiges Gesetz zwar den Profit vom Arbeitgeber reduziert, dies aber durch den Zugewinn für den Arbeitnehmer überkompensiert wird. Unter dem Begriff „Informationsasymmetrien“ haben Stigler (1980) und Posner (1981) postuliert, dass das Verbergen von persönlichen Informationen zwischen Arbeitnehmer und Arbeitgeber zu Marktineffizienzen führt. Praktisch schrecken Unternehmen vor der Überwachung ihrer Mitarbeiter auch deshalb zurück, weil sie über den Arbeitsmarkt nur schwer Ersatz finden können — diese Überlegung ist in die bekannten Modelle bisher noch nicht eingeflossen.

Sipior und Ward (1996) haben bereits im Jahr 1996 eine Studie zum Thema Verletzung der E-Mail-Privatheit in Unternehmen durchgeführt. Die Autoren haben das US-amerikanische Rechtssystem analysiert und festgestellt, dass ein Schutz der E-Mail-Privatheit bis dato fehlte. Die Autoren stellen auf Basis dieser Analyse ein Framework vor, welches dabei helfen soll, mögliche rechtliche Konsequenzen unter verschiedenen Bedingungen am Arbeitsplatz zu identifizieren. Agarwal und Rodhain (2002) haben ebenfalls Privatheit im Kontext von E-Mails untersucht. Die Autoren untersuchen die Einstellungen der Mitarbeiter gegenüber E-Mails, ihre Wahrnehmungen und Erwartungen bezüglich Privatheit und Besitztum von E-Mails sowie unterschiedliche Eigenschaften des Unternehmensumfelds.

Kurkovsky und Syta (2011) haben in ihrer Studie die Überwachung von elektronischer Kommunikation an Universitäten untersucht. Die Autoren legten einen speziellen Fokus auf den Effekt von institutionellen Richtlinien bezüglich der Überwachung von elektronischer Kommunikation und einem möglichen Verlust von Privatheit und Vertrauen. Die Autoren kommen zu dem Ergebnis, dass Individuen eine inhärente Erwartung haben, dass ihre elektronische Kommunikation auf dem Gelände der Universität privat bleibt. Zudem zeigen die Ergebnisse, dass die meisten Nutzer die Auswirkungen der Richtlinien für die elektronische Überwachung ihrer Privatheit nicht verstehen. Diejenigen Nutzer, die die Richtlinien verstehen, passen entsprechend ihr Kommunikationsverhalten als Antwort auf die geminderte Privatheit an (Kurkovsky und Syta 2011).

Der zweite Teilbereich im Themenfeld von Privatheit in der Arbeitswelt befasst sich mit der Privatheit von Jobsuchenden im Arbeitsmarkt. Ein zentrales Thema ist hier die Diskriminierung von Bewerbern. Insbesondere im Arbeitsmarkt kommt es auf Basis der zur Verfügung stehenden Informationen, etwa in sozialen Netzwerken zu Diskriminierung zwischen verschiedenen Bewerbern (Acquisti und Fong 2015; Bertrand und Duflo 2017).

Die Verbreitung von sozialen Netzwerken wie Facebook, Instagram oder Snapchat, hat dazu geführt, dass eine enorme Menge an persönlichen Informationen öffentlich geteilt wird. Individuen teilen ihre sexuelle Orientierung, Glaubenszugehörigkeit, ihren Beziehungsgrad, private Interessen und tägliche Aktivitäten. Arbeitgeber haben somit auf unterschiedliche Weise Zugang zu persönlichen Informationen, die auf Sozialen Netzwerken geteilt wurden (Acquisti und Fong 2015). Wenngleich eine Suche von persönlichen Informationen über Jobkandidaten gegen kein bestehendes Gesetz verstößt, so stellen sich gleichwohl Fragen bezüglich des Schutzes der Privatheit der Bewerber (Acquisti und Fong 2015).

In ihrer Studie untersuchen Acquisti und Fong (2015), ob künftige Arbeitgeber nach persönlichen Informationen, die Jobkandidaten auf Sozialen Netzwerken posten, gezielt suchen und diese verwerten. Die Autoren haben dafür Profile von Jobkandidaten auf bekannten Sozialen Netzwerken, wie Facebook, erstellt und dabei Informationen manipuliert. Anschließend haben sie Bewerbungen an mehr als 4000 Arbeitgeber geschickt. Die Autoren kommen zu dem Ergebnis, dass Arbeitgeber auf Sozialen Netzwerken nach Jobkandidaten suchen. Während die Autoren keine Diskriminierung bei der Sexualität der Bewerber feststellen konnten, so meldeten sich bei muslimischen Kandidaten 13% weniger Unternehmen zurück als bei Christen, insbesondere in US-Bundesstaaten, die republikanisch geprägt sind, wie etwa Texas. Die Autoren konnten zeigen, dass die Wahrscheinlichkeit der Diskriminierung bei der Einstellung je nach Arbeitgeber variiert (Acquisti und Fong 2015). Eine ähnliche Studie haben Manant et al. (2014) für den französischen Arbeitsmarkt durchgeführt. Hierfür haben die Autoren reale Stellenanzeigen für Wirtschaftsprüfer im Großraum von Paris genutzt und zwei fiktive Bewerberidentitäten erstellt. Die Autoren konnten zeigen, dass allein aufgrund von Informationen zum Herkunftsland auf Sozialen Netzwerken scheinbar arabische Bewerber von Personalern benachteiligt wurden. Nur wenn Personaler die Facebook-Profile der Bewerber nicht geprüft haben, war die Wahrscheinlichkeit für beide Bewerber gleich hoch, für ein Gespräch eingeladen zu werden. Die Ergebnisse der beiden Studien zeigen, dass das Informationspreisgabeverhalten im Internet (hier am Beispiel von Sozialen Netzwerken), die Rekrutierungsentscheidung von Unternehmen beeinflussen und somit zu Diskriminierung führen kann. Lambrecht und Tucker (2016) haben zusätzlich gezeigt, dass Algorithmen von Sozialen Netzwerken Offline-Diskriminierung von Individuen und insbesondere von Frauen nachbilden. Goldin und Rouse (1997) zeigen in diesem Kontext, dass anonymes (sogenanntes blindes) Vorspielen zu fairen Einstellungsentscheidungen der Arbeitgeber führt.

6 Forschungsstrang 3: die Marktperspektive

Als dritte zentrale Perspektive in der WiWi-Forschung ist die Marktperspektive zu berücksichtigen. Aus dieser Perspektive finden sich Wohlfahrt, Datenmärkte und Regulierung als zentrale Teilaspekte. Wir stellen die in diesen Feldern gewonnenen Einsichten nachfolgend vor.

6.1 Privatheitsschutz und Wohlfahrt

Die klassische Literatur zu diesem Thema teilt sich in zwei Lager. Während die Forscher der Chicago School (Posner 1981; Stigler 1980) argumentieren, dass sich Privatheitsschutz negativ auf die Wohlfahrt auswirkt, argumentiert die andere Gruppe an Forschern für einen positiven Effekt. So argumentiert Hirshleifer (1971) zum Beispiel, dass Privatheitsschutz für die Gesamtwohlfahrt wesentlich ist, da Individuen bei der Entscheidung einer Informationspreisgabe nicht rational handeln. Der Autor stellt fest, dass Privatheitsregulierung eine effizienzsteigernde Rolle haben kann.

Aktuellere Studien kommen ebenfalls zu teilweise widersprüchlichen Ergebnissen in Bezug auf die Effekte für die Gesamtwohlfahrt. Calzolari und Pavan (2006) argumentieren etwa, dass der Austausch von persönlichen Informationen zwischen Unternehmen Informationsverzerrungen reduziert und dadurch die soziale Wohlfahrt erhöht. In ihrer Studie untersuchen sie die optimale Preisgaberichtlinie bei der Gestaltung von Verträgen für Konsumenten, die sich in einer Situation befinden, in der sie mehrfach zwischen verschiedenen Anbietern wählen können. Verschiedene Studien zeigen jedoch negative Auswirkungen von Privatheitsschutz auf die Wohlfahrt (Campbell et al. 2015).

Auf Basis eines spieltheoretischen Ansatzes haben Lee et al. (2011) im Kontext von Personalisierung untersucht, welche Motivation Unternehmen für den Schutz von Privatheit haben und welchen Einfluss dieser auf den Wettbewerb und die soziale Wohlfahrt hat. Die Autoren zeigen, dass Privatheitsschutz als Mechanismus zur Abschwächung von Wettbewerb im Markt funktionieren kann, indem er Asymmetrie in den Kundensegmenten erzeugt, denen die Unternehmen Personalisierung anbieten. Durch diesen Mechanismus erhöhen sich für Unternehmen die Möglichkeiten der Profiterzielung. Die Autoren zeigen, dass eigenständige Entscheidungen für den Schutz von Privatheit von Unternehmen, die Personalisierung betreiben, die soziale Wohlfahrt steigern können. Dies erfolgt jedoch auf Kosten der Konsumentenrente. Zudem kommen die Autoren zu dem Ergebnis, dass es aus Perspektive der sozialen Wohlfahrt effizient sein kann, wenn Regulierung die Implementierung von fairen Informationspraktiken erzwingt. Dies liegt insbesondere daran, dass die Anreize für Unternehmen, den wettbewerbsabschwächenden Effekt auszunutzen begrenzt werden (Lee et al. 2011). Acquisti und Varian (2005) sowie Conitzer et al. (2012) untersuchen theoretische Modelle, in welchen die Anbieter die Möglichkeit für Tracking-Technologien und Konsumenten Zugang zu Anonymisierungstechnologien haben. Acquisti und Varian (2005) widmeten sich der Frage, wann es für Unternehmen profitabel ist, Preise auf Basis des früheren Einkaufsverhaltens der Konsumenten zu diskriminieren. Die Autoren zeigen, dass es in

einem Monopolmarkt für den Anbieter nicht optimal ist, Preise je nach Art der Kunden (wertvolle und weniger wertvolle) festzulegen. Liegt jedoch ein Wettbewerbsmarkt vor, in dem es nicht mehr möglich ist, dass sich Anbieter auf eine Preispolitik festlegen, ist es für Anbieter profitabel, Preise auf Basis des früheren Einkaufsverhaltens anzupassen. In den Studien von Conitzer et al. (2012) und Koh et al. (2017) stehen Konsumenten einem Monopol gegenüber und können entscheiden, ob sie persönliche Informationen preisgeben wollen oder nicht. Conitzer et al. (2012) zeigen in ihrem Modell, dass die Konsumentenrente und die soziale Wohlfahrt bei einem mittleren Grad an Privatheit am höchsten ist. Koh et al. (2017) untersuchen die Effekte auf die Gesamtwohlfahrt im E-Commerce-Kontext am Beispiel von *freiwilligem Profiling*. Freiwilliges Profiling beschreibt, dass Konsumenten erst zustimmen müssen, bevor Unternehmen zum Beispiel das Einkaufsverhalten und andere persönliche Daten der Konsumenten sammeln und nutzen dürfen (Koh et al. 2017). Ein Beispiel für freiwilliges Profiling ist etwa das Bonusprogramm PAYBACK in Deutschland, für das sich Konsumenten mit ihren persönlichen Daten registrieren können. Die Konsumenten willigen ein, ihre Einkaufshistorie gegen Rabatte „einzutauschen“. Beim Zahlvorgang an der Kasse lassen die Kunden ihre PAYBACK-Karte einlesen, dadurch werden ihnen Punkte gutgeschrieben bzw. direkte Rabatte verrechnet. PAYBACK kann auf Basis dieser Daten anschließend per Post oder über die eigene App Produktgutscheine versenden und auf personalisierte Angebote aufmerksam machen. Für Konsumenten ergibt sich daher der Vorteil, dass ihre Suchkosten reduziert werden und sie leichter ein ideales Produkt finden können. Jedoch kann ein derartiges Profiling zu ungewollter Werbung und Privatheitsverletzungen führen. Die Autoren kommen zu dem Ergebnis, das weder die soziale Wohlfahrt noch die aggregierte Konsumentenrente höher sind, wenn freiwilliges Profiling vorliegt. Die Autoren argumentieren, dass selbst wenn freiwilliges Profiling zu einem Anstieg der sozialen Wohlfahrt führe, dann erfolge dies auf Kosten der Konsumentenrente (Koh et al. 2017, S. 23).

Neben diesen — wenigen — Studien findet sich in der Literatur auch ein Link von der Diskussion zur Preisdifferenzierung hin zur Wohlfahrt. So zeigen Rayna et al. (2015) in ihrer Studie, dass sogar Preisdiskriminierung der ersten Ordnung unter bestimmten Bedingungen positive Auswirkungen auf die soziale Wohlfahrt haben kann. Selbst wenn Unternehmen und Konsumenten sich egoistisch verhalten, kann ein „größeres Gut“ durch Preisdiskriminierung der ersten Ordnung erzielt werden, da es einen zusätzlichen Überschuss durch diese Form der Preisdiskriminierung gibt, welcher dann unter den Akteuren aufteilt wird. Voraussetzung für dieses Ergebnis ist es, dass Unternehmen die Aktivitäten der Konsumenten vollständig überwachen können.

6.2 Märkte für personenbezogenen Daten

Eine weitere zentrale Frage liegt in der Bedeutung von personenbezogenen Daten für die Marktstruktur. Arnold et al. (2016) argumentieren, dass internetbasierte Plattformen für positive gesamtwirtschaftliche Effekte sorgen, da sie den Wettbewerb intensivieren. Derartige Märkte lassen sich als zweiseitige Märkte charakterisieren. Diese Plattformen haben Zugang zu einer enormen

Menge an Konsumentendaten und könnten diese ökonomisch verwerten. Zum einen können sie die Daten an Werbetreibende verkaufen, aber auch an Datenintermediäre, die die Daten weiterverwerten. Häufig haben derartige Internetunternehmen, wie etwa Google, Facebook oder Amazon aufgrund von Netzwerkeffekten in zweiseitigen Märkten schnell eine enorme Marktmacht, im Extremfall bis hin zur Monopolstellung. Dadurch entstehen Markteintrittsbarrieren für andere Unternehmen. Verschiedene Autoren kommen zu dem Schluss, dass sozial optimale Preissetzung in einem zweiseitigen Markt zu einem Kostendeckungsproblem und somit zu Verlusten für die Plattform führen können (Bolt und Tieman 2006; Roson 2004). Beispielsweise argumentieren Bolt und Tieman (2006), dass aufgrund der zweiseitigen Marktstruktur positive externe Effekte zwischen den beiden Marktseiten entstehen. Diese tragen mehr zur Gesamtwohlfahrt bei als der Preis, den die einzelne Marktseite bezahlen müsste. Der sozial optimale Preis im Monopolfall liegt daher unter den marginalen Kosten (Bolt und Tieman 2006). Wenn in einem Duopol eine Plattform geringere Preise ansetzen kann, kann sie beide Seiten des Marktes bedienen, was ein Monopol zur Folge hat (Caillaud und Jullien 2003).

Aus Sicht der Unternehmen stellen persönliche Daten eine Ressource mit hohem Wertpotential dar. Für die Verwendung von persönlichen Daten durch Unternehmen gibt es zwei distinktive Szenarien. Zum einen erheben Unternehmen solche Daten und verwerten diese intern, so z.B. zur Personalisierung des Angebots oder zur Verbesserung der Produkte. Zum anderen erwerben Drittanbieter persönliche Daten und verkaufen diese gegebenenfalls weiter (Hess und Schreiner 2012). Der zweiten Frage wollen wir uns hier widmen.

Varian (1996) hat hierfür den Begriff die sekundäre Nutzung von persönlichen Informationen geprägt. Diese Form der Datennutzung erfolgt, wenn Informationen an Drittanbieter oder Datenhändler (sog. Broker) gegeben werden, wie etwa Datenaggregatoren oder Werbetreibende (Akçura und Srinivasan 2005). Händler und Soziale Netzwerke verkaufen persönliche Informationen an Vermittler (sog. Broker), die ihre Daten nutzen, um relevante Marktdemographika und relevante Kundensegmente zu identifizieren (Norman et al. 2016). Derartige Informationen sind in einer Vielzahl an Branchen von Wert, sei es in der Modeindustrie bis hin zur Gesundheitsbranche (Norman et al. 2016).

Ein wichtiges Thema ist die Bestimmung des Werts von personenbezogenen Daten. Die OECD und verschiedene Forscher haben Vorschläge gemacht, wie man Privatheit ökonomisch bewerten könnte (Acquisti 2010, 2014; OECD 2013; Spiekermann et al. 2012). Die OECD weist darauf hin, dass es keine einheitlich akzeptierte Methode gibt, den Wert von persönlichen Daten zu schätzen. Mögliche Ansätze können entweder auf der Marktbewertung von persönlichen Daten basieren, auf anderen Marktwerten oder auf der individuellen Bewertung. Beispiele auf Basis einer Marktbewertung sind: Marktpreise für Daten, Datenpreise in illegalen Märkten, Kosten bei Datenschutzverletzungen oder Umsätze pro Datensatz. Auf Basis von individueller Bewertung gibt es die Möglichkeit, Umfragen und

ökonomische Experimente durchzuführen und die individuelle Zahlungsbereitschaft für den Schutz von Daten abzufragen (OECD 2013, S. 19).

Das Agieren an Datenmärkten hat Rückkoppelungen für die Beschaffung von personenbezogenen Daten. Bei der Entscheidung, wieviel persönliche Informationen Nutzer preisgeben sollen, wägen diese die Vorteile gegenüber den möglichen Kosten, wie etwa Gefahren für ihre Privatheit, ab (Akçura und Srinivasan 2005). Je eher die Konsumenten erwarten, dass ein Anbieter ihre persönlichen Informationen in einem zweiten Markt verkauft, desto weniger Informationen würden sie preisgeben. Dementsprechend begrenzen Anbieter das Ausmaß, zu welchem sie Informationen verkaufen, um so Konsumenten dazu zu bewegen, mehr Informationen auf dem ersten Markt preiszugeben (Hui und Png 2005). Geben Unternehmen persönliche Informationen an Drittanbieter oder nutzen sie diese selbst für andere Zwecke, betrachten Nutzer dies als weniger rechtmäßig, wenn sie zuvor darüber nicht informiert wurden (Cecere et al. 2017). Daher bildet die sekundäre Verwendung von personenbezogenen Daten eine zentrale Dimension des Konzepts der Privatheitsbedenken (Smith et al. 1996), wie in Kapitel 4.1 beschrieben. Konsumenten betrachten den Handel mit ihren Daten zumeist als nachteilig und für Unternehmen, die mit Kundendaten handeln, können Reputationsverluste die Folge sein (Norman et al. 2016).

Ein neuerer Literaturzweig in der VWL befasst sich mit Anreizen für Datenhändler im Kontext von Targeting (Belleflamme et al. 2017; Braulin und Valletti 2016; Montes et al. 2015). Sowohl Braulin und Valletti (2016) als auch Montes et al. (2015) kommen zu dem Ergebnis, dass es für Datenhändler am profitabelsten ist, die Daten ausschließlich an ein einziges Unternehmen zu verkaufen. Jedoch führt dies zu einer ineffizienten Marktallokation. Belleflamme et al. (2017) kommen hingegen zu dem Ergebnis, dass Datenhändler Anreize haben können, Kundendaten an alle konkurrierenden Unternehmen zu verkaufen, wenngleich die bei den einzelnen Unternehmen vorliegenden Kundendaten von unterschiedlicher Qualität sind. Bergemann und Bonatti (2015) zeigen, dass es für einen Intermediär nachteilig sein kann, Werbetreibenden vollen Zugang zu persönlichen Informationen zu geben, da dies zu sinkenden Umsätzen führt. Intermediäre limitieren daher die Informationspreisgabe. Ein gewisser Grad an Privatheit ist folglich optimal für Intermediäre.

Weitgehend unklar ist bisher, wie die Wertschöpfungsstruktur für Daten genau aussieht. Diese Fragestellung haben in einer kürzlich erschienenen Studie Bründl et al. (2016) adressiert. Die Autoren haben in ihrer Studie die Wertschöpfungsstruktur in Datenmärkten aufgearbeitet. Sie unterscheiden dabei sieben verschiedene Rollen in der Wertschöpfungsstruktur: Advertiser, Publisher, Supply-Side-Plattform, Demand-Side-Plattform, Datensammler, Data-Management Plattform und Data Exchanges.

6.3 Regulierung

Konsumenten können nur schwer erkennen, welchen Wert die auf sie bezogenen Daten haben. Ungewünschte Verwendung, gerade auch im Zusammenspiel mit anderen Daten, erkennen sie in der Regel nicht. Auch ist für sie die weitere Verwendung in der Regel nicht transparent. Zudem messen die Konsumenten dem Schutz ihrer Daten je nach Land unterschiedliche Bedeutung zu. Gleichzeitig kann die Verwendung von personenbezogenen Daten für Konsumenten Vorteile haben, z.B. günstigere Angebote oder schnellerer Suche von Produkten. Auch versprechen datenbasierte Geschäftsmodelle durchaus Wachstum. Dies alles haben wir in den vorausgehenden Kapiteln bereits singulär herausgearbeitet. Nimmt man dies zusammen, so kann man daraus (siehe auch Acquisti et al. 2016) eine starke Informationsasymmetrie zu Lasten des Konsumenten und damit im Schutzbedürfnis des Konsumenten ableiten. Die Einführung von Regeln zum Schutz von Nachfragern wird als Regulierung bezeichnet.

Zwei zentrale Formen der Regulierung lassen sich unterscheiden: Staatliche Regulierung und Selbstregulierung durch die Anbieter. Die Forscher der oben bereits erwähnten Chicago School (Posner 1981; Stigler 1980) argumentieren, dass keine regulatorischen Eingriffe in den Markt notwendig seien, da der Markt von sich aus sozial gewünschte Ergebnisse erzielt. Darauf aufbauend weisen einige Autoren auf die Nachteile einer Regulierung hin (Goldfarb und Tucker 2011b; Miller und Tucker 2009). Privatheitsregulierung wirkt sich danach nicht nur auf das Verhalten von Konsumenten und Unternehmen aus, sondern kann auch indirekte Auswirkungen auf die Marktstruktur haben (Cecere et al. 2017). Beispielsweise zeigen Campbell et al. (2015), dass Privatheitsregulierung die ungewollte Etablierung von Monopolen zur Folge haben kann. Stigler (1980) und Posner (1981) argumentieren dagegen, dass Privatheitsschutz zu Ineffizienzen im Markt führt, da dem Markt potentiell nützliche Informationen vorenthalten werden. Im Gegensatz dazu plädiert Hirshleifer (1971) für den Schutz von Privatheit.

Selbstregulierungsansätze umfassen zum Beispiel Datenschutzrichtlinien und das Prinzip der Einverständniserklärung durch die Konsumenten als auch den Einsatz von Datenschutzsiegeln. Im Rahmen der Selbstregulierung wird von Konsumenten erwartet, dass sie die Datenschutzrichtlinien lesen und entsprechend zustimmen oder ablehnen. Ein umfangreicher Literaturzweig hat sich diesem Thema gewidmet (Böhme und Koble 2007; Bowie und Jamal 2006; Xu et al. 2012). Datenschutzrichtlinien sollen Konsumenten Informationen darüber bereitstellen, wie und in welchem Maße Unternehmen Informationen sammeln, verwerten und mit welchen Drittanbietern sie diese möglicherweise teilen (Tsai et al. 2011). Zahlreiche Studien zeigen jedoch, dass Konsumenten diese Datenschutzrichtlinien nicht im Detail lesen, da diese meist zu lang und für Individuen ohne Fachkenntnisse zu komplex sind, um diese zu verstehen (Milne und Culnan 2004). Ein weiteres Themenfeld im Bereich der Selbstregulierung, das in den WiWi viel Aufmerksamkeit erhalten hat, ist der Bereich der Gütesiegel von Online-Anbietern. Datenschutzrichtlinien und

Hinweise für den Datenschutz gehören mit zu den wichtigsten Eigenschaften von Websiten, um das Vertrauen der Konsumenten und ihre Bereitschaft, persönliche Informationen preiszugeben, zu steigern (Bansal und Gefen 2015). Ein Beispiel auf dem deutschen Markt für ein Datenschutz-Siegel ist etwa das Trusted Shop Gütesiegel (Noll und Winkler 2004). Diese Gütesiegel sollen dazu beitragen, dass Konsumenten schneller feststellen können, ob ein Anbieter entsprechende Datenschutzregelungen einhält und Konsumenten nicht Gefahr laufen, dass ihre Privatheit gefährdet wird. Diese Siegel senken folglich die Kosten für Konsumenten. Einige Studien haben jedoch gezeigt, dass derartige Siegel nicht immer wirken und sich Nutzer stattdessen auf ihr Vertrauen in den Händler verlassen, unabhängig vom Siegel und der tatsächlichen Vertrauenswürdigkeit (Bélanger et al. 2002; Hui et al. 2007).

Cecere et al. (2017) argumentieren, dass Regulierungsbehörden hier einschreiten sollten, um die Qualität der Siegel sicherzustellen. Goldfarb und Tucker (2011a) haben mit Hilfe eines großzahligen Feldexperiments zudem untersucht, wie die Inkraftsetzung der europäischen Privatheitsregulierung die Wirksamkeit von Bannerwerbung auf das individuelle Verhalten beeinflusst hat. Die Autoren zeigen, dass Privatheitsregulierung, die verhaltensbasiertes Targeting verbietet, die Wirksamkeit von Werbung verringert.

Norman et al. (2016) untersuchen in ihrer Studie, ob ein selbstregulierter Markt, der mit transparenten Datenschutzrichtlinien agiert, zu einem effizienten Marktergebnis führt. Die Autoren identifizieren Marktbedingungen, unter welchen ein übermäßiger Verkauf von Konsumentendaten vorliegt. Die Autoren zeigen aber auch Fälle auf, in denen Konsumenten und Unternehmen durch striktere Datenschutzgesetzgebung oder -restriktionen besser gestellt sind.

Deutlich weniger Arbeiten befassen sich mit der ökonomischen Wirkung der Ausgestaltung von Datenschutzgesetzen. Adjerid et al. (2015) untersuchen beispielsweise die Auswirkungen von Gesetzen innerhalb der USA auf die Verbreitung von Technologien für den Austausch von Gesundheitsdaten. Die Autoren zeigen, dass die Kombination aus Subventionen und Datenschutz in einer höheren Akzeptanz resultiert. Die Studie zeigt folglich, dass Datenschutzregulierung einen Einfluss auf die ökonomische Wohlfahrt haben kann. Campbell et al. (2015) haben ebenfalls die Auswirkungen von Datenschutzregulierung auf die Wohlfahrt untersucht. Dabei zeigen sie, wie regulatorische Versuche, die Privatheit der Konsumenten zu schützen, die Wettbewerbsstruktur im Markt beeinflussen kann (Campbell et al. 2015, S. 47). Datenschutzregulierung kann negative Auswirkungen auf den Wettbewerb und somit auf die Gesamtwohlfahrt haben (Campbell et al. 2015). Schließlich haben auch Chellappa und Shivendu (2007) untersucht, wie sich verschiedene Datenschutzregulierungsansätze auf die Wohlfahrt auswirken. Das Ergebnis ihrer Studie zeigt, dass weniger Regulierung gesamtgesellschaftlich vorteilhaft sein kann. Statt einem ausschließlichen Fokus auf Regulierung empfehlen die Autoren, Eigentumsrechte den Konsumenten zuzuteilen.

7 Fazit und Ausblick

Dieser Beitrag hat die WiWi-Literatur aus Sicht der drei wesentlichen Perspektiven *Konsument*, *Anbieter* und *Markt* präsentiert. Aus Konsumentenperspektive wird deutlich, dass Konsumenten einem komplexen Entscheidungsprozess gegenüberstehen. Einerseits können Individuen durch die Preisgabe von persönlichen Informationen in den (zumeist kostenlosen) Nutzen von Diensten und Angeboten kommen und somit auf verschiedene Weise profitieren. Andererseits bedeutet eine Informationspreisgabe auch die Gefahr von Datenmissbrauch und Privatheitsverlust.

Zur Konsumentenperspektive finden sich bereits eine Reihe interessanter Arbeiten. Gerade die Privatheitsbedenken als auch das Privatheitsparadox scheinen schon recht gut verstanden zu sein. Beim Privatheitskalkül bietet sich die verstärkte Berücksichtigung verhaltenswissenschaftlicher Einsichten in das Entscheidungsverhalten von Personen und auch von Gruppen sowie die Berücksichtigung nur mittelbar tangierter Personen an. Studien zur Zahlungsbereitschaft für ein Mehr an Privatheit scheitern bisher sehr häufig an methodischen Problemen.

Die Literatur zur Anbieterperspektive verdeutlicht vor allem die verschiedenen Strategien, die Unternehmen anwenden, um von persönlichen Daten der Kunden und Nutzer zu profitieren, sei es durch die Personalisierung von Empfehlungen sowie Diensten und Angeboten als auch durch verbesserte Preisdiskriminierung.

Eher ernüchternd war die Analyse der Arbeiten zur Marktperspektive. Es finden sich Arbeiten zur Wirkung der Selbstregulierung von Anbietern. Zentrale Fragen, insbesondere zur Wirkung staatlicher Regulierung über Datenschutzgesetze, bleiben bisher unbeantwortet. Auch weiß man heute erstaunlich wenig über Märkte für personenbezogene Daten.

Insgesamt lässt sich festhalten, dass die Marktperspektive bisher recht kurz kommt. Es ist vor allem die mikroökonomische Perspektive, die in der VWL intensiver betrachtet wurde. Insbesondere mit Blick auf gesamtgesellschaftliche Wohlfahrtseffekte sollte künftig mehr Forschung erfolgen. Bisherige Ergebnisse zu den Wohlfahrtseffekten von Privatheitsschutz und Regulierungsmaßnahmen sind teilweise widersprüchlich und bieten sich daher für die Ableitung wirtschaftspolitischer Maßnahmen nicht unbedingt an.

Angeregt sei auch, dass sich die Forschung mit der Ausgestaltung und Bewertung neuer Ideen beschäftigt. Solch ein Thema ist die Datensouveränität, die von der Politik vermehrt in die Diskussion eingebracht wird. Jedoch fehlt es bislang an konkreten Strategien und Vorschlägen, wie Nutzern Souveränität über ihre persönlichen Daten zu Teil werden kann und gleichzeitig Unternehmen auch davon profitieren können bzw. gar neue Geschäftsmodelle entwickeln könnten. Aus Anbieter- und Marktperspektive ist es daher relevant, einen Weg zu identifizieren, um Privatheit bzw. persönlichen Daten einen (monetären) Wert zuordnen zu können, um daraus Ableitungen für Strategien zu treffen und die Erfolgswahrscheinlichkeit von Regulierungsmaßnahmen entsprechend zu berechnen. Ein

zweites Feld, mehr im innerbetrieblichen Bereich, könnte der Aufbau einer inversen Transparenz (Brin 1998) sein. Grundidee ist dabei, dass die wachsende Transparenz durch Daten um eine Transparenz bei der Datenerhebung und -verwendung selbst ergänzt werden muss. Inverse Transparenz zielt so darauf, die Datensouveränität der Beschäftigten zu stärken und diese selbst in die Lage zu versetzen, nachvollziehen zu können, wie die eigenen Daten verwendet werden.

8 Literaturverzeichnis

Aaken, D., Ostermaier, A., und Picot, A. 2014. "Privacy and Freedom: An Economic (Re-) Evaluation of Privacy," Kyklos 67(2), 133-155.

Acquisti, A. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," Proceedings of the 5th ACM Conference on Electronic Commerce: ACM, 21-29.

Acquisti, A. 2009. "Nudging Privacy: The Behavioral Economics of Personal Information," IEEE Security & Privacy 7(6).

Acquisti, A. 2010. "The Economics of Personal Data and the Economics of Privacy," Background Paper for the Joint WPISP-WPIE Roundtable: The Economics of Personal Data and Privacy - 30 Years after the OECD Privacy Guidelines, Paris (France): OECD, 1-50.

Acquisti, A., und Fong, C.M. 2015. "An Experiment in Hiring Discrimination via Online Social Networks,", Abgerufen am 07.06.2017, von https://ssrn.com/abstract=2031979.

Acquisti, A., und Grossklags, J. 2005. "Privacy and Rationality in Individual Decision Making," IEEE Security & Privacy, 26-33.

Acquisti, A., Taylor, C.R., und Wagman, L. 2016. "The Economics of Privacy," Journal of Economic Literature 54(2), 1-53.

Acquisti, A., und Varian, H.R. 2005. "Conditioning Prices on Purchase History," Marketing Science 24(3), 367-381.

Adjerid, I., Acquisti, A., Telang, R., Padman, R., und Adler-Milstein, J. 2015. "The Impact of Privacy Regulation and Technology Incentives: The Case of Health Information Exchanges," Management Science 62(4), 1042-1063.

Agarwal, R., und Rodhain, F. 2002. "Mine or Ours: Email Privacy Expectations, Employee Attitudes, and Perceived Work Environment Characteristics," Proceedings of the 35th Annual Hawaii International Conference, Hawaii, 2471-2480.

Ajzen, I. 1991. "The Theory of Planned Behavior," Organizational Behavior and Human Decision Processes 50(2), 179-211.

Ajzen, I., und Fishbein, M. 1975. Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research, Reading, MA: Addison-Wesley.

Akçura, M.T., und Srinivasan, K. 2005. "Research Note: Customer Intimacy and Cross-Selling Strategy," Management Science 51(6), 1007-1012.

Akerlof, G.A. 1970. "The Market for "Lemons": Quality Uncertainty and the Market Mechanism. The Quarterly Journal of Economics 84(3), 488-500.

Alashoor, T., und Baskerville, R. 2015. "The Privacy Paradox: The Role of Cognitive Absorption in the Social Networking Activity," Proceedings of the 36th Conference on Information Systems (ICIS), Fort Worth, Texas, USA.

Allen, W.M., Coopman, S.J., Hart, J.L. und Walker, K.L. 2007. " Workplace Surveillance and Managing Privacy Boundaries," Management Communication Quarterly 21(2), 172-200.

Altman, I. 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding, Broks/Cole Pub. Co.

Anderson, C.L., und Agarwal, R. 2011. "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information," Information Systems Research 22(3), 469-490.

Armstrong, M., und Zhou, J. 2010. "Conditioning Prices on Search Behaviour," Technical Report 19985, MPRA Paper, University Library of Munich.

Aslam, S. 2017. "Snapchat by the Numbers: Stats, Demographics & Fun Facts," Abgerufen am 22.03.2017, von https://www.omnicoreagency.com/snapchat-statistics/.

Awad, N.F., und Krishnan, M.S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," MIS Quarterly 30(1), 13-28.

Bansal, G., und Gefen, D. 2015. "The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern," European Journal of Information Systems 24(6), 624-644.

Bansal, G., Zahedi, F.M., und Gefen, D. 2016. "Do Context and Personality Matter? Trust and Privacy Concerns in Disclosing Private Information Online," Information & Management 53(1), 1-21.

Bélanger, F., Hiller, J.S., und Smith, W.J. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," The Journal of Strategic Information Systems 11(3), 245-270.

Bélanger, F., und Crossler, R.E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," MIS Quarterly 35(4), 1017-1042.

Belleflamme, P., Lam, W.M.W., und Vergote, W. 2017. "Price Discrimination and Dispersion under Asymmetric Profiling of Consumers," 2017.

Belleflamme, P., und Vergote, W. 2016. "Monopoly Price Discrimination and Privacy: The Hidden Cost of Hiding," Economics Letters 149(52), 141-144.

Beresford, A.R., Kübler, D., und Preibusch, S. 2012. "Unwillingness to Pay for Privacy: A Field Experiment," Economics Letters 117(1), 25-27.

Bergemann, D., und Bonatti, A. 2015. "Selling Cookies," American Economic Journal: Microeconomics 7(3), 259-294.

Bertrand, M., und Duflo, E. 2017. "Field Experiments on Discrimination," Handbook of Economic Field Experiments (1), 309-393.

Biczók, G., und Chia, P.H. 2013. "Interdependent Privacy: Let Me Share Your Data," International Conference on Financial Cryptography and Data Security: Springer, 338-353.

Bolt, W. und Tieman, A.F. 2006. "Social Welfare and Cost Recovery in Two-Sided Markets," Review of Network Economics 5(1), 103-117.

Boyd, D. 2012. "Networked Privacy," Surveillance & Society 10(3/4), 348-350.

Böhme, R. und Koble, S. 2007. "On the Viability of Privacy-Enhancing Technologies in a Self-Regulated Business-to-Consumer Market: Will Privacy Remain a Luxury Good?," Workshop on the Economics of Information Security (WEIS), 1-21.

Bowie, N.E., und Jamal, K. 2006. "Privacy Rights on the Internet: Self-Regulation or Gorvernment Regulation?," Business Ethics Quarterly 16(3), 323-342.

Braulin, F.C., und Valletti, T. 2016. "Selling Customer Information to Competing Firms," Economics Letters (149), 10-14.

Brin, G.D. 1998. The Transparent Society: Will Technology Force us to Choose Between Privacy and Freedom, Perseus Books.

Bründl, S., Matt, C., und Hess, T. 2015. "Wertschöpfung in Datenmärkten," Forschungsbericht des Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt.

Bründl, S., Matt, C., und Hess, T. 2016. "Daten Als Geschäft - Rollen Und Wertschöpfungsstrukturen Im Deutschen Markt Für Persönliche Daten," Wirtschaftsinformatik & Management 6(2016), 78-83.

Caillaud, B. und Jullien, B. 2003. "Chicken & Egg: Competition Among Intermediation Service Providers," RAND Journal of Economics 34(2), 309-328.

Calzolari, G., und Pavan, A. 2006. "On the Optimality of Privacy in Sequential Contracting," Journal of Economic Theory 130(1), 168-204.

Campbell, J., Goldfarb, A., und Tucker, C.E. 2015. "Privacy Regulation and Market Structure," Journal of Economics and Management Strategy 24(1), 47-73.

Campbell, J.E., und Carlson, M. 2002. "Panopticon. Com: Online Surveillance and the Commodification of Privacy," Journal of Broadcasting & Electronic Media 46(4), 586-606.

Caudill, E.M., und Murphy, P.E. 2000. "Consumer Online Privacy: Legal and Ethical Issues," Journal of Public Policy & Marketing 19(1), 7-19.

Cecere, G., Le Guel, F., Manant, M., und Soulié, N. 2017. "The Economics of Privacy," The New Palgrave Dictionary of Economics.

Chan, Y.E., und Greenaway, K.E. 2005. "Theoretical Explanations for Firms' Information Privacy Behaviors," Journal of the Association for Information Systems 6(6), 171-198.

Chau, M., und Clemons, E.K. 2011. "Individual Privacy and Online Services," Proceedings of the 44th Hawaii International Conference on System Sciences (HICSS), Hawaii.

Chellappa, R.K., und Shivendu, S. 2007. "An Economic Model of Privacy: A Property Rights Approach to Regulatory Choices for Online Personalization," Journal of Management Information Systems 24(3), 193-225.

Chellappa, R.K., und Sin, R.G. 2005. "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," Information Technology and Management 6(2-3), 181-202.

Child, J.T., Pearson, J.C., und Petronio, S. 2009. "Blogging, Communication, and Privacy Management: Development of the Blogging Privacy Management Measure," Journal of the American Society for Information Science and Technology 60(10), 2079-2094.

Choudhary, V., Ghose, A., Mukhopadhyay, T., und Rajan, U. 2005. "Personalized Pricing and Quality Differentiation," Management Science 51(7), 1120-1130.

CMA 2015 Competition & Markets Authority 2015. "The Commercial Use of Consumer Data," CMA Report.

Conitzer, V., Taylor, C.R., und Wagman, L. 2012. "Hide and Seek: Costly Consumer Privacy in a Market with Repeat Purchases," Marketing Science 31(2), 277-292.

Culnan, M.J. 1993. "How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," MIS Quarterly 17(3), 341-363.

Culnan, M.J., und Armstrong, P.K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," Organization Science 10(1), 104-115.

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

Davies, S.G. 1998. "Cctv: A New Battleground for Privacy," Surveillance, Closed Circuit Television and Social Control, 249-251.

Dewan, R., Jing, B., und Seidmann, A. 2003. "Product Customization and Price Competition on the Internet," Management Science 49(8), 1055-1070.

Dinev, T. 2014. "Why Would We Care About Privacy?," European Journal of Information Systems 23(2), 97-102.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., und Colautti, C. 2006. "Privacy Calculus Model in E-Commerce - A Study of Italy and the United States," European Journal of Information Systems 15(4), 389-402.

Dinev, T., und Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," Information Systems Research 17(1), 61-80.

Dinev, T., McConnell, A.R., und 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.

Egelman S., Felt, A.P., und Wagner, D. 2013. "Choice Architecture and Smartphone Privacy: There's a Price for That," The Economics of Information Security and Privacy, 211-236.

Feri, F, Giannetti, C. und Jentzsch, N. 2016. "Disclosure of Personal Information Under Risk of Privacy Shocks," Journal of Economic Behavior & Organization 123(2016), 138-148.

Foley, D.K. 1970. "Lindahl's Solution and the Core of an Economy with Public Goods," Econometrica: Journal of the Econometric Society 38(1), 66-72.

Forum Privatheit 2017. "Forum Privatheit - Selbstbestimmtes Leben in der digitalen Welt," Abgerufen am 20.07.2017, von www.forum-privatheit.de.

Frik, A., und Gaudeul, A. 2016. "The Relation Between Privacy Protection and Risk Attitudes, With a New Experimental Method to Elicit the Implicit Monetary Value of Privacy," Center for European, Governance and Economic Development Research Discussion Paper 296, University of Goettingen, Department of Economics https://ideas.repec.org/p/zbw/cegedp/296.html.

Goldfarb, A., und Tucker, C. 2011a. "Online Display Advertising: Targeting and Obtrusiveness," Marketing Science 30(3), 389-404.

Goldfarb, A., und Tucker, C.E. 2011b. "Privacy Regulation and Online Advertising," Management Science 57(1), 57-71.

Goldin, C., und Rouse, C. 1997. "Orchestrating Impartiality: The Impact of" Blind" Auditions on Female Musicians," National Bureau of Economic Research.

Goode, L. 2016. "Messenger and Whatsapp Process 60 Billion Messages a Day, Three Times More Than SMS," Abgerufen am 22.03.2017, von http://www.theverge.com/2016/4/12/11415198/facebook-messenger-whatsapp-number-messages-vs-sms-f8-2016.

Gross, R. und Acquisti, A. 2005. "Information Revelation and Privacy in Online Social Networks," Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, 71-80.

Gürtler, O., und Höffler, F. 2015. "Monitoring of Workers and Product Market Competition: The Role of Works Councils," Economic Inquiry 53(2), 1366-1379.

Handelsblatt 2013. Handelsblatt-VWL-Ranking 2013: Journal List. Abgerufen am: 03.03.2017, von https://www.handelsblatt.com/downloads/9665428/1/journal-ranking.pdf.

Hann, I.-H., Hui, K.-L., Lee, S.-Y.T., und Png, I.P. 2002. "Online Information Privacy: Measuring the Cost-Benefit Trade-Off," Proceedings of the 23rd International Conference on Information Systems (ICIS), Barcelona, Spain.

Hann, I.-H., Hui, K.-L., Lee, S.-Y.T., und Png, I.P. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," Journal of Management Information Systems 24(2), 13-42.

Hartman, L.P. 2001. "Technology and Ethics: Privacy in the Workplace," Business and Society Review 106(1), 1-27.

Hermalin, B.E., und Katz, M.L. 2006. "Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy," Quantitative Marketing and Economics 4(3), 209-239.

Hess, T., und Scheiner, M. 2012. "Ökonomie Der Privatheit - Eine Annäherung Aus Drei Perspektiven," Datenschutz und Datensicherheit (DuD) 2(2012), 105-109.

Hirshleifer, J. 1971. "The Private and Social Value of Information and the Reward to Inventive Activity," The American Economic Review 61(4), 561-574.

Hirshleifer, J. 1980. "Privacy: Its Origin, Function, and Future," The Journal of Legal Studies 9(4), 649-664.

Hong, W., und Thong, J.Y. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," MIS Quarterly 37(1), 275-298.

Huberman, B. A., Adar, E., und Fine, L.R. 2005. “Valuating Privacy,” IEEE Security & Privacy, 3(5), 22-25.

Hui, K.-L., und Png, I.P. 2005. "Economics of Privacy," Handbook of Information Systems and Economics.

Hui, K.L., Teo, H.H., und Lee, S.Y. T. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," MIS Quarterly 31(1), 19-33.

James, T.L., Wallace, L., Warkentin, M., Kim, B.C., und Collignon, S.E. 2017. "Exposing Others' Information on Online Social Networks (Osns): Perceived Shared Risk, Its Determinants, and Its Influence on Osn Privacy Control Use," Information & Management (2017), 1-15.

Jentzsch, N. 2014. “Monetarisierung der Privatsphäre: welchen Preis haben persönliche Daten?,” DIW Wochenbericht 34(2014), 793-798.

Jentzsch, N. 2016. "State-of-the-Art of the Economics of Cyber-Security and Privacy," IPACSO - Innovation Framework for ICT Security Deliverable, 1-78.

Jia, H., und Xu, H. 2016. "Measuring Individuals' Concerns over Collective Privacy on Social Networking Sites," Cyberpsychology: Journal of Psychosocial Research on Cyberspace 10(1), 1-20.

Kehr, F., Kowatsch, T., Wentzel, D., und Fleisch, E. 2015. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus," Information Systems Journal 25(6), 607-635.

Koh, B., Raghunathan, S., und Nault, B.R. 2017. "Is Voluntary Profiling Welfare Enhancing?," MIS Quarterly 41(1), 23-41.

Koohikamali, M., Peak, D.A., und Prybutok, V. 2017. "Beyond Self-Disclosure: Disclosure of Information About Others in Social Network Sites," Computers in Human Behavior 69(2017), 29-42.

Krasnova, H., Veltri, N.F., und Güther, O. 2012. "Die Rolle der Kultur in der Selbstoffenbarung und Privatsphäre in sozialen Onlinenetzwerken," Wirtschaftsinformatik 54(3), 123-133.

Krasnova, H., Spiekermann, S., Koroleva, K., und Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," Journal of Information Technology 25(2),109-125.

Kurkovsky, S., und Syta, E. 2011. "Monitoring of Electronic Communications at Universities: Policies and Perceptions of Privacy," Proceedings of the 44th Hawaii International Conference (HICSS), Hawaii.

Lambrecht, A., und Tucker, C. 2013. "When Does Retargeting Work? Information Specificity in Online Advertising," Journal of Marketing Research 50(5), 561-576.

Lambrecht, A., und Tucker, C.E. 2016. "Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of Stem Career Ads," Abgerufen am 03.07.2017, von https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852260

Laufer, R.S., und Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," Journal of Social Issues 33(3), 22-42.

Lee, D.-J., Ahn, J.-H., und Bang, Y. 2011. "Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection," MIS Quarterly 35(2), 423-444.

Li, M., Lou, W., und Ren, K. 2010. "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Communications 17(1).

Li, T., und Unger, T. 2012. "Willing to Pay for Quality Personalization? Trade-Off between Quality and Privacy," European Journal of Information Systems 21(6), 621-642.

Li, Y. 2011. "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," Communications of the Association for Information Systems 28(1), 453-496.

Li, Y. 2012. "Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework," Decision Support Systems 54(1), 471-481.

Li, X.B., und Sarkar, S. 2011. "Protecting Privacy Against Record Linkage Disclosure: A Bounded Swapping Approach for Numeric Data," Information Systems Research 22(4), 774-789.

Liang, T.-P., Lai, H.-J., und Ku, Y.-C. 2006. "Personalized Content Recommendation and User Satisfaction: Theoretical Synthesis and Empirical Findings," Journal of Management Information Systems 23(3), 45-70.

Lugaresi, N. 2010. "Electronic Privacy in the Workplace: Transparency and Responsibility," International Review of Law, Computers & Technology 24(2), 163-173.

Malhotra, N.K., Kim, S.S., und Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model," Information Systems Research 15(4), 336-355.

Manant, M., Pajak, S., und Soulié, N. 2014. "Do Recruiters' Like'it? Online Social Networks and Privacy in Hiring: A Pseudo-Randomized Experiment," MPRA 56845.

Margulis, S.T. 2003. "Privacy as a Social Issue and Behavioral Concept," Journal of Social Issues 59(2), 243-261.

Martin, K.D., und Murphy, P.E. 2017. "The Role of Data Privacy in Marketing," Journal of the Academy of Marketing Science 45(2), 135-155.

Marwick, A.E., und Boyd, D. 2014. "Networked Privacy: How Teenagers Negotiate Context in Social Media," New Media & Society 16(7), 1051-1067.

Mas-Colell, A., Whinston, M.D., und Green, J.R. 1995. "Microeconomic Theory". New York: Oxford University Press.

Milberg, S.J., Smith, H.J., und Burke, S.J. 2000. "Information Privacy: Corporate Management and National Regulation," Organization Science 11(1), 35-57.

Miller, A.R., und Tucker, C. 2009. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records," Management Science 55(7), 1077-1093.

Milne, G.R., und Culnan, M.J. 2004. "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices," Journal of Interactive Marketing 18(3), 15-29.

Milne, G.R., und Gordon, M.E. 1993. "Direct Mail Privacy-Efficiency Trade-Offs within an Implied Social Contract Framework," Journal of Public Policy & Marketing 12(2), 206-215.

Montes, R., Sand-Zantman, W., und Valletti, T.M. 2015. "The Value of Personal Information in Markets with Endogenous Privacy," CEIS Working Paper No. 352.

Morlok, T., Matt, C., und Hess, T. 2016. "Führung Und Privatheit in Der Digitalen Arbeitswelt," Datenschutz und Datensicherheit (DuD) 40(5), 310-314.

Nissenbaum, H. 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

Noll, J., und Winkler, M. 2004. "Gütesiegel und Vertrauen im E-Commerce," der markt 43(1), 23-32.

Norberg, P.A., Horne, D.R., und Horne, D.A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors," Journal of Consumer Affairs 41(1), 100-126.

Norman, G., Pepall, L., Richards, D., und Tan, L. 2016. "Competition and Consumer Data: The Good, the Bad, and the Ugly," Research in Economics 70(4), 752-765.

Odlyzko, A. 2003. "Privacy, Economics, and Price Discrimination on the Internet," Proceedings of the 5th International Conference on Electronic Commerce: ACM, 355-366.

OECD 2013. "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value".

Olteanu, A.-M., Huguenin, K., Shokri, R., Humbert, M., und Hubaux, J.-P. 2016. "Quantifying Interdependent Privacy Risks with Location Data," IEEE Transactions on Mobile Computing 16(3), 829-842.

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

Pavlou, P.A. 2011. "State of the Information Privacy Literature: Where Are We Now and Where Should We Go?," MIS Quarterly 35(4), 977-988.

Png, I.P.L. 2007. On the Value of Privacy from Telemarketing: Evidence from the 'Do Not Call' Registry,".

Posner, R.A. 1981. "The Economics of Privacy," American Economic Review 71(2), 405-409.

Pu, Y., und Grossklags, J. 2015. "Using Conjoint Analysis to Investigate the Value of Interpendent Privacy in Social App Adoption Scenarios," Proceedings of the 36th International Conference on Information Systems (ICIS), Fort Worth, Texas, USA.

Pu, Y., und Grossklags, J. 2016. "Towards a Model on the Factors Influencing Social App Users' Valuation of Interdependent Privacy," Proceedings on Privacy Enhancing Technologies 2016(2), 61-81.

Raij, A., Ghosh, A., Kumar, S., und Srivastava, M. 2011. "Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Vancouver, British Columbia, Canada: ACM, 11-20.

Rayna, T., Darlington, J., und Striukova, L. 2015. "Pricing Music Using Personal Data: Mutually Advantageous First-Degree Price Discrimination," Electronic Markets 25(2), 39-154.

Roson, R. 2004. "Two-Sided Markets: A Tentative Survey," Review of Network Economics 4(2), 142-160.

Rust, R. T., Kannan, P. K., und Peng, N. 2002. "The Customer Economics of Internet Privacy," Journal of the Academy of Marketing Science, 30(4), 455-464.

Saeri, A.K., Ogilvie, C., La Macchia, S.T., Smith, J.R., und Louis, W.R. 2014. "Predicting Facebook Users' Online Privacy Protection: Risk, Trust, Norm Focus Theory, and the Theory of Planned Behavior," The Journal of Social Psychology 154(4), 352-369.

Schmitz, P.W. 2005. "Workplace Surveillance, Privacy Protection, and Efficiency Wages," Labour Economics 12(6), 727-738.

Schoeman, F.D. 1984. "Privacy: Philosophical Dimensions of the Literature," in Philosophical Dimensions of Privacy: An Anthology, F.D. Schoeman (ed.). Cambridge: Cambridge University Press, 1-33.

Schreiner, M. 2016. "Privacy-Friendly Online Services: Empirical Studies on Consumers' Privacy Protection Behaviors" epubli:Berlin.

Schreiner, M., und Hess, T. 2015. "Why Are Consumers Willing to Pay for Privacy? An Application of the Privacy-Freemium Model to Media Companies," Proceedings of the 23rd European Conference on Information Systems (ECIS), Münster, Germany.

Shaffer, G., und Zhang, Z.J. 2002. "Competitive One-to-One Promotions," Management Science 48(9), 1143-1160.

Sheng, H., Nah, F.F.-H., und Siau, K. 2008. "An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns*," Journal of the Association for Information Systems 9(6), 344-376.

Shi, P., Xu, H., Erickson, L., und Zhang, C. 2012. "See Friendship: Interpersonal Privacy Management in a Collective World," Proceedings of the 18th Amercian Conference on Information Systems (AMCIS), Washington, Seattle, USA.

Sipior, J., und Ward, B. 1996. "United States Cases of Employee E-Mail Privacy Intrusions: Do You Really Know the Legal Consequences?," Proceedings of the 17th International Conference on Information Systems (ICIS), Cleveland, Ohio, USA.

Sipior, J.C., Burke, T.W., Connolly, R., und MacGabhann, L. 2013. "Privacy in Online Social Networking: Applying a Privacy Calculus Model. Proceedings of the 17th Pacific Asia Conference on Information Systems (PACIS), Jeju Island, South Korea.

Smith, H.J., Dinev, T., und Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," MIS Quarterly 35(4), 989-1016.

Smith, H.J., Milberg, S.J., und Burke, S.J. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," MIS Quarterly 20(2), 167-196.

Snyder, J.L. 2010. "E-Mail Privacy in the Workplace: A Boundary Regulation Perspective," The Journal of Business Communication 47(3), 266-294.

Solove, D.J. 2006. "A Taxonomy of Privacy," University of Pennsylvania Law Review 154(3), 477-564.

Son, J.-Y., und Kim, S.S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," MIS Quarterly 32(3), 503-529.

Spiekermann, S. 2012. "The Challenges of Privacy by Design," Communications of the ACM 55(7), 38-40.

Spiekermann, S., Korunoska, J., und Bauer, C. 2012. "Psychology of Ownership and Asset Defense: Why People Value Their Personal Information Beyond Privacy,". Abgerufen am 10.12.2016, von https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2148886.

Spiekermann, S., Acquisti, A., Böhme, R., und Hui, K.-L. 2015. "The Challenges of Personal Data Markets and Privacy," Electronic Markets 25(2), 161-167.

Stewart, K.A., und Segars, A.H. 2002. "An Empirical Examination of the Concern for Information Privacy Instrument," Information Systems Research 13(1), 36-49.

Stigler, G.J. 1980. "An Introduction to Privacy in Economics and Politics," The Journal of Legal Studies 9(4), 623-644.

Sutanto, J., Palme, E., Tan, C.-H., und Phang, C.W. 2013. "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users," MIS Quarterly 37(4), 1141-1164.

Taylor, C.R. 2004. "Consumer Privacy and the Market for Customer Information," The RAND Journal of Economics 35(4), 631-650.

Thisse, J.F., und Vives, X. 1988. "On the Strategic Choice of Spatial Price Policy," The American Economic Review 78(1), 122-137.

Tsai, J.Y., Egelman, S., Cranor, L., und Acquisti, A. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study,"Information Systems Research 22(2), 254-268.

Tucker, C.E. 2010. "The Economics Value of Online Customer Data," Background Paper.

Tucker, C.E. 2014. "Social Networks, Personalized Advertising, and Privacy Controls," Journal of Marketing Research 51(5), 546-562.

Varian, H.R. 1996. "Economic Aspects of Personal Privacy," Abgerufen am 15.07.2017, von http://people.ischool.berkeley.edu/~hal/Papers/privacy/

Varian, H., Wallenberg, F., und Woroch, G. 2005. "The Demographics of the Do-Not-Call List," IEEE Secruity & Privacy 31(1), 34-39.

VHB-JOURQUAL3 2017. "VHB-JOURQUAL3," Abgerufen am 10.06.2017, von vhbonline.org/vhb4you/jourqual/vhb-jourqual-3/.

Villas-Boas, J.M. 2004. "Price Cycles in Markets with Customer Recognition," RAND Journal of Economics 35(3), 486-501.

Warren, S.D., und Brandeis, L.D. 1890. "The Right to Privacy," Harvard Law Review 4(5), 193-220.

Wathieu, L., und Friedman, A.A. 2007. " An Empirical Approach to Understanding Privacy Valuation," HBS Marketing Research Paper No.07-075.

Webster, J., und Watson, R.T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," MIS Quarterly 26(2), xiii-xxiii.

Wenninger, H., Widjaja, T., Buxmann, P., und Gerlach, J. 2012. "Der" Preis Des Kostenlosen"," Darmstadt Technical University, Department of Business Administration, Economics and Law, Institute for Business Studies (BWL).

Westin, A.F. 1967. Privacy and Freedom. New York: Atheneum Press.

WhatsApp. 2017. "Where Can I Find My Whatsapp Media Files?," Abgerufen am 17.03.2017, von https://www.whatsapp.com/faq/en/wp/30034176.

Wilson, D., und Valacich, J.S. 2012. "Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus," Proceedings of th 33rd International Conference on Information Systems (ICIS), Orlando, USA.

Wilson, D.W., Proudfoot, J.G., und Valacich, J.S. 2014. "Saving Face on Facebook: Privacy Concerns, Social Benefits, and Impression Management," Proceedings of the 35th International Conference on Information Systems (ICIS), Auckland, New Zealand.

Xu, H., Dinev, T., Smith, H.J., und Hart, P. 2008. "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," Proceedings of the 29th International Conference on Information Systems (ICIS), Paris, France.

Xu, H., Dinev, T., Smith, J., und Hart, P. 2011a. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," Journal of the Association for Information Systems 12(12), 798-824.

Xu, H., Luo, X.R., Carroll, J.M., und Rosson, M.B. 2011b. "The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing," Decision Support Systems 51(1), 42-52.

Xu, H., Teo, H.-H., Tan, B.C., und Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," Journal of Management Information Systems 26(3), 135-174.

Xu, H., Teo, H.H., Tan, B.C., und Agarwal, R. 2012. "Research Note - Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services," Information Systems Research 23(4), 1342-1363.

Yoo, Y. 2010. "Computing in Everyday Life: A Call for Research on Experiential Computing," MIS Quarterly 32(2), 213-231.

Yoo, C.W., Ahn, H.J., und Rao, H.R. 2012. “An Exploration of the Impact of Information Privacy Invasion,” Proceedings of the 33rd International Conference on Information Systems (ICIS), Orlando, Florida, USA.