Zum Zusammenspiel zwischen Unternehmen und Verbrauchern in der Datenökonomie

Herausforderungen und neue Gestaltungsansätze

Thomas Hess, Christian Matt, Verena Thürmel und Mena Teebken

1 Einführung

Durch die immer stärkere Durchdringung von Wirtschaft und Gesellschaft mit digitalen Technologien werden in bislang ungekanntem Maß Daten (teil-) automatisch erhoben, gespeichert und verarbeitet. Exemplarisch sind Technologien wie künstliche Intelligenz, Web-Tracking oder Blockchain zu nennen. Der Zugang zu großen Datenbeständen kann wiederum das Entscheidungsverhalten von Unternehmen und Verbrauchern verändern, mitunter sogar auch über die Grenzen von physischer und digitaler Welt hinweg. Heutzutage ist es einfacher möglich, Daten aus unterschiedlichen Quellen miteinander zu verknüpfen und auszuwerten.

T. Hess (✉) · V. Thürmel · M. Teebken
Institut für Digitales Management und Neue Medien,
Ludwig-Maximilians-Universität München, München, Deutschland
E-Mail: thess@lmu.de

V. Thürmel
E-Mail: thuermel@lmu.de

M. Teebken
E-Mail: teebken@lmu.de

C. Matt
Institut für Wirtschaftsinformatik, Universität Bern, Bern, Schweiz
E-Mail: christian.matt@iwi.unibe.ch

A. Roßnagel und M. Friedewald (Hrsg.), *Die Zukunft von Privatheit und Selbstbestimmung,* DuD-Fachbeiträge,
https://doi.org/10.1007/978-3-658-35263-9_3

Ebenso stehen leistungsfähige, IT-gestützte Verfahren zur Auswertung dieser Daten zur Verfügung, die darauf aufbauend Prognosen zukünftiger Entwicklungen ableiten können.[1]

In einer derartigen „Datenökonomie“ entstehen zahlreiche Möglichkeiten für Unternehmen, wie etwa bessere Einblicke in das Konsumentenverhalten oder die Identifikation von Interessen und Verhaltensmustern.[2] Verfügt ein Anbieter über mehr Informationen über (potentielle) Kunden, so kann er generell ein zielgruppengerechteres Angebot erstellen und komplementäre Güter anbieten. Auch ist die Nutzung von Kundendaten teils essentiell für das Erbringen bestimmter datengetriebener Dienstleistungen und kritisch für die Innovationstätigkeit zahlreicher Unternehmen, insbesondere für Startups.[3] So erproben Unternehmen aktuell Erlösmodelle, die auf der verstärkten Verwertung „personenbezogener Daten“ beruhen. Ebenfalls bieten Daten auch direktes Monetarisierungspotenzial; sie werden zu einem ökonomisch handelbaren Gut, welches durch spezialisierte Anbieter auf sogenannten Datenmärkten angeboten wird.[4]

Auch für Konsumenten hat diese Entwicklung durchaus Vorteile, wie etwa eine bessere Anpassung von Dienstleistungen anhand von deren Präferenzen sowie schnellere und zielgerichtetere Suchmöglichkeiten. Ebenso haben Konsumenten verstärkt die Möglichkeit, personenbezogene Daten als eine Art Zahlungsmittel einzusetzen, um hierdurch bspw. Apps kostenfrei nutzen zu können. Im ersten Schritt ist hierfür jedoch die Preisgabe von Daten durch den Konsumenten erforderlich und diese wird im Kontext der zunehmenden Digitalisierung häufig kritisch diskutiert. Auch hier ist das Zusammenspiel von Anbieter und Nachfrager eine geeignete Sichtweise zur Illustration des Basiskontexts. Ein (potentieller) Kunde wird generell abwägen, ob er der Verwendung von Daten zustimmt. Die Preisgabe von Daten wird vom Konsumenten häufig per se zunächst als tendenziell risikoreich eingeschätzt. Demgegenüber muss ein positiver Nutzen stehen, der die möglichen Risiken aufwiegt. Das Individuum berücksichtigt bei dieser Entscheidung ein ökonomisches Kalkül, am Ende dessen die Entscheidung für oder gegen die Nutzung eines Dienstes steht.[5] Je mehr Daten ein Anbieter erfragt, umso höher muss der daraus resultierende Nutzen

[1] Kelleher et al. (2015).

[2] Ochs et al. (2019).

[3] Martin et al. (2019).

[4] Bründl et al. (2015).

[5] Dinev und Hart (2006).

für den Konsumenten sein, um diesen zur Preisgabe seiner Daten zu bewegen. „Pokert" ein Anbieter zu hoch und verlangt sehr viele Daten, kann dies zwar durchaus legal sein, aber möglicherweise den Konsumenten von der Nutzung des Dienstes abhalten.

Im Rahmen dieser grundlegenden Austauschbeziehung stellen sich zentrale ökonomische Fragen der Gestaltung und Regulierung in der digitalisierten Welt, welche jeweils im Hinblick auf aktuelle technologische Entwicklungen zu betrachten sind. So hat etwa die zuvor genannte zentrale Abwägung einer Datenpreisgabe in sozialen Netzwerken heutzutage oftmals nicht nur Auswirkungen auf den Teilenden, sondern auch auf andere Personen, etwa wenn diese auf geteilten Bildern ebenfalls zu erkennen sind. Folglich gestaltet sich diese zentrale Entscheidungssituation für Individuen zunehmend komplexer und erfordert einen gewissen kognitiven Aufwand – nicht selten entscheiden hier nicht ausschließlich rationale Faktoren. Gleichzeitig versuchen Anbieter oftmals mittels sogenannter Nudging-Techniken[6] Verbraucher zur Preisgabe von personenbezogenen Daten zu bewegen, was gerade im Kontext von sehr sensitiven – und somit für den Anbieter häufig auch besonders wertvollen – Daten (etwa Gesundheitsdaten) oftmals schwierig ist.

Die personenbezogenen Daten haben somit sowohl für die Konsumenten als auch für die anfragenden Unternehmen einen Wert und einen damit verbundenen Preis. Es zeigt sich somit ein facettenreiches Bild hinsichtlich der zugrunde liegenden Austauschbeziehung zwischen Unternehmen und Konsumenten. Dieser Beitrag verfolgt das Ziel, anhand einzelner exemplarischer Kontexte, das ökonomische Verständnis von Privatheit als Wechselspiel zwischen Anbieter und Nachfrager aufzuzeigen und insbesondere mittels aktueller Erkenntnisse zu erweitern. Der Beitrag ist wie folgt strukturiert: In Abschn. 2 präsentieren wir ein wirtschaftswissenschaftliches Verständnis von Privatheit und stellen die vier relevantesten Forschungsstränge aus Sicht von Unternehmen dar. In Abschn. 3 beschreiben wir zwei unserer Untersuchungen, die sich aus der originären Sicht von Unternehmen mit der Nutzung personenbezogener Daten beschäftigen. Abschn. 4 widmet sich drei von uns durchgeführten Studien, die sich dem Thema aus Sicht der Konsumenten nähern. Wir schließen den Beitrag mit einer Zusammenfassung und dem Ausblick in Abschn. 5 ab.

[6] Schöning et al. (2019).

2 Privatheit aus der Sicht der Wirtschaftswissenschaften

2.1 Grundlegendes Verständnis von Privatheit

Das Konzept der Privatheit wird von unterschiedlichen Disziplinen behandelt, was zu einer Vielzahl von verschiedenen Konzeptualisierungen und Definitionen des Begriffs führt.[7] In Morlok et al.[8] beschreiben wir den zeitlichen Wandel und die disziplinspezifischen Unterschiede des Privatheitskonzepts. Charakteristisch für die Privatheitsforschung ist das hohe Maß an unterschiedlichen Zugängen zum Thema. Anfänglich wurde Privatheit explizit als physische Privatheit verstanden. Diese physische Privatheit bezieht sich auf den körperlichen Zugang zu einem Individuum und dessen räumlicher Umgebung. Im juristischen Kontext wird Privatheit, resultierend aus der physischen Privatheit, definiert als das „Recht, alleine gelassen zu werden"[9]. Weiterhin wird die Privatheit in der Philosophie und der Psychologie beschrieben als der „Zustand des begrenzten Zugangs oder der Isolation".[10] Dagegen wird die Privatheit in den Sozialwissenschaften als ein soziales Problem oder als ein Verhaltenskonzept begriffen.[11]

Im Kontext des vorliegenden Beitrags steht das Konzept der informationellen Privatheit im Fokus, welches den Zugang zu Informationen, die explizit einer Person zuordenbar sind, beschreibt.[12] Im Zentrum der allgemeinen ökonomischen Definition des Begriffs Privatheit steht die Definition von Privatheit als Kontrolle und als Fähigkeit zur Kontrolle.[13] Angewandt auf informationelle Privatheit umfasst dies die Kontrolle über die Preisgabe und die Verwendung von Informationen.[14] Die Wirtschaftswissenschaften adressieren dabei häufig Fragen der Verwendung von *personenbezogen* Daten durch Unternehmen. Unter dem Begriff personenbezogen fallen nicht nur explizit preisgegebene Daten, sondern auch unbewusst geteilte Daten, etwa über das Nutzungsverhalten im Internet.

[7] Smith et al. (2011).

[8] Morlok et al. (2018).

[9] Warren und Brandeis (1890).

[10] Schoeman (1984).

[11] Margulis (2003).

[12] Smith et al. (2011).

[13] ebd, Westin (1967).

[14] Awad und Krishnan (2006), Hann et al. (2007).

Nach Morlok et al.[15] ist es ebenfalls wichtig, beim Umgang mit dem Thema Privatheit auf die unterschiedlichen Akteure und Betrachtungsebenen einzugehen. Wesentliche Akteure sind Unternehmen und Konsumenten und deren Wechselspiel. Auf diese Akteure konzentrieren wir uns nachfolgend. Bei den Unternehmen ist neben der Betrachtung des Unternehmens als Ganzes auch die Betrachtung der in einem Unternehmen agierenden Individuen (Mitarbeiter, Manager) möglich. Konsumenten betrachten wir – etwas vereinfachend – auf Individualebene.

Aus wirtschaftswissenschaftlicher Sicht ebenfalls wichtig sind die Rahmenbedingungen des Zusammenwirkens von Unternehmen und Verbrauchern, sei es in konkreten Marktkonstellationen oder durch Regulationen vorgegeben. Dieses sehr umfassende Themenfeld klammern wir nachfolgend aus.

2.2 Relevante Forschungsstränge

In Morlok et al.[16] geben wir einen Überblick über die wesentlichen Forschungsstränge der Literatur im Bereich der Wirtschaftswissenschaften. Bezüglich des Zusammenspiels von Unternehmen und Verbrauchern findet sich eine beachtliche Zahl von Studien zu den Themen Personalisierung und Preisdifferenzierung.

Unternehmen können ihre Angebote personalisieren, indem sie auf Basis der gesammelten Konsumentendaten die Verhaltensweisen und Präferenzen ihrer Kunden verstehen und sich dementsprechend ausrichten. Forschung über die personalisierte Ansprache durch die Verwendung von personenbezogenen Daten beschäftigt sich mit einer Vielzahl von Themengebieten. Kern der Forschung in diesem Bereich ist, dass Unternehmen möglichst viele personenbezogene Daten auswerten möchten, um ihre Kunden bestmöglich ansprechen zu können. Auf der einen Seite schätzen Kunden die Vorteile der Personalisierung, auf der anderen Seite haben sie häufig Privatheitsbedenken, wenn Angebote durch die Analyse ihrer personenbezogenen Daten entstehen. Dieses Phänomen wird als „Personalization Privacy Paradox“ bezeichnet.[17] Forschung in Bezug auf

[15] Morlok et al. (2018).

[16] Morlok et al. (2017).

[17] z. B. Xu et al. (2011).

die individualisierte Kundenansprache fokussiert sich darauf, unter welchen Bedingungen und zu welchem Grad Unternehmen Systeme zur Personalisierung einsetzen können, ohne dass Konsumenten sich durch die Personalisierung bedroht fühlen. Beispielsweise untersuchen Karwatzki et al.[18], wie digitale Services gestaltet werden sollten, um den Kunden trotz Privatheitsbedenken zum Teilen von personenbezogenen Daten zu bewegen.

Auch zur Preisdifferenzierung finden sich eine Reihe interessanter Studien. Unternehmen können die gesammelten Daten verwenden, um die Zahlungsbereitschaft ihrer Konsumenten präziser als bisher zu bestimmen. Die Vorhersage der Zahlungsbereitschaft von Kunden ermöglicht den Unternehmen die Preisdiskriminierung zumindest bestimmter Kundengruppen, im Einzelfall sogar einzelner Kunden. Im Gegensatz zur Personalisierung geht die Preisdiskriminierung zumeist mit monetären Nachteilen für den Kunden einher.[19]

Personenbezogene Daten können von Unternehmen zudem genutzt werden, um das Verhalten ihrer Mitarbeiter zu steuern. Dies wird in einem dritten, relativ neuen Themenfeld, aufgegriffen. Beispielsweise kann Software zur Überwachung in Unternehmen die Produktivität, das Arbeitsverhalten oder die Bewegungsmuster von Mitarbeitern verfolgen. Unabhängig von der rechtlichen Betrachtungsweise von Überwachung am Arbeitsplatz ergeben sich ökonomische Fragestellungen bezüglich der Privatheit der Mitarbeiter. Literatur in dem unternehmensinternen Kontext beschäftigt sich mit den Auswirkungen von Überwachung auf das Unternehmen und auf dessen Mitarbeiter. So untersuchen Connolly und McParland[20] welchen Einfluss digitale Technologien am Arbeitsplatz auf die Privatheitsbedenken von Arbeitnehmern haben. Des Weiteren beschäftigt sich Literatur zur Privatheit von Jobbewerbern insbesondere mit der Diskriminierung von Bewerbern. In diesem Teilaspekt geht es darum, dass Arbeitgeber auf unterschiedlichen Wegen Zugang zu Informationen von Bewerbern haben, da diese ihre Daten in sozialen Netzwerken teilen.[21] Demnach können im Rahmen der Bewerberauswahl künftige Arbeitgeber gezielt nach Informationen von Bewerbern suchen und diese auswerten. Der öffentliche Zugang zu privaten Informationen wie täglichen Aktivitäten oder privaten Interessen wird durch soziale Netzwerke gefördert.

[18] Karwatzki et al. (2017).

[19] Acquisti et al. (2016).

[20] Connolly und McParland (2012).

[21] Acquisti und Fong (2020).

Jenseits von der unternehmensinternen Nutzung von Daten können Unternehmen von personenbezogenen Daten profitieren, wenn sie diese an Dritte weiterverkaufen. Der vierte ebenfalls noch recht kleine Literaturstrang beschäftigt sich daher mit der ökonomischen Verwertung von Konsumentendaten, die auf internetbasierten Plattformen gesammelt werden. Plattformen können die von ihnen gesammelten Daten an Werbetreibende oder an Datenintermediäre verkaufen, die die Daten anschließend weiterverwerten. Literatur in diesem Bereich beschäftigt sich häufig mit der sekundären Nutzung von personenbezogenen Daten, wenn Informationen von Unternehmen an Drittanbieter oder Datenhändler weitergegeben werden. Hartmann et al.[22] untersuchen Geschäftsmodelle von Startups, die sich auf personenbezogene Daten als Schlüsselressource spezialisieren. Die Hauptaktivität dieser Unternehmen besteht in der Aggregation, Analyse oder Generierung von Daten aus unterschiedlichen Quellen. Welchen Herausforderungen Unternehmen beim Datenhandel gegenüberstehen und welche unternehmensinternen Voraussetzungen sie treffen sollten, wird von Wixom und Ross[23] beschrieben.

3 Personenbezogene Daten als unternehmerische Ressource

Nachfolgend stellen wir zwei Studien vor, die wir in ökonomischen Teilprojekten in den letzten Jahren durchgeführt haben. Die Studien beschäftigen sich mit der unternehmensinternen und -externen Verwendung von Daten.

3.1 Unternehmen als Teil von Datenmärkten und Wertschöpfungsstrukturen für Daten

Im Rahmen einer explorativen Studie haben wir uns in Bründl et al.[24] genauer mit der Struktur von und der Wertschöpfung in Datenmärkten und den damit verbundenen Rollen von Unternehmen auseinandergesetzt. Um tiefere Einblicke in den Markt für personenbezogene Daten zu erhalten, haben wir Experten aus

[22] Hartmann et al. (2016).

[23] Wixom und Ross (2017).

[24] Bründl et al. (2016).

datengetriebenen Unternehmen für echtzeitbasierte Online-Werbung (Real-Time-Advertising) befragt. Mit einem geschätzten Marktvolumen von zum Zeitpunkt der Studie 1,6 Mrd. Euro p. a. ist dies der größte Teilmarkt. Ziel der Experteninterviews war es, zu erfahren, welche Geschäftsmodelle und Anwendungsbeispiele für den Datenhandel vorliegen, welchen monetären Wert Daten auf diesem Markt haben und welche Faktoren den Datenwert beeinflussen. Mit Hilfe der Interviews konnten wir konzeptualisieren, wie Wertschöpfungsstrukturen aussehen, wie der Wert von Daten festgelegt wird und welche Akteure in diesem Prozess beteiligt sind. Im Folgenden fassen wir die Hauptergebnisse der empirischen Studie zusammen.

Akteure

Wir differenzieren sieben Rollen, die sich im Datenmarkt bewegen: *Advertiser, Publisher, Demand-, Supply-Side-Plattformen, Datensammler, Data-Exchange- und Data-Management-Plattformen* (Abb. 1). Wertschöpfungsaktivitäten werden von Datensammlern initiiert. Diese generieren unterschiedliche Arten von Daten und nutzen diese sowohl für eigene Zwecke, als auch für den Verkauf an andere Akteure. Datensammler sind vor allem Anbieter von Online-Plattformen, auf

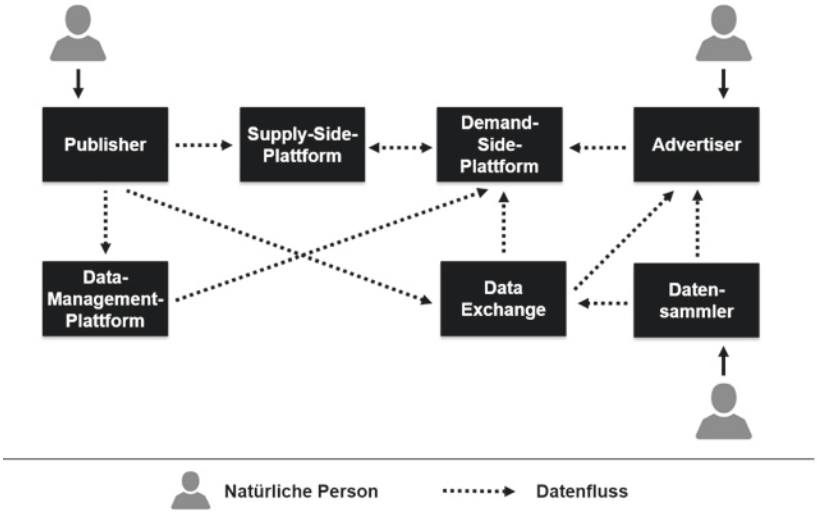

Abb. 1. Wertschöpfungskette für personenbezogene Daten (Quelle: Bründl et al. 2016)

denen kostenfreie Dienste angeboten werden. Diese kostenlosen Dienste werden finanziert durch die Weitergabe der gesammelten Daten an Dritte. Am anderen Ende der Wertschöpfungskette stehen Advertiser (Werbetreibende). Diese wollen ihre Produkte oder Dienste an potentielle Kunden vermarkten. Um auf die digitalen Werbeplätze der Publisher zugreifen zu können, nutzen sie die Dienste von Intermediären (Demand-Side-Plattformen). Damit die Werbung an spezielle Kundensegmente ausgeliefert werden kann, ziehen Demand-Side-Plattformen personenbezogene Daten der Kunden heran. Publisher offerieren auf Webseiten oder in mobilen Applikationen digitale Werbeplätze. An dieser Stelle greifen Publisher auf Intermediäre in Form von Supply-Side-Plattformen zurück, damit sie ihre eigenen Werbeplätze gewinnmaximierend anbieten können. Durch Supply-Side-Plattformen können Publisher ihre Werbeplätze automatisiert in Echtzeit vermarkten (*Real-Time-Bidding*). Supply-Side-Plattformen übermitteln den verfügbaren Werbeplatz und Kontakteigenschaften an Demand-Side-Plattformen. Wenn die übertragenen Eigenschaften vom Werbeplatz mit den vom Advertiser gestellten Anforderungen übereinstimmen, bieten Demand-Side-Plattformen automatisiert einen vordefinierten Preis. Letztendlich erhält den Werbeplatz für den spezifischen Kontakt der höchstbietende Advertiser. So wirken Demand-Side-Plattformen als Intermediäre, durch die Advertiser datengetriebene, zielgruppengerechte Werbekontakte in automatisierter Form erwerben können. Demand-Side-Plattformen aggregieren Daten von Supply-Side-Plattformen, Data-Management-Plattformen und Data Exchanges, um verfügbare Angebote mit den Anforderungen von Advertisern in Einklang zu bringen. Data-Management-Plattformen nutzen Algorithmen des maschinellen Lernens, um Akteure bei Zielgruppenidentifikation zu unterstützen, indem sie die Charakteristika von Kundensegmenten einschätzen. Oftmals eng verknüpft mit Data-Management-Plattformen sind Data Exchanges. Diese wirken als Handelsplätze von Third-Party-Daten von potentiellen Zielgruppen und geben so Auskunft über spezielle Kundensegmente.

Wertschöpfungsstrukturen

Wir beschreiben die Wertschöpfung im Umgang mit Daten auf der Unternehmensebene anhand von vier aufeinanderfolgenden Schritten. Im ersten Schritt werden personenbezogene Daten durch Unternehmen gesammelt. Nachfolgend werden die gesammelten Daten aufbereitet und aggregiert. Im dritten Schritt werden die Daten auf gewisse Muster analysiert. Schließlich können die Daten im letzten Schritt distribuiert und genutzt werden. Der Datenmarkt stellt durch seine Wertschöpfungsprozesse für Unternehmen einen interessanten Anknüpfungspunkt dar. Anhand der Darstellung können Unternehmen geeignete Partner

identifizieren, um ihre vorhandene Datenbasis zu monetarisieren. Die Erhebung von bislang unbeachteten Daten kann sich anbieten, um neue Erlösquellen zu erschließen. Gleichzeitig müssen die Interessen der Kunden und rechtliche Erfordernisse beachtet werden.

In Anbetracht aktueller Entwicklungen des Datenmarkts, wird dieser in Zukunft voraussichtlich an Relevanz gewinnen. Die Menge an verfügbaren Daten wächst durch Trends wie das Internet der Dinge und Big Data weiter an. Auf der einen Seite führt das steigende Angebot an Daten bei gleichbleibender Nachfrage zu sinkenden Preisen. Auf der anderen Seite steigt die Datenqualität wegen zunehmender Möglichkeiten der Vernetzung weiter an. Der zunehmende Preis für personenbezogene Daten stellt ein monetäres Potential für Unternehmen dar. Die zunehmende Generierung von Daten, verbunden mit dem Potential diese Daten gewinnbringend auszuwerten, führt zu einer zunehmenden Bedeutung des Datenhandels und der Rolle von Daten für Unternehmen.

3.2 Daten als Ressource für Unternehmen

Heutzutage sammeln Unternehmen eine zunehmend große Menge an Daten aus unterschiedlichen Quellen. Wenn heterogene Datensets aus unterschiedlichen Quellen miteinander kombiniert werden, kann dies zu vielversprechenden unternehmensinternen Vorteilen führen.[25] Miteinander kombinierte Daten haben einen höheren Wert als Daten, die einzeln betrachtet werden. In Weibl und Hess[26] beschäftigen wir uns mit der Frage, wie Synergieeffekte aus kombinierten Daten konzeptualisiert werden können und wie Synergieeffekte zu unternehmerischen Vorteilen führen.

Ansatz

Die Ergebnisse der Arbeit sind in einem konzeptionellen Framework dargestellt (Abb. 2). Theoretische Basis für das Framework bilden die Systemtheorie und das Konzept von Synergie nach Nevo und Wade.[27] Die Systemtheorie stellt die theoretische Grundlage des Konzepts synergistischer Ressourcen dar[28] und zeigt

[25] Shollo und Galliers (2016).

[26] Weibl und Hess (2020).

[27] Nevo und Wade (2010).

[28] Someh und Shanks (2013).

Abb. 2. Konzeptionelles Modell von Datensynergien (basierend auf Weibl und Hess, 2020)

auf, dass Systeme im Ganzen betrachtet werden sollten.[29] Synergistische Interaktionen zwischen Komponenten eines Systems führen dazu, dass ein System nicht nur aus der Summe seiner Komponenten, sondern auch aus deren Interaktionen besteht.[30] Synergien werden in der Literatur in unterschiedlichen Fachbereichen und aus verschiedenen Perspektiven betrachtet. Nevo und Wade[31] stellen das Konzept von Synergien in der Wirtschaftsinformatik in einem konzeptuellen Framework dar. Dieses beinhaltet in einer ersten Stufe potentielle Synergien aus IT-Ressourcen und organisatorischen Ressourcen. In der zweiten Stufe werden potentielle Synergien mit organisatorischen Voraussetzungen verbunden, damit Synergien praktisch realisiert werden können.

Methodisch verfolgen wir in Weibl und Hess[32] einen zweistufigen Ansatz. In einem ersten Schritt konstruieren wir ein initiales Modell der Datensynergien aus relevanter Literatur. Das Framework der Synergieeffekte nach Nevo und Wade[33] dient an dieser Stelle als Ausgangspunkt. In Kombination mit einer strukturierten Analyse weiterer relevanter Literatur bilden wir ein initiales Framework der Datensynergien. Dieses erste Framework wird in einem zweiten Schritt durch 24

[29] Ackoff (1971).
[30] ebd.
[31] Nevo und Wade (2010).
[32] Weibl und Hess (2020).
[33] Nevo und Wade (2010).

semi-strukturierte Experteninterviews verfeinert. Die ausgewählten Interviewpartner arbeiten als Datenexperten innerhalb von unterschiedlichen Unternehmen und erfüllen verschiedene Positionen. Die Kombination aus Theorie und Empirie führt zu dem konzeptuellen Modell von Datensynergien (Abb. 2). Das Framework stellt dar, welche Voraussetzungen für die Realisierung von Synergien getroffen werden sollten. Außerdem zeigt es auf, welche Arten von Synergieeffekten durch die Kombination von Daten entstehen können.

Voraussetzungen auf Management-Ebene

Die Ergebnisse zeigen fünf Voraussetzungen auf, die das Erschließen von Datensynergien ermöglichen. Diese beziehen sich auf die Managementebene und auf die Eigenschaften der verwendeten Daten. Zwei Bedingungen für die erfolgreiche Synergie von Daten müssen von Seiten des Managements erfüllt werden: Integration und Kontextualisierung.

Obwohl Daten fast augenblicklich über weite Entfernungen transportiert werden können, hat unsere Studie gezeigt, dass Unternehmen spezielle Vorkehrungen zur Integration und Zentralisierung von Daten in ganzheitlichen Data Warehouses (sog. Data Lakes) treffen sollten. Die Sammlung von Daten in Data Lakes bringt mehrere Vorteile mit sich: Auf der einen Seite bietet die zentrale Speicherung von Daten den Vorteil, dass Datenwissenschaftler und Entscheidungsträger einen holistischen Überblick über die vorhandenen Datensätze erhalten und diese so einfacher zu Synergien kombinieren können. Auf der anderen Seite muss gewährleistet sein, dass auf diese Daten von unterschiedlichen Funktionen und Divisionen im Unternehmen zugegriffen werden kann. Dementsprechend ist es die Aufgabe des Managements, die Datenspeicherung in Silos aufzubrechen, um Daten in einem ganzheitlichen System speichern zu können. Dieser Schritt der Datenintegration ermöglicht die (Re-)Kombination von Daten und stellt die Basis für die Erschließung von Datensynergien dar.

Die Kontextualisierung und Verknüpfung von Daten durch das Management eines Unternehmens ist unerlässlich. Um die Verbindung von Daten zu ermöglichen, sollten Unternehmen mit einem geschäftsorientierten Anwendungsfall starten und Daten insofern kombinieren, dass Hypothesen über ihre synergistische Beziehung bestätigt werden können. In dieser Art kann der geschäftsgetriebene Anwendungsfall den Impuls geben, passende Datenquellen zu kombinieren. Ein beispielhafter Anwendungsfall ist die Zusammenführung von Daten, um Erkenntnisse für die Planung einer Marketingkampagne zu erhalten. Die Kombination von bestimmten Datenquellen ist nur dann erfolgreich, wenn Teilinformationen aus unterschiedlichen Kontexten in einer wertstiftenden Form subsumiert werden.

Datenbezogene Voraussetzungen

Zusätzlich zu den managementbezogenen Voraussetzungen müssen drei datenbezogene Voraussetzungen erfüllt werden, um Synergieeffekte zwischen Daten zu fördern: Kompatibilität, Datenqualität und Speicherinfrastruktur.

Wie bereits beschrieben, müssen heterogene Ressourcen miteinander kompatibel sein, um Synergieeffekte zu ermöglichen. So wird sichergestellt, dass Ressourcen nahtlos miteinander verbunden werden können.[34] Die Interviews haben aufgezeigt, dass ein gemeinsamer Schlüssel benötigt wird, damit Daten miteinander verbunden werden können. Dies kann beispielsweise eine zeitliche Dimension sein oder auf Produktebene die Artikelnummer. Darüber hinaus müssen heterogene Datenformate gemeinsame Eigenschaften haben, damit diese in Kombination miteinander genutzt werden können.

Weiterhin wurde in den Interviews eine hohe Qualität der Daten als unerlässlich beschrieben. Dies ist besonders im E-Commerce von hoher Relevanz: Wenn es Datenprobleme im Tracking von Produkten gibt und somit die Verfügbarkeit von Produkten nicht aktualisiert wird, kann dies zu Problemen bei Bestellungen führen. Daher ist eine hohe Datenqualität eine integrale Voraussetzung, um Synergien aus Datenquellen zu schaffen.

Eine weitere entscheidende Voraussetzung ist die Bereitstellung der benötigten Infrastruktur um unterschiedliche Daten aus verschiedenen Quellen in einer einheitlichen Weise zu speichern. Im Gegensatz zu anderen organisatorischen Ressourcen, können Daten schnell und über lange Zeiträume hinweg gespeichert werden und augenblicklich über weite Distanzen transferiert werden. Viele Organisationen verlassen sich im hohem Maße auf externe Cloud-Lösungen (z. B. Microsoft Azure) und zusätzlich verwaltete Services als bevorzugte Speicherform. Auf diese Weise können Datensätze in effizienter Form in Data Lakes gespeichert werden.

Erhöhter Informationswert durch Synergieeffekte

Der erhöhte Informationswert von kombinierten Daten wird durch einen multidimensionalen Blick auf die gesammelten Daten erreicht. Ein einzelner Datensatz hat nur einen begrenzt informativen Charakter. Wenn jedoch mehrere Datensets miteinander kombiniert werden, kann dies den Informationscharakter erhöhen.

Beispielsweise kann die Kombination von historischen Verkaufszahlen mit Standort- und Zeit-Daten zu der Erkenntnis führen, wie viele Produkte

[34] Someh und Shanks (2013).

an bestimmten Tagen zur Verfügung stehen sollten. Eine der befragten Organisationen hat die Verkaufsdaten aus bestimmten Produktkategorien mit Kundendaten kombiniert, um zu sehen, für welche Produktgruppen sich bestimmte Kunden besonders interessieren. Die getrennte Betrachtung von Verkaufszahlen oder Kundenzahlen würde es nicht ermöglichen, etwaige Korrelationen zu erkennen und daraus Segmente zu identifizieren, um neue Erkenntnisse zu gewinnen.

Die synergistische Interaktion zwischen Daten ermöglicht die Betrachtung eines Subjektes aus unterschiedlichen Betrachtungswinkeln. Durch die Aggregation von Daten können bestimmte Muster festgestellt werden, beispielsweise im Online-Kundenverhalten. Unternehmen können neue Erkenntnisse über das Kundenverhalten erlangen, indem sie Transaktionsdaten von Kunden mit personenbezogenen Daten oder dem Online-Surfverhalten verbinden. Die Kombination dieser Daten ermöglicht Einblicke in die Online-Aktivitäten von Kunden und vor allem in die Bedürfnisse von Konsumenten und deren Interessen. Als Folge der gewonnenen Erkenntnisse über den Kunden, können Unternehmen ihre Online-Präsenz optimieren oder Kunden personalisierte Inhalte ausspielen.

Tangible Vorteile in Form von erhöhten Transaktionswerten

Unsere Studie zeigt auf, dass Daten-Synergieeffekte zu tangiblen Vorteilen in Form von individualisierten Marktangeboten und automatisierten Geschäftsprozessen führen können. Die Möglichkeit Daten zu strukturieren und zu segmentieren, erlaubt es Unternehmen, spezielle Kundengruppen mit Angeboten gezielt zu adressieren. Beispielsweise hat einer der Experten angegeben, dass seine Organisation Daten kombiniert mit dem Ziel, Kundenabwanderung zu verhindern. Das Unternehmen erreichte dies, indem es Transaktionsdaten der Kunden mit Informationen über Kunden-Berührungspunkte, den Suchhistorien im Online-Shop und demografischen Daten verbunden hat. Die Kundeninformationen, die so aus mehreren Quellen kombiniert wurden, geben dem Unternehmen ein vervollständigtes Bild über den Kunden.

Laut der befragten Experten kann die Kombination von Daten zu verbesserten und automatisierten Reportingprozessen führen. Daher wird die Datenkombination als typische „quick win“ Aktion in Datenprojekten angesehen. Einer der Datenexperten hat angegeben, dass seine Organisation die managementbezogenen Indikatoren aus unterschiedlichen Quellen effizienzsteigernd zu einem automatisierten Reporting Prozess transformiert hat, indem Rohdaten aus den Data Warehouses verbunden und im Anschluss visuell dargestellt wurden.

Ziel der Studie war es, das synergistische Potential der Wertgenerierung aus Daten zu untersuchen. Daten als Ressource führen durch ihre spezifischen

Eigenschaften auf andere Weise zu synergistischen Interaktionen als andere organisatorische Ressourcen. Die Kernergebnisse aus der Studie von Weibl und Hess[35] führen zu einem konzeptionellen Framework, das im ersten Schritt bestimmte Voraussetzungen beschreibt, die notwendig sind, um synergistische Interaktionen zu ermöglichen. Im zweiten Schritt werden die Ergebnisse der Synergieeffekte beschrieben: Daten in kombinierter Form führen zu einem erhöhten Informations- und Transaktionswert durch automatisierte Entscheidungsfindung und Effizienzsteigerung im Unternehmen.

4 Die Verbraucherperspektive

Verbraucher produzieren Daten als „Nebenprodukt". Für sie stellt sich die Frage, ob sie dieses Nebenprodukt behalten oder weitergeben wollen. Nachfolgend stellen wir drei Studien vor, in denen wir uns diesem Thema aus unterschiedlichen Perspektiven nähern.

4.1 Zahlungsbereitschaft für Privatheit

Dank des interaktiven Charakters digitaler Medien, können Unternehmen große Mengen an personenbezogenen Informationen über Konsumenten und deren Verhaltensweisen erfassen und analysieren. Viele Anbieter haben die resultierenden kommerziellen Möglichkeiten genutzt und neue Geschäftsmodelle entwickelt, die von den gesammelten personenbezogenen Daten profitieren. Doch die Kommerzialisierung personenbezogener Daten löst bei vielen Konsumenten Privatheitsbedenken aus, die zur Beendigung der Nutzung entsprechender Dienste führen können und somit langfristig ein unternehmerisches Risiko für die Anbieter darstellen. Daher ist es ein neuer Ansatz, den Wert personenbezogener Daten zu monetarisieren. Dieser Ansatz basiert auf der Annahme, dass, obwohl es einige Verbraucher bevorzugen Online-Dienste im Austausch gegen die Bereitstellung personenbezogener Informationen kostenlos zu nutzen, andere es vorziehen, für den Schutz ihrer Privatsphäre zu bezahlen. So können Anbieter sozialer Netzwerke den Konsumenten neben einer kostenlosen Version im Austausch gegen ihre personenbezogenen Informationen auch eine Premium-Version mit zusätz-

[35] Weibl und Hess (2020).

lichen Funktionen zur Kontrolle der Privatsphäre anbieten. Dies erlaubt den Verbrauchern zu entscheiden, ob sie für ihre Privatsphäre bezahlen wollen oder nicht. Bisherige Forschung hat aufgezeigt, dass dieses sogenannte Privatheits-Freemium Modell gleich zwei Probleme lösen kann: Einerseits bietet es Anbietern sozialer Netzwerke die Möglichkeit mit nutzergenerierten Inhalten Geld zu verdienen und andererseits können auf diese Weise die Datenschutzbedenken der Konsumenten bei der Verwendung sozialer Netzwerke adressiert werden.[36]

Empirische Untersuchung der Zahlungsbereitschaft für Privatheit

Allerdings hatte die Forschung bis zu diesem Zeitpunkt noch keine theoretische Erklärung für die Zahlungsbereitschaft der Konsumenten für Privatheit gefunden. Vor diesem Hintergrund haben wir uns in Schreiner und Hess[37] mit Höhe und Determinanten der Zahlungsbereitschaft für Privatheit beschäftigt. In dieser Studie haben wir anhand einer Online-Umfrage die Zahlungsbereitschaft der Konsumenten für eine zahlungspflichtige Premium-Version von Facebook untersucht. Mittels der *Theory of Planned Behavior*[38], wollten wir die tatsächliche Zahlungsbereitschaft für Privatheit der Konsumenten bestimmen. Die *Theory of Planned Behavior* wurde bereits in vielen Studien der Wirtschaftswissenschaften als theoretischer Rahmen zur Erklärung des Verhaltens von Individuen angewandt. Die Theorie besagt, dass die Verhaltensweise von Individuen basierend auf ihrer Einstellung gegenüber dem Verhalten, subjektiven Normen und der wahrgenommenen Verhaltenskontrolle vorhergesagt werden kann. In Schreiner und Hess[39] haben wir diesen theoretischen Rahmen auf den Kontext unserer Studie angewandt und um drei Antezedenten der Einstellung erweitert: Wahrgenommenes Risiko der Privatheit, wahrgenommene Nützlichkeit und Vertrauen. Unter dem wahrgenommenen Risiko der Privatheit verstehen wir die Unsicherheit der Konsumenten bezüglich möglicher negativer Konsequenzen, die die Nutzung sozialer Netzwerke mit sich bringen kann. Folglich stellen wir die Hypothese auf, dass das wahrgenommene Risiko der Privatheit im digitalen Kontext die Einstellung der Verbraucher gegenüber einer Premium-Version mit

[36] Schreiner und Hess (2013).

[37] Schreiner und Hess (2015).

[38] Ajzen (1991).

[39] Schreiner und Hess (2015).

zusätzlichen Funktionen zur Kontrolle der Privatsphäre positiv beeinflusst. Des Weiteren vermuten wir, dass die Einstellung gegenüber der Premium-Version positiv beeinflusst wird, wenn Konsumenten einen Mehrwert der angebotenen Funktionen in Bezug auf die Verbesserung des Datenschutzes sehen. Außerdem stellen wir die Hypothese auf, dass Vertrauen in die Premium-Version die Einstellung der Konsumenten gegenüber der Nutzung der Premium-Version positiv beeinflusst.

Das resultierende Forschungsmodell haben wir anhand einer Online-Umfrage getestet.[40] Hierfür haben wir den Teilnehmern der Umfrage eine Premium-Version des sozialen Netzwerks Facebook vorgestellt. Im Vergleich zu der kostenlosen Basisversion, hatte diese Version zusätzliche Funktionen, um die Erfassung, Nutzung, Weitergabe und Speicherung personenbezogener Daten zu kontrollieren. So können Konsumenten der Premiumversion beispielsweise bestimmen, welche ihrer personenbezogenen Daten erfasst und für welche Zwecke diese genutzt wurden. Im Anschluss hatten die Teilnehmer die Möglichkeit, ihren Basis-Facebook-Account zu erweitern, um zusätzliche Kontrollfunktionen für ihre Privatsphäre zu erhalten. Um die tatsächliche Zahlungsbereitschaft der Teilnehmer für die Premiumversion zu erfassen, haben wir eine anreizkompatible Methodik genutzt. Hierfür wurde den Teilnehmern erzählt, dass der Preis für die Premiumversion noch nicht festgelegt worden ist und dass sie entscheiden können, ob und wieviel sie pro Monat für die Premiumversion zahlen wollen. Ist ihr Gebot mindestens so hoch wie ein automatisch generierter Zufallspreis, können sie die Premiumversion zu diesem Preis nutzen. Ist das Gebot dahingegen niedriger als der zufällig generierte Preis, können sie die Premiumversion nicht nutzen und müssen den Preis auch nicht zahlen. Dieses Vorgehen hat es uns ermöglicht, die tatsächliche Zahlungsbereitschaft der Teilnehmer zu erfassen.

Die angegebene Zahlungsbereitschaft der Teilnehmer bewegte sich zwischen 0 und 15 € mit einer durchschnittlichen Zahlungsbereitschaft von 0,63 € für die Premiumversion.

Das resultierende Strukturgleichungsmodel ist in Abb. 3 dargestellt. Die Ergebnisse unserer Studie zeigen, dass die wahrgenommene Nützlichkeit und das Vertrauen die Einstellung der Konsumenten gegenüber einer Premiumversion mit zusätzlichen Funktionen zum Schutz der Privatsphäre signifikant positiv beeinflussen. Das wahrgenommene Risiko der Privatheit hat dahingegen

[40] Ebd.

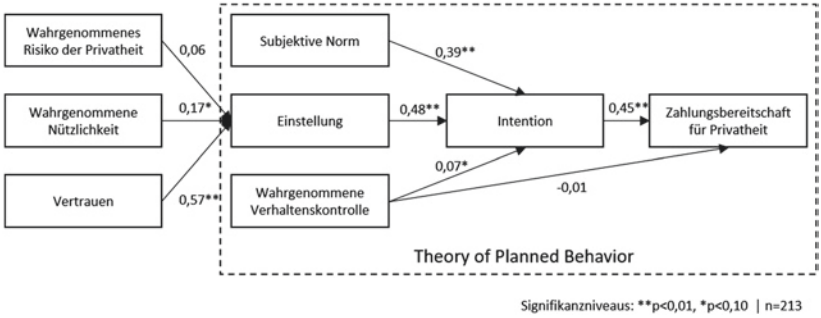

Abb. 3. Determinanten der Zahlungsbereitschaft (basierend auf Schreiner und Hess, 2015)

keinen signifikanten Einfluss auf die Einstellung. In Einklang mit der *Theory of Planned Behavior* zeigt unsere Studie außerdem, dass subjektive Normen, die Einstellung der Verbraucher und die wahrgenommene Verhaltenskontrolle die Nutzungsintention positiv beeinflussen, welche wiederum einen signifikant positiven Einfluss auf die Zahlungsbereitschaft für Privatheit hat. Für Betreiber sozialer Netzwerke bedeutet das, dass das Anbieten einer Premiumversion mit zusätzlichen Funktionen zur Kontrolle der Privatsphäre einen guten Ansatz zur Monetarisierung des Schutzes der Privatheit als Erlösmodel darstellt. Wichtig hierbei ist, dass die angebotene Premiumversion die Möglichkeiten der Konsumenten zum Schutz ihrer personenbezogenen Daten tatsächlich erhöht. Außerdem sollten die Anbieter sozialer Netzwerke sicherstellen, dass die Konsumenten der Premiumversion vertrauen können. Um das Vertrauen der Verbraucher zu stärken, könnten beispielsweise Informationskampagnen gestartet werden, um die Transparenz bezüglich der Unterschiede zwischen der kostenlosen und der Premiumversion zu erhöhen, oder unabhängige Dritte könnten den Schutz der Privatsphäre verifizieren.

Nachfolgende empirische Erkenntnisse

Auch neuere Studien haben sich der Zahlungsbereitschaft für Privatheit gewidmet und zeigen, dass das Entscheidungsverhalten der Individuen sehr komplex ist und die Zahlungsbereitschaft für Privatheit stark vom jeweiligen Kontext abhängt. Zwei kontextspezifische Faktoren scheinen in diesem Hinblick eine besonders zentrale Rolle zu spielen: Die generellen Privatheitsbedenken des Konsumenten

und der Grad der Sensibilität der Daten.[41] Umso sensitiver die Daten und umso höher die generellen Privatheitsbedenken des Einzelnen sind, umso höher ist der Preis, der für die Datenpreisgabe gefordert wird. Nguyen et al.[42] kommen in ihrer Studie zu ähnlichen Ergebnissen wie wir in Schreiner und Hess[43] und zeigen, dass Smartphonenutzer bereit sind, einen Preisaufschlag zu zahlen, um ihre Privatsphäre zu schützen. Außerdem zeigen sie, dass höhere generelle Privatheitsbedenken der Verbraucher zu einer gesteigerten Zahlungsbereitschaft für Privatheit führen. Des Weiteren spielt auch die Sensibilität der offenzulegenden Daten eine wichtige Rolle. Egelman et al.[44] haben eine Studie mit zwei Experimenten durchgeführt, um die Zahlungsbereitschaft der Verbraucher für Privatheit bei der Wahl neuer Apps zu untersuchen. Die Ergebnisse zeigen, dass Konsumenten bei der Wahl zwischen verschiedenen Apps mit ähnlichen Funktionalitäten bereit sind 1,50 US$ für die App zu bezahlen, die am wenigsten Zugriffserlaubnisse fordert. Die Autoren kommen zu dem Schluss, dass viele Smartphonenutzer um ihre Privatheit besorgt sind und daher bereit sind, einen Aufschlag für Apps zu bezahlen, die weniger sensible Daten anfordern. Auch Winegar und Sunstein[45] kommen zu ähnlichen Ergebnissen. In einer Studie mit 2.416 US-amerikanischen Teilnehmern untersuchen sie den Wert, den Individuen ihren personenbezogenen Daten bei der Nutzung digitaler Plattformen beimessen. Die Ergebnisse ihrer Studie zeigen, dass Verbraucher signifikant mehr Geld verlangen, um Daten preiszugeben, die gesundheitsbezogene Informationen beinhalten, im Vergleich zu demographischen Daten. Außerdem belegt die Studie den sogenannten *Superendowment Effect,* der besagt, dass Individuen ihren Daten einen viel größeren Wert beimessen, wenn es darum geht, einen monetären Wert für die Bereitstellung personenbezogener Daten festzulegen verglichen mit der Zahlungsbereitschaft, die Individuen haben, um ihre personenbezogenen Daten zu schützen. Pu und Grossklags[46] haben eine Conjoint Analyse durchgeführt, um den monetären Wert zu quantifizieren, den Individuen sowohl ihren eigenen Informationen als auch denen ihrer Freunde bei der Nutzung einer sozialen App beimessen. Die Ergebnisse zeigen, dass der wahrgenommene Wert

[41] Wagner et al. (2018).

[42] Nguyen et al. (2016).

[43] Schreiner und Hess (2015).

[44] Egelman et al. (2013).

[45] Winegar und Sunstein (2019).

[46] Pu und Grossklags (2016).

personenbezogener Daten der Freunde davon abhängt, ob die gesammelten Informationen für die Funktionalität der App von Bedeutung sind. Ist das der Fall werden die personenbezogenen Informationen der Freunde mit 1,01 US$ bewertet, während ihnen nur ein Wert von 0,68 US$ zugeschrieben wird, wenn sie keinen Mehrwert für die Nutzung der App bieten. Den eigenen Daten wird entsprechend ein Wert von 1,48 bzw. 1,52 US$ beigemessen.

4.2 Bereitschaft zur Offenlegung personenbezogener Daten

Neben dem Wert personenbezogener Daten spielt auch die generelle Bereitschaft der Individuen, personenbezogene Daten offenzulegen, eine zentrale Rolle. im Besonderen gilt dies bei Gesundheitsdaten. Wir haben diese Frage in Verbindung mit sogenannten Health Wearables untersucht und die Ergebnisse in Becker et al.[47] dargelegt. Nachfolgend stellen wir die Ergebnisse und das dahinterliegende Projekt vor.

Personenbezogene Gesundheitsdaten
Besonders im Gesundheitswesen ist die Offenlegung personenbezogener Daten ein zentrales Thema, da es sich bei Gesundheitsdaten um eine sehr sensible Ressource handelt, die es zu schützen gilt. Daher haben viele Individuen Privatheitsbedenken hinsichtlich der Erfassung und Nutzung ihrer Gesundheitsdaten. Vor allem haben sie Bedenken bezüglich möglicher unerwünschter wirtschaftlicher und sozialer Folgen, die der Missbrauch solcher Informationen mit sich bringen kann. Basierend auf dem Privatheitskalkül führen Individuen daher eine Kosten-Nutzen-Analyse durch, um zu entscheiden, welche personenbezogenen Gesundheitsinformationen sie offenlegen. Folglich stellt sich die Frage, auf welche Art und Weise Unternehmen die Bereitschaft ihrer Kunden, personenbezogene Gesundheitsdaten offenzulegen, erhöhen können.

Das Privatheitskalkül als Bezugsrahmen
Ein zentraler Aspekt der Privatheitsforschung in den Wirtschaftswissenschaften und darüber hinaus ist daher das sogenannte Privatheitskalkül, welches einen bewussten kognitiven Prozess zur Entscheidung der Offenlegung

[47] Becker et al. (2020).

personenbezogener Daten beschreibt. Es geht davon aus, dass Individuen sich bewusst entscheiden, welche Informationen sie preisgeben. Der Ansatz des Privatheitskalküls beschreibt, dass Individuen eine Kosten-Nutzen-Analyse durchführen und dabei die Nachteile der Datenpreisgabe gegenüber möglichen Vorteilen abwägen. Das heißt, Individuen wägen einen möglichen Verlust der Privatheit gegen einen potentiellen Nutzen, den die Informationspreisgabe mit sich bringt, ab. Überwiegt der wahrgenommene Nutzen, so entscheidet sich das Individuum, seine personenbezogenen Daten offenzulegen[48] – ggf. unter dem Einfluss von Verzerrungen wie sie aus der Psychologie bekannt sind.

Empirische Untersuchung der Offenlegung personenbezogener Gesundheitsdaten

Um dies genauer zu untersuchen, haben wir in Becker et al.[49] die bereits erwähnte Studie zur Erforschung der Bereitschaft, personenbezogene Gesundheitsdaten zur Nutzung sogenannter Health Wearables preiszugeben, durchgeführt. Health Wearables sind eine spezielle Form der Gesundheitsinformationstechnologie, bei der automatisch individuelle Gesundheitsdaten erfasst werden, um dem Verbraucher darauf basierend medizinischen Rat für seine Gesundheit und sein Wohlbefinden geben zu können. Auch wenn die Offenlegung personenbezogener Gesundheitsdaten sowohl dem Anbieter als auch den Konsumenten von Health Wearables wesentliche Vorteile wie beispielsweise eine verbesserte Personalisierung des Trainingsplans bieten kann, sind Konsumenten oft zögerlich ihre sensiblen Daten preiszugeben. Daher haben wir in Becker et al.[50] untersucht, welchen Einfluss das Framing der Produkteigenschaften und die Informationsqualität der Argumente zur Datenerfassung auf die Bereitschaft zur Offenlegung personenbezogener Gesundheitsdaten haben. Neben den Produkteigenschaften und der Datenschutzerklärung, wird die Bereitschaft personenbezogene Daten offenzulegen meist auch davon beeinflusst, auf welche Art und Weise diese Informationen präsentiert werden. Somit könnten spezielle Kommunikationsstrategien als Teil der Produktpräsentation einen erheblichen Einfluss auf die Einstellung der Verbraucher haben. In diesem Fall könnten die Anbieter von Health Wearables die wahrgenommenen Vorteile ihrer Produkte durch das richtige

[48] Chellappa und Sin (2005), Dinev und Hart (2006).

[49] Becker et al. (2020).

[50] Ebd.

Framing der Produkteigenschaften hervorheben. Außerdem könnte auch die Formulierung der Datenschutzerklärung das wahrgenommene Risiko, das mit der Datenerfassung verbunden ist, minimieren. Anbieter, die die Datenerfassung anhand logischer Argumentationen mit hohem Informationsgehalt rechtfertigen, könnten somit die Bereitschaft der Konsumenten personenbezogene Gesundheitsdaten preiszugeben erhöhen. Um diese Zusammenhänge genauer zu untersuchen, haben wir danach gefragt, welchen Einfluss das Framing der Produkteigenschaften und die Argumentationskraft der Datenschutzerklärung auf die Bereitschaft, personenbezogene Gesundheitsinformationen offenzulegen, haben.[51]

Empirische Einsichten

Zur Beantwortung dieser Frage wurde ein Online-Experiment mit 529 Teilnehmern durchgeführt. Im Rahmen des Experiments haben wir den Teilnehmern die Fitnessarmbanduhr Charge 2 des Anbieters Fitbit vorgestellt. Hierfür wurde die Webseite der originalen Fitbit Charge 2 hinsichtlich der Produkteigenschaften und der Datenschutzerklärung angepasst. Die Produkteigenschaften wurden verlustorientiert, neutral und gewinnorientiert formuliert, um zu untersuchen, ob positiv formulierte Produkteigenschaften die Konsumenten motivieren, personenbezogene Gesundheitsinformationen preiszugeben. Bei der Datenschutzerklärung wurde zwischen logischen, unlogischen und keinen Argumenten für die Datenerhebung unterschieden. Die Hypothese war, dass Konsumenten ihre Daten eher offenlegen, wenn ihnen überzeugendere Datenschutzerklärungen mit hoher Argumentationskraft präsentiert werden. Nach der Erkundung der Webseite sollten die Teilnehmer angeben, in welchem Ausmaß sie dem Anbieter Fitbit personenbezogene Gesundheitsdaten bereitstellen würden.

Die Ergebnisse sind in Abb. 4 dargestellt. Unsere Studie zeigt, dass Konsumenten, denen positiv formulierte Produkteigenschaften präsentiert werden, eher dazu bereit sind personenbezogene Gesundheitsdaten offenzulegen. Dies bedeutet, dass bei diesen Konsumenten die wahrgenommenen positiven Produkteigenschaften gegenüber den wahrgenommenen Risiken überwiegen. Daher sind sie eher dazu geneigt, das Risiko der Datenpreisgabe einzugehen. Des Weiteren zeigen die Ergebnisse der Studie, dass eine Datenschutzerklärung mit starker Argumentationskraft überzeugender auf die Verbraucher wirkt als unlogische oder gar keine Argumente. Interessanterweise zeigen die Ergebnisse aber auch, dass unlogische Argumente zu einer höheren Bereitschaft führen Daten offenzulegen als fehlende

[51] Ebd.

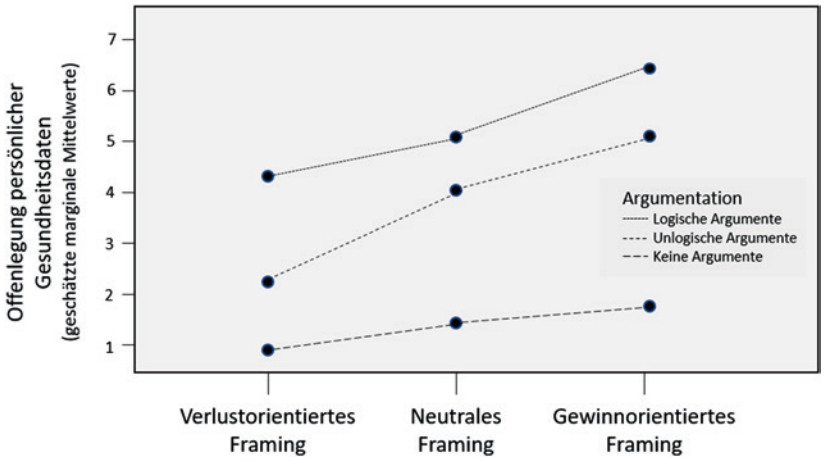

Abb. 4. Offenlegung und Framing (basierend auf Becker et al. 2020)

Argumente. Dieses Phänomen der placebischen Informationen wurde auch schon von früheren Studien nachgewiesen.[52] Mitunter kann der Einsatz unlogischer Argumente effektiver sein als das Fehlen jeglicher Begründung, da Verbraucher die Datenschutzerklärung oft nur gedankenlos überfliegen, anstatt sie aufmerksam zu lesen.

Zusammenfassend lässt sich sagen, dass eine Datenschutzerklärung mit hoher Argumentationskraft die wahrgenommen Risiken der Datenerfassung minimiert, während positiv formulierte Produkteigenschaften die wahrgenommenen Vorteile der Datenerfassung maximieren. Folglich wird die Bereitschaft der Verbraucher, personenbezogene Gesundheitsdaten zur Nutzung von Health Wearables offenzulegen, gesteigert. Die Erkenntnisse unserer Studie zeigen damit auch, dass Anbieter von Health Wearables davon profitieren können, die Argumentationskraft der Datenerfassung und das Framing der Produkteigenschaften anzupassen und somit die Offenlegungsbereitschaft ihrer Kunden zu erhöhen.

[52] z. B. Langer et al. (1978).

4.3 Die Rolle der Privatsphäre Dritter im Entscheidungskalkül eines Konsumenten

Viele Studien gehen implizit davon aus, dass Konsumenten lediglich personenbezogene Daten zu ihrer Person offenlegen (oder eben nicht). Gerade in sozialen Netzwerken sieht man, dass diese Annahme so allgemein nicht mehr stimmt. Somit kann das Offenlegungsverhalten von Verbrauchern nicht nur ihre eigene Privatsphäre (interne Privatsphäre), sondern auch die Privatsphäre von Dritten (externe Privatsphäre) gefährden. Um ihren Erfolg zu sichern, ist es daher für Anbieter sozialer Netzwerke ausschlaggebend zu verstehen, inwieweit Konsumenten die Privatsphäre Dritter in ihrem Entscheidungskalkül zur Offenlegung personenbezogener Daten berücksichtigen.

Kontext

Um dies genauer zu erforschen haben wir in Morlok[53] untersucht, wie die Intention Informationen über andere in sozialen Netzwerken zu teilen durch externe Privatheitsbedenken beeinflusst wird. Außerdem haben wir untersucht, inwiefern Erfahrungen mit Privatsphäreingriffen die externen Privatheitsbedenken und die Intention, Informationen über Dritte zu teilen, beeinflussen.

Ein wichtiger Unterschied sozialer Netzwerke zu anderen Kontexten, in denen personenbezogene Daten preisgegeben werden, ist, dass die Informationen nicht nur gegenüber einer Organisation, sondern auch gegenüber anderen Verbrauchern offengelegt werden. Daher haben Konsumenten nicht nur informationelle Privatheitsbedenken gegenüber der Organisation, wie beispielsweise Facebook, sondern auch soziale Privatheitsbedenken gegenüber anderen Verbrauchern. Folglich kann zwischen *externen informationellen Privatheitsbedenken,* das heißt Bedenken, dass das Verhalten von Organisationen die externe Privatsphäre negativ beeinflusst, und *externen sozialen Privatheitsbedenken,* das heißt Bedenken in Bezug auf die Handhabung der offengelegten Daten durch andere Verbraucher, unterschieden werden. Die *externen sozialen Privatheitsbedenken* setzen sich wiederum aus drei Dimensionen zusammen: Exposition, Eindringen und Identifizierung. Exposition bezieht sich auf die Enthüllung physischer und emotionaler Eigenschaften eines Individuums, wie beispielsweise Kummer oder Nacktheit. Eindringen bezieht sich auf das wahrgenommene Eingreifen in die Privatsphäre

[53] Morlok (2016).

und das personenbezogene Leben eines Individuums wie beispielsweise dessen Komfortzone. Und Identifizierung beschreibt das Bedenken, dass identifizierbare Informationen ermöglichen, dass ein Individuum identifiziert oder lokalisiert werden kann.

Theoretische Grundlagen

Als theoretische Grundlage zur Untersuchung dieses Phänomens eignet sich die *Communication Privacy Management Theory,* da sie ein konzeptionelles Verständnis für den Umgang mit der Privatsphäre anderer Individuen bereitstellt.[54] Die Theorie bezieht sich auf sogenannte metaphorische Grenzen, die aufzeigen, wie Individuen mit ihrer eigenen und der Privatsphäre Dritter umgehen. Hierbei müssen Individuen sowohl personenbezogene als auch kollektive Grenzen gleichzeitig managen. Personenbezogene Grenzen beschreiben die eigene Privatsphäre, während sich kollektive Grenzen auf die Privatsphäre anderer Personen beziehen. Petronio argumentiert, dass Individuen sich auch für die Privatsphäre anderer verantwortlich fühlen.[55]

Basierend auf der *Communication Privacy Management Theory* wurde ein Forschungsmodell entwickelt, das sowohl den Einfluss *externer informationeller Privatheitsbedenken* als auch *externer sozialer Privatheitsbedenken* auf die Bereitschaft, personenbezogene Daten offenzulegen, untersucht. Die *externen sozialen Privatheitsbedenken* setzen sich in dem Modell aus Expositionsbedenken, Eindringungsbedenken und Identifikationsbedenken zusammen. Außerdem vermuten wir, dass Konsumenten, sobald sie einmal eine Verletzung ihrer internen Privatsphäre erlebt haben, eher zögern, Informationen anderer preiszugeben. Folglich stellen wir die Hypothese auf, dass ein vorheriges Eindringen in die personenbezogene Privatsphäre den Einfluss von externen sozialen und informationellen Privatheitsbedenken auf die Offenlegungsbereitschaft moderiert. Des Weiteren stellen wir die Hypothese auf, dass der wahrgenommene Besitz der Informationen von Dritten einen positiven Einfluss auf die Bereitschaft hat, diese Daten offenzulegen. Das Phänomen des wahrgenommenen Besitzes beschreibt, dass Konsumenten die Daten Dritter als ihr Eigentum wahrnehmen, wenn sie Kontrolle über diese haben.

[54] Petronio (2002).

[55] Ebd.

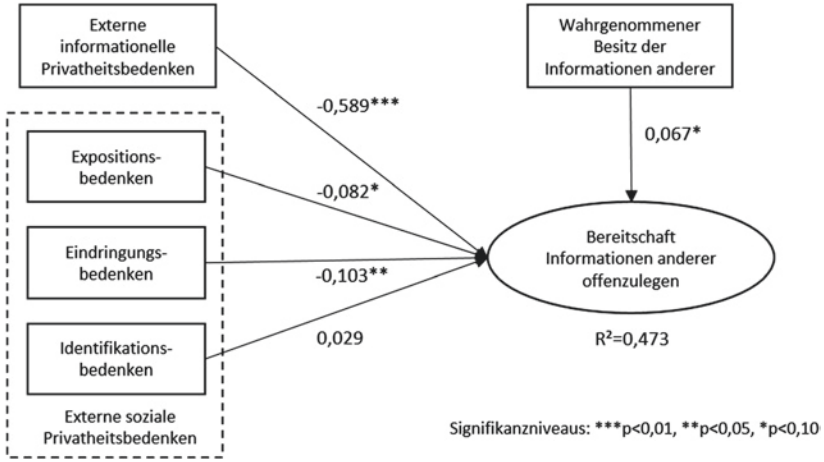

Abb. 5. Determinanten der Bereitschaft zur Offenlegung von Daten Dritter (basierend auf Morlok, 2016)

Empirische Einsichten

Um das Forschungsmodell zu überprüfen, haben wir in Morlok[56] eine Online-Umfrage mit 265 Teilnehmern durchgeführt und anhand eines Strukturgleichungsmodells ausgewertet (Abb. 5).

Die Ergebnisse zeigen, dass sich die Absicht von Konsumenten personenbezogene Daten in sozialen Netzwerken offenzulegen sowohl durch die externen sozialen und informationellen Privatheitsbedenken als auch den wahrgenommenen Besitz der Informationen von Dritten erklären lässt. Der wahrgenommene Besitz der Informationen von Dritten verstärkt die Offenlegungsbereitschaft der Konsumenten. Haben Verbraucher allerdings externe informationelle Privatheitsbedenken, hat dies einen negativen Einfluss auf ihre Bereitschaft personenbezogene Daten offenzulegen. Auch Expositionsbedenken und Eindringungsbedenken verringern die Offenlegungsbereitschaft der Konsumenten, während die dritte Dimension der externen sozialen Privatheitsbedenken, die Identifikationsbedenken, keinen signifikanten Einfluss auf die Offenlegungsabsicht hat. Allerdings zeigt die Studie auch, dass diese Zusammenhänge stark

[56] Morlok (2016).

davon abhängen, ob ein Verbraucher in der Vergangenheit Opfer eines Eingriffs in seine persönliche Privatsphäre geworden ist. Verbraucher, die bereits eine Verletzung ihrer Privatsphäre erfahren haben, machen ihr Offenlegungsverhalten von den Eindringungsbedenken abhängig, nicht aber von Identifikationsbedenken. Konsumenten, die diese Erfahrung noch nicht gemacht haben, sind sich zusätzlich auch der Expositionsbedenken bewusst. Diese Ergebnisse verdeutlichen die bisher kaum untersuchte, aber sehr komplexe Beziehung zwischen externen sozialen Privatheitsbedenken und der Offenlegungsabsicht in sozialen Netzwerken. Wenn Verbraucher einmal einen Eingriff in ihre interne Privatsphäre erlebt haben, werden sie sich auch mehr Sorgen über den Eingriff in die externe Privatsphäre machen, da es für diese Verbraucher einfacher ist, sich in die Lage anderer zu versetzen. Somit hängt das Bewusstsein über die Bedrohungen der externen Privatsphäre von den Erfahrungen der Konsumenten mit eigenen Privatsphäreverletzungen ab.

Die Offenlegung personenbezogener Daten spielt eine wichtige Rolle für Anbieter sozialer Netzwerke, da sie soziale Interaktion, Personalisierung und Ausspielung passender Werbung ermöglicht. Mit dieser Studie zeigen wir in Morlok[57], dass die externen Privatheitsbedenken der Verbraucher eine wichtige Rolle im Zusammenhang mit der Offenlegung personenbezogener Daten in sozialen Netzwerken spielen. Für die Betreiber sozialer Netzwerke bedeutet das, dass nicht nur Kontrollmechanismen zur Gewährleistung der internen, sondern auch der externen Privatsphäre implementiert werden sollten. Außerdem sollten sowohl informationelle als auch soziale Aspekte beim Datenschutz beachtet werden. Die Berücksichtigung dieser beiden Aspekte kann den Betreibern sozialer Netzwerke helfen, die Loyalität ihrer Verbraucher zu stärken und sich so von der Konkurrenz zu differenzieren.

5 Zusammenfassung und Ausblick

Die wirtschaftswissenschaftliche Forschung zur Privatheit um das Zusammenspiel von Unternehmen und Verbrauchern hat sich bisher stark auf die Personalisierung von Angeboten und die verbesserten Möglichkeiten der Differenzierung von Preisen fokussiert. Dies sind wichtige und interessante Perspektiven. Zur vollständigen Erfassung des Phänomens der informationellen

[57] Ebd.

Privatheit, insbesondere vor dem Hintergrund der technischen Entwicklungen bei der Erfassung und der Verarbeitung von Daten, greift dies aber zu kurz. Daher haben wir eine Reihe von Projekten durchgeführt, die bewusst einige wichtige weitere Perspektiven eingenommen haben. Das vorliegende Kapitel gibt einen Überblick über die zentralen Ergebnisse dieser Projekte.

Ein erster Teil der Projekte lässt sich in der unternehmenszentrierten Perspektive verankern. Zwei Szenarien der Verwendung von personenbezogenen Daten durch Unternehmen sind der Datenhandel auf sogenannten Datenmärkten und die unternehmensinterne Verwendung von Daten zwecks Auswertung. In einer ersten Studie wird aus struktureller Perspektive die Wertschöpfung auf Märkten für personenbezogene Daten am Beispiel des Marktes für Online-Werbung untersucht. Die Studie zeigt auf, welche Akteure auf Datenmärkten miteinander agieren und wie personenbezogene Daten zur Wertschöpfung genutzt werden. Die unternehmensinterne Nutzung von Daten zur Schaffung von Synergien wird in einer zweiten Studie thematisiert. Das im Rahmen dieser Studie erarbeitete konzeptionelle Framework zeigt auf, welche unternehmensinternen Voraussetzungen auf Management- und Datenebene gegeben sein müssen, damit Synergieeffekte aus Daten realisiert werden können.

Ein zweiter Teil unserer Projekte bezieht sich auf die verbraucherorientierte Perspektive. Von zentraler Bedeutung sind hier die Offenlegung von Daten sowie die Zahlungsbereitschaft für den Verzicht auf die Weitergabe von Daten. Eine erste Studie hat die Zahlungsbereitschaft von Konsumenten für personenbezogene Daten in sozialen Netzwerken untersucht. Dabei zeigte sich, dass die Zahlungsbereitschaft für eine privatsphäreschützende Premiumversion eines sozialen Netzwerkes signifikant durch den wahrgenommenen Nutzen und das Vertrauen in die Plattform beeinflusst wird. Neben dem Wert, den Verbraucher ihren personenbezogenen Daten beimessen, ist ebenfalls deren Bereitschaft, besagte Daten preiszugeben, relevant. In einer zweiten Studie wurde anhand des Beispiels von Health Wearables dargestellt, dass Konsumenten durch eine aussagekräftige Datenschutzerklärung und positiv formulierte Produkteigenschaften zur Offenlegung ihrer personenbezogenen Gesundheitsdaten bestärkt werden können. Dass Konsumenten nicht nur ihre eigenen personenbezogenen Daten, sondern auch die Daten Dritter in Händen halten, wird von einer dritten Studie herausgearbeitet. In diesem Kontext wird betont, dass Plattformbetreiber nicht nur auf interne Privatheitsbedenken von Konsumenten, sondern auch auf deren externe Privatheitsbedenken eingehen sollten.

Dieses Thema ist keinesfalls erschöpfend behandelt. Schon jetzt bestehen weitere wichtige Lücken. Exemplarisch sei der Umgang mit Privatheit am Arbeitsplatz genannt, hierzu gibt es bisher nur sehr wenige Studien. Darüber

hinaus wird es, aufgrund von technischen Entwicklungen, zu weiteren Lücken kommen. Die zunehmende Verbreitung von mobilen Endgeräten führt zu einer wachsenden Vernetzung der Konsumenten – und das nicht nur untereinander. Man denke daher nur an technologische Trends wie das Internet der Dinge, das physische Objektive mit dem Internet und somit mit dem Konsumenten verbindet. Die zunehmende Entwicklung solcher digitalen Technologien treibt die wachsende Generierung personenbezogener Daten der Verbraucher voran. Dies stellt sowohl die Praxis als auch die Forschung vor immer neue Herausforderungen und fordert neue Gestaltungsansätze. Das Kapitel von Conrad u. a. in diesem Band geht auf jene Gestaltungsansätze ein und beschreibt, wie erhöhte Transparenz über den eigenen digitalen Fußabdruck die informationelle Selbstbestimmung von Konsumenten schützen kann.

Literatur

Ackoff, R. L. (1971). Towards a system of systems concepts. *Management Science, 17(11)*, 661–671.

Acquisti, A., & Fong, C. (2020). An experiment in hiring discrimination via online social networks. *Management Science, 66(3)*, 1005–1024.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54(2)*, 442–492.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50(2)*, 179–211.

Awad, N. F., & 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.

Becker, M., Matt, C., & Hess, T. (2020). It's not just about the product: How persuasive communication affects the disclosure of personal health information. *ACM SIGMIS Database: The Database for Advances in Information Systems, 51(1)*, 37–50.

Bründl, S., Matt, C., & Hess, T. (2015). *Wertschöpfung in Datenmärkten – Eine explorative Untersuchung am Beispiel des deutschen Marktes für persönliche Daten*. Ludwig-Maximilans-Universität, Institut für Wirtschaftsinformatik und Neue Medien (WIM).

Bründl, S., Matt, C., & Hess, T. (2016). Daten als Geschäft – Rollen und Wertschöpfungsstrukturen im deutschen Markt für persönliche Daten. *Wirtschaftsinformatik & Management, 8(6)*, 66–71.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management, 6(2)*, 181–202.

Connolly, R., & McParland, C. (2012). Dataveillance: Employee monitoring & information privacy concerns in the workplace. *Journal of Information Technology Research, 5(2)*, 31–45.

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

Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice architecture and smartphone privacy: There's a price for that. In: R. Böhme (Hrsg.), *The economics of information security and privacy*. Springer, 211-236.

Hann, I.-H., Hui, K.-L., Lee, S.-Y., & Png, I. P. L. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24(2)*, 13–42.

Hartmann, P. M., Zaki, M., Feldmann, N., & Neely, A. (2016). Capturing value from big data – A taxonomy of data-driven business models used by start-up firms. *International Journal of Operations & Production Management, 36(10)*, 1382–1406.

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization-privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems, 34(2)*, 369–400.

Kelleher, J. D., Namee, M., & Brian und D'arcy, Aoife,. (2015). *Fundamentals of machine learning for predictive data analytics: Algorithms, worked examples, and case studies*. MIT Press.

Langer, E. J, Blank, A., & Chanowitz, B. (1978). The mindlessness of ostensibly thoughtful action: The role of "placebic" information in interpersonal interaction. *Journal of Personality and Social Psychology, 36(6)*, 635-642.

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues, 59(2)*, 243–261.

Martin, N., Matt, C., Niebel, C., & Blind, K. (2019). How data protection regulation affects startup innovation. *Information Systems Frontiers, 21(6)*, 1307–1324.

Morlok, T. (2016). Sharing is (not) caring-the role of external privacy in users' information disclosure behaviors on social network sites. In *Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS), 2016, Chiayi, Taiwan.*

Morlok, T., Matt, C., & Hess, T. (2017). *Privatheitsforschung in den Wirtschaftswissenschaften: Entwicklung, Stand und Perspektiven*. Ludwig-Maximilians-Universität, Institut für Wirtschaftsinformatik und Neue Medien (WIM).

Morlok, T., Matt, C., & Hess, T. (2018). Perspektiven der Privatheitsforschung in den Wirtschaftswissenschaften.In: M. Friedewald (Hrsg.): *Privatheit und selbstbestimmtes Leben in der digitalen Welt*. Springer, 179-220.

Nevo, S., & Wade, M. R. (2010). The formation and value of IT-enabled resources: Antecedents and consequences of synergistic relationships. *MIS Quarterly, 34(1)*, 163–183.

Nguyen, K. D., Rosoff, H., & John, R. S. (2016). The effects of attacker identity and individual user characteristics on the value of information privacy. *Computers in Human Behavior, 55*, 372–383.

Ochs, C., Friedewald, M., Hess, T., & Lamla, J. (2019). *Die Zukunft der Datenökonomie: Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz*. Springer Fachmedien.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.

Pu, Y., & Grossklags, J. (2016). Towards a model on the factors influencing social app users' valuation of interdependent privacy. *Proceedings on Privacy Enhancing Technologies, 2,* 61-81.

Schoeman, F. D. (1984). Privacy: Philosophical dimensions of the literature. In: F.D. Schoeman (Hrsg.), *Philosophical dimensions of privacy: An anthology*. Cambridge University Press.

Schöning, C., Matt, C., & Hess, T. (2019). Personalised nudging for more data disclosure? On the adaption of data usage policies format to cognitive styles. In *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS), 2019, Hawaii, USA*.

Schreiner, M., & Hess, T. (2013). Published. On the willingness to pay for privacy as a freemium model: First empirical Evidence. In *Proceedings of the 21st European Conference on Information Systems (ECIS), 2013, Utrecht, Niederlande.*

Schreiner, M., & Hess, T. (2015). Why are consumers willing to pay for privacy? An application of the privacy-freemium model to media companies. C*ompleted Research Paper of the 23rd European Conference on Information Systems (ECIS), 2015, Münster, Deutschland.*

Shollo, A., & Galliers, R. D. (2016). Towards an understanding of the role of business intelligence systems in organisational knowing. *Information Systems Journal, 26(4)*, 339–367.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35(4)*, 989–1015.

Someh, I. A., & Shanks, G. (2013). The role of synergy in achieving value from business analytics systems. In *Proceedings of the 34th International Conference on Information Systems (ICIS), 2013, Mailand, Italien.*

Wagner, A., Wessels, N., Buxmann, P., & Krasnova, H. (2018). Putting a Price Tag on Personal Information – A Literature Review. In *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS), 2018, Hawaii, USA*.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4(3)*, 193–220.

Weibl, J., & Hess, T. (2020). Turning data into value – Exploring the role of synergy in leveraging value among data. *Information Systems Management, 37(3)*, 227–239.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum Press.

Winegar, A. G., & Sunstein, C. R. (2019). How much is data privacy worth? A preliminary investigation. *Journal of Consumer Policy, 42(3)*, 425–440.

Wixom, B. H., & Ross, J. W. (2017). How to monetize your data. *MIT Sloan Management Review, 58(3)*, 9–13.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51(1)*, 42–52.

Prof. Dr. Thomas Hess ist Direktor des Instituts für Digitales Management und Neue Medien der Fakultät für Betriebswirtschaft der Ludwig-Maximilians-Universität München.

Prof. Dr. Christian Matt ist Professor und Mitdirektor des Instituts für Wirtschaftsinformatik der Universität Bern.

Verena Thürmel ist wissenschaftliche Mitarbeiterin des Instituts für Digitales Management und Neue Medien der Ludwig-Maximilians-Universität München.

Mena Teebken ist wissenschaftliche Mitarbeiterin des Instituts für Digitales Management und Neue Medien der Ludwig-Maximilians-Universität München.