Eine ökonomische Analyse des Wertes von Privatsphäre und personenbezogener Daten aus Unternehmens- und Nutzerperspektive

TECHNISCHE UNIVERSITÄT DARMSTADT

Vom Fachbereich Rechts- und Wirtschaftswissenschaften
der Technischen Universität Darmstadt

genehmigte

Dissertation

von

Nora Hanna Cordula Weßels, M.Sc.
geboren in Frankfurt am Main

zur Erlangung des akademischen Grades
Doctor rerum politicarum (Dr. rer. pol.)

Erstgutachter:	Prof. Dr. Peter Buxmann
Zweitgutachter:	Prof. Dr. Alexander Benlian
Hochschulkennziffer:	D17
Darmstadt	2019

Weßels, Nora Hanna Cordula: Eine ökonomische Analyse des Wertes von Privatsphäre und personenbezogener Daten aus Unternehmens- und Nutzerperspektive

Darmstadt, Technische Universität Darmstadt

Jahr der Veröffentlichung der Dissertation auf TUprints: 2019

Tag der mündlichen Prüfung: 04.07.2019

Veröffentlicht unter CC BY-SA 4.0 International

https://creativecommons.org/licenses/

Ehrenwörtliche Erklärung

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig angefertigt habe. Sämtliche aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde bisher weder einer anderen Prüfungsbehörde vorgelegt noch veröffentlicht.

Nora Hanna Cordula Weßels

Darmstadt, den 14. März 2019

Hinweis zur genderneutralen Sprache

Zur besseren Lesbarkeit wird in dieser Arbeit die männliche Form bei personenbezogenen Substantiven und Pronomen verwendet. Diese Regelung stellt jedoch keine Benachteiligung des weiblichen Geschlechtes dar, sondern soll lediglich der Vereinfachung dienen.

Zusammenfassung

Für Unternehmen stellen die personenbezogenen Daten ihrer Nutzer und die daraus gewonnenen Informationen eine wertvolle Ressource dar. Schließlich sammeln Unternehmen die Daten ihrer Nutzer, verarbeiten diese für ihre Geschäftszwecke und verkaufen sie oft an Dritte weiter. Darüber hinaus wird der Handel mit Nutzerinformationen auch durch sogenannte Datenmarktplätze weiter vorangetrieben. Dabei werden solche Datenpraktiken, die mit der Erhebung, Verarbeitung und Kommerzialisierung großer Mengen an personenbezogenen Daten einhergehen, von Nutzern oft kritisch gesehen und führen verstärkt zu Bedenken über den Schutz ihrer Privatsphäre. Natürlich profitieren auch die Nutzer von Diensten und Produkten, die auf Daten basieren, allerdings scheinen die Vor- und Nachteile zwischen Anwender- und Anbieterseite aus Nutzerperspektive ungleich verteilt zu sein. Darüber hinaus entwickeln Nutzer ein immer größer werdendes Bewusstsein über den Wert ihrer Daten, zumindest auf abstrakter Ebene und einige fordern sogar eine klare Kompensation für ihre Datenpreisgabe. Vor diesem Hintergrund ist die Erforschung von Datenpraktiken und Geschäftsmodellen, die sowohl für die Anwender als auch für die Anbieter von Internetdiensten annehmbar sind, überaus wichtig. Schließlich sollten Datenpraktiken so gestaltet werden, dass sie die Privatsphäre der Nutzer adäquat schützen, sie sollten aber auch den Unternehmen ermöglichen, ihre Geschäftsziele zu erreichen und wettbewerbsfähig sowie profitabel zu bleiben.

Die vorliegende Arbeit gliedert sich in die Literatur zur Erforschung solcher Privatsphäre-freundlicher Datenpraktiken ein, indem eine zweiseitige Analyse des Wertes von Privatsphäre und personenbezogener Daten in der digitalen Ökonomie aus der Unternehmens- und Nutzerperspektive vorgenommen wird. In dieser Arbeit wird daher zunächst aus Unternehmensperspektive untersucht, wie Organisationen mit dem Zielkonflikt zwischen ihrem Bedarf an Nutzerinformationen, der gegebenenfalls Privatsphäre-einschneidend sein kann, und ihrem Bedarf zur Gewinnung und Bindung von Kunden, die einen angemessenen Privatsphäre-Schutz fordern, einhergehen. Anschließend analysiert diese Arbeit aus Nutzerperspektive, welchen monetären Wert Individuen ihren personenbezogenen Informationen und damit ihrer Privatsphäre beimessen. Dazu wird zunächst der bisherige

Stand der Forschung mit Hilfe einer strukturierten Literaturrecherche zusammengefasst und die Ergebnisse der Studien miteinander verglichen. Weiterhin wird eine Studie zur Untersuchung des Wertes von Daten aus Nutzerperspektive mit Hilfe einer neuen, vielversprechenden Messmethode, der *Name-Your-Own-Price* (NYOP) Auktion mit Option des wiederholten Bietens, durchgeführt. Schließlich untersucht die letzte Studie dieser Dissertation die Wertermittlung von Daten in einem natürlichen, bislang unerforschten Kontext: den Datenverkaufsplattformen. Auf diesen Plattformen können Nutzer kontrolliert Informationen, die sie zu teilen bereit sind, an ausgewählte Unternehmen verkaufen. Die zweistufige Studie untersucht dabei welche Faktoren Individuen in ihrer Bereitschaft, Daten auf solchen Plattformen zu verkaufen, beeinflussen und welche Wichtigkeiten einer Auswahl dieser Faktoren zugeschrieben werden. Somit wird in diesem Zuge auch die Nutzerakzeptanz von Datenverkaufsplattformen untersucht, die einen alternativen Datenpraktik-Ansatz darstellen können.

Die Analysen dieser Arbeit zeigten dabei, dass Unternehmen durchaus Spannungen zwischen dem Umgang mit Nutzerdaten und der Privatsphäre der Individuen wahrnehmen, die durch interne und externe Belastungen noch verstärkt werden. Organisationen versuchen die gegensätzlichen Anforderungen auszugleichen, indem sie verschiedene Taktiken anwenden, um mit den negativen Auswirkungen ihrer Entscheidungen über die Erhebung und Verwendung von Nutzerdaten umzugehen. Die Untersuchungen aus Perspektive der Nutzer zeigten weiterhin, dass die Wertermittlung von Daten stark kontextabhängig ist. So haben die Methode, die zur Messung der Wertvorstellung der Individuen herangezogen wird, aber auch der Datentyp sowie weitere Untersuchungsfaktoren Einfluss auf den monetären Wert von Privatsphäre, wie die strukturierte Literaturrecherche zeigte. Mit der NYOP-Auktion konnte dabei eine Methode eingeführt werden, die es Individuen erleichtert, ihre individuelle Wertvorstellung von Daten auszudrücken und auch der Kontext von Datenverkaufsplattformen stellte sich als geeignete Forschungsumgebung heraus. Zudem zeigte sich, dass der Ansatz der Datenverkaufsplattformen aus Nutzerperspektive unter bestimmten, designtechnischen Ausgestaltungen adoptiert werden würde.

Abstract (Englische Übersetzung der Zusammenfassung)

For companies, the personal data of their users and the information gained from it represent a valuable resource. Companies collect the data of their users, process it for their business purposes, and often resell it to third parties. Additionally, the trade with user information is also driven by so-called data markets. Such data practices, which are associated with the collection, processing, and commercialization of large amounts of personal data, are often criticized by users and raise concerns about the protection of their privacy. Of course, users also benefit from data-driven services and products, but the advantages and disadvantages seem to be imbalanced between users and providers from a users' perspective. Moreover, users are becoming increasingly aware of the value of their data, at least at the abstract level, and some even expect clear compensation for their data disclosure. Against this background, research of data practices and business models that are acceptable to both users and providers of Internet services is essential. Data practices should be designed to adequately protect the privacy of users, but should also enable companies to reach their business objectives and remain competitive and profitable.

This dissertation integrates into the literature on research of such privacy-friendly data practices by providing a two-sided analysis of the value of privacy and personal data in the digital economy from an organizational and user perspective. To achieve this, this dissertation first examines from an organizational perspective how companies perceive and handle the trade-off between their need for customer information, which may lead to privacy-intrusiveness, and their need to attract and retain customers that require adequate privacy protection. Furthermore, this dissertation analyses from a user perspective what monetary value individuals assign to their personal information and, thus, to their privacy. For this purpose, first, the current state of research is summarized using a structured literature review and the results of the studies are compared with each other. Furthermore, a study is presented that investigates the value of data from the users' perspective using a new and promising measurement method, the *Name-Your-Own-Price* (NYOP) auction with the option of repeated bidding. Finally, the last study of this dissertation examines the valuation of data in the

natural and previously unexplored context of data-selling platforms. On these platforms, users can sell information they are willing to share to selected companies in a controlled manner. The two-step study examines which factors influence individuals' willingness-to-sell data on such platforms and what importance they assign to a selection of these factors. Thus, the user acceptance of data-selling platforms, representing an alternative data practice approach, is also investigated.

The analyses in this dissertation showed that companies actually perceive tensions between the handling of user data and the privacy of individuals, which are intensified by internal and external pressures. Organizations try to balance the conflicting requirements by using different tactics to deal with the negative impact of their decisions on the collection and use of user data. In addition, from a user perspective, the research showed that the valuation of data is very context-specific. Thus, the method used to measure individuals' valuation, the type of data, and other factors have an impact on the monetary value of privacy, as the literature review revealed. The NYOP auction is a method that makes it easier for individuals to express their individual assessment of data, and the context of data-selling platforms also proved to be an appropriate research environment. In addition, it has been found that the approach of data-selling platforms would be adopted from the user's perspective under certain design conditions.

Inhaltsverzeichnis

Abbildungsverzeichnis ..... **XI**

Tabellenverzeichnis ..... **XII**

Abkürzungsverzeichnis ..... **XIII**

1 Einleitung **1**

1.1 Motivation und Relevanz der Arbeit 1

1.2 Zielsetzung und Struktur der Arbeit 3

2 Theoretische Grundlagen der Privatsphäre-Forschung **9**

2.1 Definition des Privatsphäre-Begriffes 9

2.2 Themenfelder und Grundlagen der informationellen Privatsphäre-Forschung 11

2.3 Grundlagen der Ökonomie von Privatsphäre 14

3 Eine Untersuchung der konkurrierenden Anforderungen von Unternehmen im Umgang mit Nutzerdaten und Privatsphäre **18**

3.1 Motivation und Relevanz 18

3.2 Grundlagen der organisationalen Privatsphäre-Forschung und des Informationsbedarfs aus Unternehmensperspektive 21

3.2.1 Informationsbedarf von Unternehmen 21

3.2.2 Privatsphäre-Forschung aus Unternehmensperspektive 22

3.3 Methodik 25

3.3.1 Datenerhebung 27

3.3.2 Datenanalyse, Kodierung und Memo-Schreiben 29

3.4 Ergebnisse 31

3.4.1 Spannungen der Anbieter bei der Erhebung und Nutzung von Nutzerdaten 32

3.4.2 Ambidextrie als Meta-Theorie 36

3.4.3 Aufrechterhaltung des Gleichgewichts in dynamischen Kontexten 38

3.5 Diskussion der Ergebnisse 47

3.5.1 Integration in bestehende Forschung und theoretischer Beitrag 47

3.5.2 Praktikscher Beitrag 50

3.5.3 Limitationen und weiterer Forschungsbedarf 52

4 Eine strukturierte Literaturrecherche zum Wert von Daten aus Nutzerperspektive **55**

4.1 Motivation und Relevanz 55

4.2 Methodik der strukturierten Literaturrecherche 58

4.3 Wert von Daten und seine Einflussfaktoren 61

4.3.1 Einflussfaktoren ... 63
4.3.2 Messmethoden ... 67
4.3.3 Studienergebnisse zum Wert von Daten ... 71
4.4 Diskussion der Ergebnisse ... 74
5 Eine Feldstudie zur Ermittlung des Wertes personenbezogener Daten durch eine *Name-Your-Own-Price* Auktion ... 78
5.1 Motivation und Relevanz ... 78
5.2 Forschung zum Wert von Daten ... 81
5.3 Qualitative Vorstudie ... 81
5.4 Feldstudie ... 82
5.4.1 Methode der Feldstudie ... 83
5.4.2 Ergebnisse der Feldstudie ... 88
5.5 Diskussion der Ergebnisse ... 93
5.5.1 Implikationen für die Forschung und Praxis ... 93
5.5.2 Limitationen und weiterer Forschungsbedarf ... 95
6 Eine Untersuchung von Einflussfaktoren auf die Bereitschaft personenbezogene Informationen auf Datenverkaufsplattformen zu verkaufen ... 97
6.1 Motivation und Relevanz ... 97
6.2 Grundlagen zur Wert-von-Daten-Forschung und zu Datenverkaufsplattformen ... 101
6.2.1 Forschung zum Wert von Daten ... 101
6.2.2 Datenverkaufsplattformen ... 102
6.3 Zweistufiges Studiendesign ... 105
6.4 Erster Untersuchungsschritt: Qualitative Studie ... 106
6.4.1 Methodik ... 106
6.4.2 Ergebnisse ... 108
6.5 Zweiter Untersuchungsschritt: Auswahlbasierte Conjoint-Analyse ... 113
6.5.1 Methodik ... 113
6.5.2 Ergebnisse ... 117
6.6 Diskussion der Ergebnisse ... 124
6.6.1 Implikationen für Forschung und Praxis ... 125
6.6.2 Limitationen und weiterer Forschungsbedarf ... 127
7 Zusammenfassung und Ausblick ... 129
7.1 Wissenschaftlicher Beitrag der Arbeit ... 130
7.2 Beitrag der Arbeit für die Unternehmenspraxis ... 133
7.3 Zukünftiges Forschungspotenzial ... 134
Literaturverzeichnis ... 136
Anhang ... 159

Abbildungsverzeichnis

Abbildung 1: Übersicht über die Kapitelstruktur der vorliegenden Arbeit 8
Abbildung 2: Prozessbeschreibung der Aufrechterhaltung des Gleichgewichts in dynamischen Kontexten 39
Abbildung 3: Zusammenfassung des Suchprozesses und der Anzahl der Studien am Ende jeder Phase 61
Abbildung 4: Integratives, theoretisches Framework zur Erhebung des Wertes von Daten 62
Abbildung 5: Übersicht über die in der Literatur identifizierten Einflussfaktoren auf den Wert von Daten 64
Abbildung 6: Überblick über die Messmethoden der Zahlungs- und Verkaufsbereitschaft für Daten 68
Abbildung 7: NYOP-Mechanismus der Feldstudie, angepasst von Spann et al. (2004) 86
Abbildung 8: Streudiagramm aller Gebotsreihen 90
Abbildung 9: Streudiagramm der adaptierten Gebotsreihen und deren Cluster 91
Abbildung 10: Überblick des zweistufigen Studiendesigns 105

Tabellenverzeichnis

Tabelle 1: Überblick der Privatsphäre-Literatur aus Unternehmensperspektive 23
Tabelle 2: Überblick über die Einhaltung der Anforderungen an *Grounded Theory* Studien basierend auf Birks et al. (2013) 30
Tabelle 3: Durch konkurrierende Anforderungen entstehende Spannungen 32
Tabelle 4: Statistiken der Start-, Zweit- und Finalen Gebote 89
Tabelle 5: Statistiken der Wilcoxon-Vorzeichen-Rang Tests 89
Tabelle 6: Statistiken der hierarchischen Clusteranalyse (*Ward*-Methode) in Euro 92
Tabelle 7: Überblick über aktuell bekannte Datenverkaufsplattformen 103
Tabelle 8: Einflussfaktoren für die Bereitschaft der Benutzer, personenbezogene Daten auf Datenverkaufsplattformen zu verkaufen 109
Tabelle 9: Überblick über die Attribute und ihre Level 116
Tabelle 10: Attribute, Level, Teilnutzenwerte und durchschnittliche Wichtigkeiten 120
Tabelle 11: Nutzenänderung und monetärer Wert der Änderungen 121
Tabelle 12: Durchschnittliche Wichtigkeiten der vier Gruppen 123
Tabelle 13: Teilnutzenwerte der vier Gruppen (mit nullzentrierten Differenzen) 124

Abkürzungsverzeichnis

B2B	*Business-to-Business*
BDM	Becker-DeGroot-Marshak-Mechanismus
CA	*Conjoint Analysis*
CBCA	*Choice-based Conjoint-Analysis*
CVM	*Contingent Valuation Method*
DCM	*Discrete Choice Method*
DSGVO	Datenschutz-Grundverordnung
Engl.	Englisch
EU	Europäische Union
ID	*Identification*
KI	Künstliche Intelligenz
NYOP	*Name-Your-Own-Price*
PETs	*Privacy Enhancing Technologies*
TIOLI	*Take-it-or-Leave-it*
US	*United States*
VA	Vickrey Auktion
Vgl.	Vergleiche
WTA	*Willingness-to-Accept*
WTP	*Willingness-to-Pay*
WTS	*Willingness-to-Sell*

1 Einleitung

Im Jahr 2009 leitete Meglena Kuneva, die damalige Kommissarin für Verbraucherschutz, ihre Rede vor der Europäischen Kommission mit folgenden Worten ein: *„We are here to talk about one of the most important and most controversial issues in the fast evolving world of digital communications: the explosion in the volume of collected personal data and its use for commercial purposes"* (Kuneva 2009). Wenige Sätze später zog Frau Dr. Kuneva den mittlerweile berühmt gewordenen Vergleich von Daten mit dem „Öl des Internets" und „der neuen Währung der digitalen Welt", der die Wichtigkeit von personenbezogenen Daten in dieser digitalen Zeit noch stärker hervorhebt (Kuneva 2009). Zehn Jahre später ist die Kommerzialisierung immer größer werdender Mengen von Daten und deren Sammlung, Nutzung und Analyse nicht weniger aktuell (EuropeanCommission 2019). Schließlich stehen durch den technologischen Fortschritt der letzten Jahrzehnte enorme Rechenleistungs- und Speicherkapazitäten zur Verfügung, welche die Speicherung und Auswertung von Daten in bislang ungeahnten Ausmaß ermöglichen und durch immer besser werdende Methoden des *Data-Minings* sowie *Business Intelligence & Analytics* ergänzt werden (Chen et al. 2012; Tene und Polonetsky 2012). Weiterhin ist das Internet, durch den immer stärkeren Einsatz von Rechnern, Sensoren und mobilen Endgeräten zunehmend allgegenwärtig, wodurch die Möglichkeiten, Daten zu erzeugen, zu teilen, zu verknüpfen und darauf zuzugreifen, drastisch zunahmen (Tene und Polonetsky 2012). Daten, vor allem personenbezogene Daten, haben in der Wirtschaft und Gesellschaft einen hohen Stellenwert eingenommen.

1.1 Motivation und Relevanz der Arbeit

Für Unternehmen stellen die personenbezogenen Daten ihrer Nutzer und die daraus gewonnenen Informationen einen Vermögenswert dar (Ackoff 1989; Schwartz 2004). Schließlich können sie mit den Daten beispielsweise ihre Entscheidungenprozesse verbessern (McAfee et al. 2012), Wettbewerbsvorteile realisieren (Shapiro et al. 1998) und ihre Performanz steigern (Brynjolfsson et al. 2011). Daher ist es nicht verwunderlich, dass nicht nur viele der neu auf den Markt eintretenden Geschäftsmodelle auf Daten basieren (Engelbrecht et al. 2016), sondern mittlerweile auch immer mehr traditionelle Unternehmen

Daten verstärkt in ihre Geschäftsmodelle einbinden (Buxmann 2018). Unternehmen sammeln die Daten ihrer Nutzer, verarbeiten diese für ihre Geschäftszwecke und verkaufen sie teilweise an Dritte weiter (Li et al. 2014). Daten nehmen so die Rolle eines handelbaren Gutes ein (Davies 1998; Schwartz 2004). Im Zuge dieser Kommerzialisierung von Daten sind Datenmarktplätze entstanden, auf denen personenbezogene Daten von Individuen in enormen Umfängen zwischen anfragenden Unternehmen und Datenbrokern wie beispielsweise Oracle's BlueKai, Acxiom oder TowerData gehandelt werden (Acxiom 2019; Oracle 2018; Spiekermann et al. 2015a; TowerData 2019). Das Ausmaß der dabei gesammelten und gehandelten Daten verdeutlicht die folgende Aussage, mit der Oracle den Datenmarktplatz BlueKai bewirbt: *"Oracle Data Cloud gives marketers access to 5 billion global IDs, $3 trillion in consumer transactions, and more than 1,500 data partners available through the BlueKai Marketplace. With more than 45,000 prebuilt audiences spanning demographic, behavioral, B2B, online, offline, and transactional data, we bring together more data into a single location than any other solution."(Oracle 2018)*

Solche Datenpraktiken, die mit der Erhebung derart beträchtlicher Mengen personenbezogener Daten und ihrer Verarbeitung einhergehen, führen jedoch zu wachsenden Bedenken der Datenpreisgebenden über den Schutz ihrer Privatsphäre[1], der zunehmend schwieriger zu werden scheint, wenn Daten stetig vervielfältigt und an immer mehr Parteien weitergegeben werden (Acquisti et al. 2016; Tene und Polonetsky 2012). Denn auch wenn die fortgeschrittene Verwendung von Daten, sei es durch die Adoption von Internetdiensten, die in immer besser werdender Qualität zur Verfügung stehen (Acquisti et al. 2016) oder Verbesserungen durch *Big Data*-Ansätze in Bereichen wie der Medizin (Nambiar et al. 2013), der Elektrizität (Diamantoulakis et al. 2015) oder des Verkehrsmanagements (Lv et al. 2015), auch Individuen klar profitieren lassen, scheinen die Vor- und Nachteile zwischen der Anbieter- und Anwenderseite ungleich verteilt zu sein (Li et al. 2014).

Die Privatsphäre-Bedenken der Internetnutzer werden durch die Datenskandale der letzten Jahre, wie dem NSA-Überwachungsskandal und der Enthüllung des PRISM-Programms (BBC 2014) sowie dem Bekanntwerden der Wahlprofilerstellung mit 87 Millionen Facebook-Nutzerdaten durch Cambridge Analytica (NewYorkTimes 2018), zunehmend verschärft. Dazu kommt, dass die Datenpraktiken der Unternehmen zunehmend von den Nutzern als unfair wahrgenommen werden, wenn personenbezogene Informationen ohne Zustimmung für

[1] Der Begriff „Privatsphäre" wird in dieser Arbeit als Synonym für den ebenfalls in der Literatur verwendeten Begriff „Privatheit" genutzt, die beide an den englischen Begriff „*privacy*" angelehnt sind (Geminn und Roßnagel 2015). Der Schutz von Privatsphäre wird im Folgenden auch als „Datenschutz" bezeichnet.

andere Zwecke genutzt oder weitergegeben werden (Culnan und Armstrong 1999; Culnan und Bies 2003; Li et al. 2011). Immer mehr Internetnutzer scheinen sich darüber bewusst zu werden, dass ihre personenbezogenen Daten eine wertvolle Ressource für Unternehmen sein können (Accenture 2015; Li et al. 2014) und verlangen daher eine Kompensation für die Preisgabe (Spiekermann und Korunovska 2017). So hat beispielsweise eine Studie gezeigt, dass 67% der Befragten finden, dass Unternehmen am meisten davon profitieren, wenn sie ihre Daten preisgeben, während nur 6% sich selbst im Vorteil sehen (Orange 2014). Vor diesem Hintergrund sind die gängigen Datenpraktiken der Unternehmen kritisch zu hinterfragen und zu überdenken, um die Potenziale der zunehmend größer werdenden Datenmengen für Wirtschaft und Gesellschaft mit den potenziellen Risiken in Einklang zu bringen (Hirsch 2014).

1.2 Zielsetzung und Struktur der Arbeit

Eines der übergeordneten Ziele der Privatsphäre-Forschung sollte es daher sein, Datenpraktiken und Geschäftsmodelle zu untersuchen, die sowohl für Anwender als auch Anbieter von Internetdiensten annehmbar sind. Schließlich bedarf es Ansätzen, die es Unternehmen erlauben die Daten ihrer Nutzer zu verwenden, um wettbewerbsfähig und profitabel zu bleiben (Shapiro et al. 1998). Auf der anderen Seite sollten die verwendeten Datenpraktiken nutzerfreundlich sein, in dem sie die Privatsphäre der Individuen respektieren, diesen mehr Kontrolle ermöglichen und eine stärkere Kompensation für die Datenpreisgabe anstreben, um das Ungleichgewicht in der Verteilung der Vor- und Nachteile von Datenpraktiken für die involvierten Parteien zu reduzieren (Li et al. 2014).

Grundlegend für die Erreichung dieses übergeordneten Ziels ist ein besseres Verständnis über die Bedeutung, die beide Parteien der Privatsphäre von Individuen in der digitalen Ökonomie zuweisen. In dieser Arbeit wird daher zunächst aus Unternehmensperspektive der Zielkonflikt der Anbieter von Internetdiensten zwischen der Notwendigkeit der Datensammlung und –verwendung sowie der Notwendigkeit, die Privatsphäre ihrer Nutzer zu schützen, analysiert. Anschließend erfolgt eine detaillierte Untersuchung des Wertes von personenbezogenen Daten und daher der Privatsphäre aus Nutzerperspektive. Schließlich wird in diesem Zuge ein alternativer Datenpraktik-Ansatz in Form von Datenverkaufsplattformen vorgestellt und die Nutzerakzeptanz dieses untersucht.

Die Untersuchung des Zielkonfliktes von Unternehmen zwischen Datensammlung und Datenschutz ist wichtig, denn auch wenn personenbezogene Daten für Unternehmen einen

Vermögenswert darstellen (Gregory 2011), ist der Umgang damit aus Unternehmenssicht nicht trivial. Vielmehr können Datenpraktiken auch für Unternehmen eine Herausforderung darstellen und zu einer Belastung werden (Spiekermann et al. 2015a), beispielsweise wenn die Praktiken zu Privatsphäre-intrusiv wirken und es zu Vorfällen kommt, die Imageverluste nach sich ziehen (Acquisti et al. 2016; Feri et al. 2016). Schließlich sind Nutzerdaten, wie bereits dargelegt, überaus wichtig für Unternehmen. Um jedoch an Daten zu kommen und diese zu verwerten, müssen die Unternehmen in die Privatsphäre ihrer Nutzer eingreifen. Diese Eingriffe erschweren es Unternehmen jedoch, neue Nutzer zu gewinnen und bestehende zu binden. Unternehmen sind im Umgang mit Nutzerdaten also einem Spannungsfeld ausgesetzt, welches von der bisherigen Privatsphäre-Forschung bislang nicht genauer untersucht wurde. Generell wurde der Unternehmensperspektive bisher wenig Aufmerksamkeit in der Privatsphäre-Literatur gewidmet (Bélanger und Crossler 2011; Smith et al. 2011). Daher ergibt sich die folgende Forschungsfrage:

Forschungsfrage 1: *Wie nehmen Unternehmen das Spannungsverhältnis zwischen ihrem Bedarf an Nutzerdaten und der Notwendigkeit des Privatsphäre-Schutzes ihrer Nutzer wahr und wie gehen sie mit diesem Spannungsverhältnis um?*

Um dies zu untersuchen wurde eine *Grounded Theory*-Studie durchgeführt, die auf Daten von 23 Online-Dienstleistern basiert. Die Studie konnte zeigen, dass die Privatsphäre der Nutzer für Unternehmen durchaus einen hohen Stellenwert einnimmt, dabei allerdings mit einem deutlichen Spannungsverhältnis einhergeht. Schließlich ist die Erhebung und Verwendung von Nutzerdaten für Unternehmen ebenfalls sehr wichtig und es stellt für Unternehmen eine große Herausforderung dar, ein Gleichgewicht zwischen dem Privatsphäre-Schutz und der Wertschöpfung basierend auf Nutzerdaten zu erreichen. Dies bedeutet, dass Handlungsempfehlungen für Unternehmen, die in der Privatsphäre-Forschung aus reiner Nutzerperspektive entwickelt wurden, und die hauptsächlich in Empfehlungen zur Reduktion der Datenerhebung resultieren (z.B. Hui et al. 2007; Smith et al. 1996), für Unternehmen oft impraktikabel sind. Schließlich sind Unternehmen, wie bereits erläutert, auf Daten angewiesen, um ihre Geschäftsziele zu erreichen und die Reduktion von Daten könnte, in gewissen Grad, auch für Internetnutzer mit Nachteilen verbunden sein. Schon im Jahr 1977 brachte Richard Posner die Diskussion auf, dass ein vollkommener Privatsphäre-Schutz und der damit einhergehende Verschluss von (relevanten) Daten vor anderen Marktteilnehmern zu ineffektiven Marktsituationen führen kann, die auf Kosten aller Teilnehmer gehen (Posner 1977). Denn ein vollkommener Privatsphäre-Schutz kann auch für die Nutzer mit

individuellen (Varian 2002), sozialen (Friedman und Resnick 2001) und wirtschaftlichen Opportunitätskosten einhergehen, wenn diese ihre Daten nicht preisgeben (Acquisti et al. 2016). Daher bedarf es vielmehr Ansätzen, die Nutzer zwar mehr Kontrolle über ihre Privatsphäre geben können, es Unternehmen aber auch weiterhin ermöglichen, ihre Dienste rentabel anzubieten.

Vor diesem Hintergrund bedarf es eines besseren Verständnisses dafür, wie viel Individuen ihre personenbezogenen Daten und damit auch ihre Privatsphäre wert sind. Denn nicht nur seit Angela Merkels Appell, dass „*die Bepreisung von Daten […] das zentrale Gerechtigkeitsproblem dieses Jahrzehnts [ist]*“ (FAZ 2018), ist die Relevanz des Themas bekannt. Schließlich kann Individuen ein besseres Verständnis über den Wert ihrer Privatsphäre helfen, internetbasierte Dienste und Datenpraktiken generell informierter hinsichtlich ihrer potenziellen Vor- und Nachteile zu bewerten (Carrascal et al. 2013) und so fundierte (Adoptions-)Entscheidungen zu treffen (Berthold und Böhme 2010). Und auch für Unternehmen sind Erkenntnisse darüber, wie Individuen ihre personenbezogenen Daten wertschätzen und welche Faktoren diese beeinflussen wesentlich, da diese mit möglichen Designimplikationen für Datenpraktiken einhergehen können, die von der Nutzerseite her stärker akzeptiert werden. Daher wurde dieser Thematik auch zunehmende wissenschaftliche Aufmerksamkeit geschenkt, was sich in einer anschaulichen Zahl von Studien auf diesem Gebiet widerspiegelt. Um den Wert personenbezogener Daten quantifizieren zu können, wurde in vielen Studien untersucht, wie viel Individuen bereit sind für den Schutz ihrer personenbezogenen Daten zu zahlen und wie viel sie für den Verkauf ihrer Daten verlangen würden. Um die Erkenntnisse dieser Literatur zusammenzufassen, sollten die bisherigen Studien zunächst identifiziert und miteinander verglichen werden, wodurch sich die zweite Forschungsfrage ergibt:

Forschungsfrage 2: *Was ist der Stand der Forschung zur Untersuchung des Wertes personenbezogener Daten aus Nutzerperspektive?*

Zur Beantwortung dieser Forschungsfrage wurde zunächst eine strukturierte Literaturrecherche durchgeführt, wobei 37 empirische Studien als relevant identifiziert und näher untersucht wurden. Dabei konnte gezeigt werden, dass die bisherigen Forschungsstudien in sehr heterogenen Wertvorstellungen der Individuen resultieren, die von sehr hohen Bewertungen (z.B. Huberman et al. 2005) bis zu sehr niedrigen (z.B. Bauer et al. 2012) reichen. Die ermittelten Werte schienen dabei von einer Vielzahl von Faktoren abhängig zu sein, wie der Methode, mit der der Wert gemessen wurde, dem Datentyp, der

verkauft oder geschützt werden soll, sowie weiteren Untersuchungsfaktoren. Diese Faktoren des jeweiligen Studienkontexts variieren stark zwischen den betrachteten Studien. Um eine bessere Vergleichbarkeit der Studien zu erreichen, nimmt die Literaturrecherche anhand dieser Kontexte eine Konzeptualisierung mit Hilfe eines integrativen, theoretischen Frameworks vor.

Insgesamt zeigt sich also, dass die Ermittlung des Wertes personenbezogener Daten aus Nutzerperspektive nicht trivial ist. Schließlich haben Individuen oft wenig bis keine Erfahrung mit der Monetarisierung von Daten, da sie in der Regel keinen Einblick in den bestehenden Datenhandel haben (Acquisti et al. 2016). Dies resultiert darin, dass es für Internetnutzer eine Herausforderung darstellen kann, direkt und unvermittelt ihre Wertvorstellung für Daten zu äußern, zumal sie in den bisherigen Untersuchungen auch keinerlei Rückmeldung oder Feedback zu den Werten erhalten haben. Vor diesem Hintergrund, wurde in der vorliegenden Arbeit außerdem eine neue und vielversprechende Methode, die *Name-Your-Own-Price* (NYOP) Auktion mit wiederholter Biet-Option, zur Messung des Wertes, den Individuen ihren Daten zuweisen, angewandt. Diese Messmethode ermöglicht es Individuen, Feedback bezüglich ihrer Wertvorstellungen zu erhalten, indem ihnen Rückmeldung gegeben wird, falls der genannte Werte zu hoch ist. Die Teilnehmer können auf Basis des Feedbacks ihren zunächst geäußerten Wert noch einmal überdenken und anpassen. Daher ergibt sich die folgende, dritte Forschungsfrage:

Forschungsfrage 3: *Welchen monetären Wert weisen Individuen ihren personenbezogenen Daten in einer Name-Your-Own-Price Auktion mit Option des wiederholten Bietens zu?*

Zur Untersuchung der Forschungsfrage wurde eine experimentelle Studie unter 171 Probanden durchgeführt, bei der die Teilnehmer die NYOP-Methode zur Bewertung eines personenbezogenen Datums anwenden konnten. Dabei hat sich gezeigt, dass die NYOP-Methode gut zu der vagen Wertvorstellung der Individuen passt und den Prozess der individuellen Wertermittlung erleichtern kann, da sie die Rückmeldung zu vorherigen Geboten als Informationsquelle nutzen können (Liu et al. 2016), ohne dass sie dabei zu sehr geankert werden. Wie bereits beschrieben, hat jedoch die zuvor erwähnte Literaturrecherche ergeben, dass nicht nur die Messmethode, sondern der gesamte Kontext der Studie den Wert bestimmt, den Individuen ihren Daten zuweisen. Ein Kontext, der dabei bislang noch nicht untersucht wurde, aber eine sehr natürliche und vielversprechende Forschungsumgebung darstellt und daher zur Erforschung des Wertes personenbezogener Daten herangezogen werden sollte, besteht in den sogenannten Datenverkaufsplattformen. Schon im Jahr 1996 hat

Laudon die Schaffung von Informationsmärkten vorgeschlagen, auf denen Individuen selbstständig die Rechte an ihren personenbezogenen Daten gegen einen Ausgleich an Unternehmen oder Intermediäre übertragen können, um die Nutzer stärker am Erfolg der florierenden Datenmärkte teilhaben lassen zu können (Laudon 1997; Laudon 1996). Nach diesem Vorbild sind in den letzten Jahren vermehrt Konzepte von solchen Marktplätzen (z.B. Datacoup, Datawallet, Wibson) entstanden, also Plattformen auf denen Nutzer selbst aktiv ihre Daten an ausgewählte Unternehmen oder den Plattformanbieter verkaufen können (Brustein 2012; Haberer und Schnurr 2018). Die Datenverkaufsplattformen befinden sich jedoch noch in sehr frühen Stadien. Sie können dabei allerdings als alternative Ansätze für die gängigen Datenpraktiken wie beispielsweise die bereits angesprochenen Datenmarktplätze wie BlueKai verstanden werden, was den Forschungsbedarf zu diesem Thema weiter verstärkt. Dabei sind sowohl aus theoretischer als auch aus praktischer Perspektive besonders diejenigen Faktoren interessant, die die Bereitschaft von Individuen, eigene personenbezogene Informationen auf solchen Datenverkaufsplattformen zu verkaufen, beeinflussen. Diese repräsentieren die Indikatoren, die zu einem Anstieg oder einer Senkung der Verkaufsbereitschaft führen können. Daher ergibt sich die folgende Forschungsfrage:

Forschungsfrage 4: *Welche Faktoren beeinflussen Individuen in ihrer Bereitschaft, personenbezogene Informationen auf Datenverkaufsplattformen zu verkaufen und wie werden diese Faktoren gewichtet?*

Zur Beantwortung dieser Forschungsfrage wurde in einem zweistufigen Prozess zunächst eine qualitative Studie unter 49 Internetnutzern zur Identifizierung der Einflussfaktoren durchgeführt, bevor mit einer Conjoint-Analyse unter 250 Studienteilnehmern die Wichtigkeiten einer Auswahl dieser Faktoren weiter untersucht wurden. Es konnte dabei gezeigt werden, wie vielschichtig diese Einflussfaktoren sind und dass diese sehr unterschiedlich in ihrer Gewichtung wahrgenommen werden. Dadurch konnten auch Implikationen für die Ausgestaltung solcher Datenverkaufsplattformen abgeleitet werden, die wiederum als Grundlage für Studien zur weiteren Untersuchung des Potenzials von Datenverkaufsplattformen als Alternative zu gängigen Datenpraktiken dienen können.

Die Struktur der Arbeit folgt den beschriebenen Forschungsfragen. Nach dieser Einleitung werden im 2. Kapitel zunächst die theoretischen Grundlagen der Privatsphäre-Forschung vorgestellt, wobei besonders auf die Ökonomie von Privatsphäre eingegangen wird, den Forschungsstrang, in den sich diese Arbeit inhaltlich eingliedert. Im darauffolgenden 3. Kapitel wird die erste Forschungsfrage untersucht und aus Unternehmensperspektive

analysiert, wie Anbieter von Onlinediensten das beschriebene Spannungsfeld wahrnehmen und wie diese damit umgehen. Die daran anschließenden Kapitel 4 bis 6 widmen sich der Nutzerperspektive und untersuchen den Wert, den Individuen ihren personenbezogenen Daten und ihrer Privatsphäre zuweisen. Dafür wird zunächst im 4. Kapitel die strukturierte Literaturrecherche zu bisherigen Studien in diesem Themenkomplex vorgestellt und so die zweite Forschungsfrage beantwortet, bevor im 5. Kapitel die experimentelle Studie präsentiert wird, die der Beantwortung der dritten Forschungsfrage dient und die Messung des Wertes von Daten mit der neuen Methode der *Name-Your-Own-Price* Auktion, vorstellt. Schließlich erfolgt im 6. Kapitel die Untersuchung der Einflussfaktoren auf die Bereitschaft, personenbezogene Informationen auf Datenverkaufsplattformen zu verkaufen, einem bislang für diesen Zweck unerforschten aber sehr vielversprechenden Kontext. Damit wird die vierte und letzte Forschungsfrage beantwortet und dadurch auch die Nutzerakzeptanz eines potenziellen, alternativen Datenpraktik-Ansatzes untersucht. Die Arbeit schließt mit einer Zusammenfassung der Beiträge und einem Ausblick auf zukünftiges Forschungspotenzial. Die folgende Abbildung 1 fasst die Struktur der vorliegenden Arbeit graphisch zusammen.

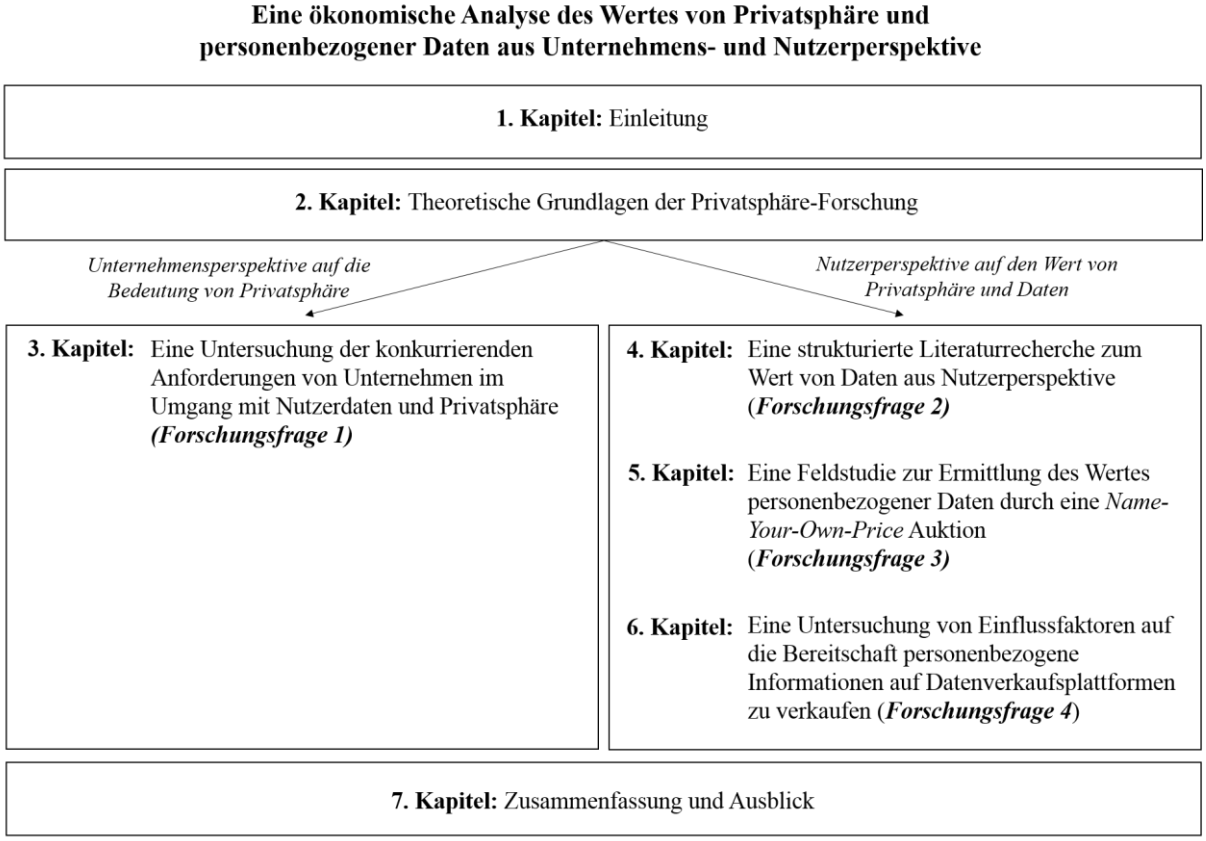


Abbildung 1: Übersicht über die Kapitelstruktur der vorliegenden Arbeit

2 Theoretische Grundlagen der Privatsphäre-Forschung

Um die in dem einleitenden Kapitel bereits vorgestellten Forschungsfragen dieser Arbeit untersuchen zu können und den Kontext in die übergeordnete Privatsphäre-Forschung einordnen zu können, wird in diesem Kapitel ein Überblick über die Grundlagen der bisherigen Privatsphäre-Forschung vorgestellt. Dazu wird zunächst auf die Definition von Privatsphäre eingegangen sowie ein kurzer Überblick über die verschiedenen Themenfelder der Privatsphäre-Forschung gegeben. Nachfolgend wird genauer auf das Teilgebiet der Ökonomie von Privatsphäre (engl. *Economics of Privacy*) eingegangen, in welches sich die vorliegende Arbeit inhaltlich eingliedert.

2.1 Definition des Privatsphäre-Begriffes

"The concept of "privacy" is elusive and ill defined. Much ink has been spilled in trying to clarify its meaning."

Richard Posner (1977, S. 393)

Auch wenn die zitierte Ausführung von Richard Posner etwas provokativ formuliert ist, bringt sie doch die Schwierigkeit der Schaffung eines einheitlichen und umfassenden Verständnis des Begriffes Privatsphäre zum Ausdruck (Thomson 1975). In einem Versuch der Klassifizierung, haben Smith et al. (2011) eine Einteilung der allgemeinen Privatsphäre-Definitionen (engl. *general privacy*) in wertbasierte und kognitionsbasierte Definitionen vorgenommen. Die wertbasierte Perspektive definiert allgemeine Privatsphäre dabei zunächst als ein Menschenrecht, das in das gesellschaftliche Wertesystem integriert ist (Smith et al. 2011). In diesem Rahmen wurde Privatsphäre beispielsweise als „*right to be left alone*" (Warren und Brandeis 1890, S. 193) oder auch als "*an aspect of human dignity*" (Bloustein 1964, S. 962) beschrieben. Eine leicht abgeschwächte wertbasierte Perspektive definiert Privatsphäre weiterhin als ein wirtschaftliches Gut, das mit Vor- und Nachteilen für die Gesellschaft einhergehen kann, die miteinander abgewogen werden müssen (Cohen 2001). So beschreibt Laudon (1996) beispielsweise: *"I believe it is possible to strengthen individual control over personal information and to strengthen (not replace) the existing legal foundations of privacy by permitting markets to work. In the end there should be as much*

privacy as people are willing to pay for, and as much use of private personal information for commercial purposes as is socially efficient." (Laudon 1996, S. 2)

Die kognitionsbasierten Ansätze definieren Privatsphäre hingegen eher als eine Auswirkung auf den Verstand, die Wahrnehmungen und die Kognition des Individuums jedoch weniger als einen absoluten Wert, weswegen Privatsphäre hierbei entweder als Zustand oder als Kontrolle gesehen wird (Smith et al. 2011). Der Zustandsbegriff wurde dabei erstmals von Alan Westin verwendet, der Privatsphäre als "*the voluntary and temporary withdrawal of a person from the general society"* (Westin 1967, S. 5) versteht. Weiterhin wurde Privatsphäre auch als „*a state or condition of limited access to a person*" (Schoeman 1984, S. 3) sowie als Konzept, das an konkrete Situationen des täglichen Lebens gebunden ist und die sich in den drei Dimensionen „*self-ego, environmental, and interpersonal"* (Laufer und Wolfe 1977, S. 22) widerspiegeln, beschrieben. Schließlich wurde allgemeine Privatsphäre noch als (per se) Kontrolle über Informationen sowie in abgeschwächter Form als die Fähigkeit der Kontrollausübung dargestellt (Smith et al. 2011). So beschreibt Westin beispielsweise: *"Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."* (Westin 1967, S. 5) während Altman Privatsphäre hingegen als "*the selective control of access to the self or to one's group*" (Altman 1975, S. 18) definiert.

Die Definitionen stammen dabei aus unterschiedlichsten Disziplinen, die unter anderem von Wirtschaft über Soziologie und Philosophie bis hin zu Recht und Psychologie reichen und in diesen auch weitreichend untersucht wurden (Smith et al. 2011). Gängigen Konzeptualisierungen folgend, fokussiert sich der Wirtschaftsinformatik-Kontext dabei meistens auf einen Teilbereich der allgemeinen Privatsphäre: die informationelle Privatsphäre (engl. *information privacy*) (Bélanger und Crossler 2011; Smith et al. 2011). In Abgrenzung zur physischen Privatsphäre (engl. *physical privacy*), die sich mit dem gegenständlichen Zugang zu einer Person oder ihrem privaten Bereich befasst, betrifft die informationelle Privatsphäre den Zugang zu identifizierbaren, personenbezogenen Daten (Smith et al. 2011). Eine weitere Konzeptualisierung von Clarke (1999a) nimmt eine Unterscheidung zwischen der Privatsphäre einer Person, des persönlichen Verhaltens, der Kommunikation sowie der personenbezogenen Daten vor, die er als die vier Dimensionen von Privatsphäre bezeichnet. Die Kommunikations- und Daten-Privatsphäre kann dabei wiederum als informationelle Privatsphäre zusammengefasst werden (Bélanger und Crossler 2011). Schließlich wird, bedingt durch den bereits beschriebenen technologischen Fortschritt, sämtliche

Kommunikation in Form von Daten und Informationen gespeichert, übertragen und integriert (Bélanger und Crossler 2011; Malhotra et al. 2004). Vor diesem Hintergrund fokussiert sich auch diese Arbeit im Folgenden auf informationelle Privatsphäre, die im weiteren Verlauf dieser Arbeit zur Vereinfachung als Privatsphäre abgekürzt wird. Analog zu der allgemeinen Privatsphäre sind auch die Definitionen dieses Teilbereiches der informationellen Privatsphäre vielfältig. Eine oft referenzierte Definition (z.B. Al-Fedaghi 2005; Bélanger und Crossler 2011; Skinner et al. 2006) stammt dabei von Clarke, der informationelle Privatsphäre als "*the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves"* (Clarke 1999b) zusammenfasst. In ähnlicher Weise, jedoch noch spezifischer, definieren Culnan und Bies Privatsphäre als "*the ability of individuals to control the terms under which their personal information is acquired and used*" (Culnan und Bies 2003, S. 326). Auch diese Definitionen sollten allerdings nicht als abschließend verstanden werden, da eine allumfassende, eindeutige Auslegung durch die vielen verschiedenen Facetten von Privatsphäre schwierig ist und Privatsphäre für verschiedene Individuen etwas anderes bedeuten kann (Acquisti et al. 2016). Daher legt auch diese Arbeit keine einzelne Definition von Privatsphäre zu Grunde, sondern akzeptiert ihre vielschichtige Natur, wobei, durch den Fokus auf Forschung zur Ökonomie von Privatsphäre, das Verständnis der informationellen Privatsphäre besonders durch die Elemente der wertbasierten Perspektive, die Privatsphäre als ein wirtschaftliches Gut sehen, ergänzt wird.

2.2 Themenfelder und Grundlagen der informationellen Privatsphäre-Forschung

Die Entwicklung hin zu dem gegenwärtigen „Informationszeitalter", in dem Produktivität und Wettbewerb und damit auch Unternehmenserfolge so stark von Wissen, Informationen und Technologien abhängen (Castells 2010), hat Privatsphäre zu einem der Kernthemen der Wirtschaftsinformatikforschung werden lassen (Pavlou 2011). Dabei befasst sich dieser Forschungsstrang mit verschiedenen Themenfeldern, die im Folgenden kurz vorgestellt werden.

Nach Smith et al. (2011) hat die bisherige Forschung sich neben der Definition und Konzeptualisierung von Privatsphäre, die bereits in Kapitel 2.1 zusammengefasst wurde, hauptsächlich mit den Themenfeldern der stark kontextuellen Natur von Privatsphäre sowie mit der Beziehung zwischen Privatsphäre und verwandten Konstrukten auseinandergesetzt. Einige dieser Beziehungen drücken sich auch in den wichtigsten Konzepten der Privatsphäre-Forschung, wie dem Privatsphäre-Paradoxon (engl. *privacy paradox*) und dem Privatsphäre-Kalkül (engl. *privacy calculus*) aus. Das Privatsphäre-Paradoxon beschreibt die Differenz

zwischen der Absicht eines Individuums zur Preisgabe personenbezogener Daten und dem tatsächlichen Verhalten (Norberg et al. 2007). Dies äußert sich beispielsweise darin, dass Internetnutzer zwar Bedenken darüber äußern, dass ihre Rechte und die Kontrollmöglichkeiten über ihre personenbezogenen Daten verletzt werden, und doch scheinen sie ihre Daten oft bereitwillig preiszugeben (Norberg et al. 2007). Die Erklärungsansätze für dieses irrationale Verhalten sind mannigfaltig (Kokolakis 2017) und reichen beispielsweise von psychologischen und kognitiven Verzerrungen wie der direkten Belohnung (engl. *immediate gratification*) (Acquisti 2004), übersteigertem Selbstvertrauen (engl. *overconfidence*) (Acquisti und Grossklags 2007) oder optimistischen Verzerrungen (engl. *optimistic bias*) (Cho et al. 2010) bis zu unvollständigen und asymmetrischen Informationsständen (Acquisti und Grossklags 2005), um nur einige mögliche Gründe zu nennen. Die Forschung basiert dabei auf der Annahme, dass Internetnutzer gemäß dem Privatsphäre-Kalkül eine Abwägung zwischen wirtschaftlichen und sozialen Vorteilen einer Datenpreisgabe einerseits sowie Kosten in Form von Risiken und anderen Konsequenzen andererseits vornehmen und ihre Daten nur preisgeben, wenn die Vorteile überwiegen (Acquisti et al. 2009; Culnan und Armstrong 1999; Dinev und Hart 2006; Pavlou 2011). Vorteile können dabei beispielsweise finanzielle Entlohnungen, Personalisierung sowie gesellschaftliche Anpassungen sein (Smith et al. 2011). Diese stehen gemäß des Kalküls den Privatsphäre-Bedenken der Nutzer gegenüber, welche die Forschung als das zentrale Konstrukt zur Messung für Privatsphäre identifiziert hat (Smith et al. 2011) und die sich in verschiedensten Dimensionen ausdrücken können (Bélanger und Crossler 2011). So können beispielsweise Bedenken bezüglich der Verwendung von im Internet preisgegebenen Daten (Dinev und Hart 2006), Unternehmenspraktiken (Smith et al. 1996), oder allgemein hinsichtlich eines fairen Verhältnisses zwischen Datenpreisgabe und -nutzung sowie Kontrolle über die Daten (Campbell 1997; Malhotra et al. 2004) bestehen. Ein besonderer Schwerpunkt der Forschung zu Privatsphäre-Bedenken untersucht dabei vor allem, wodurch die Bedenken der Nutzer entstehen und wie sich diese auswirken können. So können beispielsweise durch das APCO-Model, bestehend aus Vorläufern (engl. ***a**ntecedents*), Privatsphäre-Bedenken (engl. ***p**rivacy **c**oncerns*) und Auswirkungen (engl. ***o**utcomes*) die Beziehungen zu anderen wichtigen Konstrukten aufgezeigt und analysiert werden (Smith et al. 2011). Ein Konstrukt, das dabei besondere Aufmerksamkeit in der Forschung erhalten hat, ist Vertrauen, wobei bislang noch Uneinigkeit über die genaue Richtungsabhängigkeit der Beziehung zwischen Vertrauen und Privatsphäre besteht (Pavlou 2011; Zheng und Pavlou 2010).

Wie bereits erwähnt, beschäftigte sich die bisherige Privatsphäre-Forschung darüber hinaus als drittes Themenfeld mit der kontextuellen Natur und den Auswirkungen dieser auf die Konstrukte-Beziehungen, die sich in verschiedenen Studien entweder in direkten oder moderierenden Einflüssen ausdrückten (z.B. Bansal und Zahedi 2008; Malhotra et al. 2004; Milberg et al. 1995). Schließlich ist informationelle Privatsphäre, wie in Kapitel 2.1 bereits erläutert, weniger als ein einzelnes, eindeutiges Konzept, sondern eher als ein vielschichtiges Phänomen zu sehen, weswegen es auch durch seinen Kontext spezifiziert und konzeptualisiert werden sollte (Acquisti 2004; Pavlou 2011). Kontext wird dabei als die Stimuli definiert, die das Individuum umgeben und sich, wenn sie verarbeitet werden, auf die Entscheidungsfindung eines Einzelnen auswirken (Cummings 1981; Mowday und Sutton 1993). So kann Kontext beispielsweise durch das Netz aus Beziehungen zwischen einem Subjekt, bestimmten Informationen des Subjekts, anderen Parteien und dem Kontext, in dem diese Verbindungen stattfinden, gebildet werden (Acquisti 2004). Auf einer weiteren Abstraktionsebene konnten weiterhin verschiedene Kontextfacetten identifiziert werden, wie der Typ der gesammelten Information (z.B. Malhotra et al. 2004), die Branche (z.B. Bansal und Zahedi 2008), die politische Lage (z.B. Etzioni 2005), sowie technologische Anwendungen und Tools (z.B. Awad und Krishnan 2006), die Auswirkungen auf das Privatsphäre-Konstrukt haben können (Smith et al. 2011). Die Thematik der Privatsphäre-erhaltenden oder -invasiven Tools und Technologien wird auch von Bélanger und Crossler als zentrales Forschungsgebiet hervorgehoben, ebenso sind Datenschutzpraktiken Gegenstand vieler Studien (Bélanger und Crossler 2011). Bei diesen Studien werden meist die individuellen und organisatorischen Maßnahmen zum Schutz der Privatsphäre sowie deren Einflussfaktoren untersucht (Bélanger und Crossler 2011), beispielsweise der nutzergetriebene Einsatz von Sicherheits-Toolbars (Wu et al. 2006), Browser-Warnsystemen (Egelman et al. 2008) oder Systemen zur Evaluation der Vertrauenswürdigkeit von Webseiten (Genkina und Camp 2005). Auch die Forschung zu Praktiken, die Unternehmen einsetzen können, ist vielfältig und untersucht unter anderem Datenschutzrichtlinien (engl. *privacy policies*) (Anton et al. 2004), Privatsphäre-Siegel (Hui et al. 2007) oder das Signalisieren von fairen Datenpraktiken auf Webseiten (Pavlou et al. 2007). Allerdings sind auch jene Untersuchungen, die Empfehlungen für organisationale Praktiken herleiten, wie die gesamte Privatsphäre-Literatur, oft nur aus der Nutzerperspektive vorgenommen worden. Forschung auf einer Gruppen-, organisationalen sowie gesellschaftlichen Analyseebene hat jedoch noch recht wenig stattgefunden (Bélanger und Crossler 2011; Smith et al. 2011), weswegen die

Adoptionen der Praktiken für Unternehmen in der Regel herausfordernd sind. Auf diese Thematik wird im 3. Kapitel detaillierter eingegangen.

Den Ausführungen von Pavlou (2011) folgend, gibt es noch ein weiteres Themenfeld, welches in der bisherigen Privatsphäre-Forschung bislang noch nicht ausreichend adressiert worden ist und wo daher weiterer Forschungsbedarf besteht: die Ökonomie von Privatsphäre. Dieser Teilbereich der Privatsphäre-Forschung wird in den nächsten Abschnitten genauer analysiert und bildet die Grundlage für die in den Kapiteln 4 bis 6 behandelten Studien dieser Dissertation.

2.3 Grundlagen der Ökonomie von Privatsphäre

Insbesondere durch den schon beschriebenen technologischen Fortschritt und der damit einhergehenden Verbreitung von Informationen durch das Internet, die vermehrt kommerziell verwendet werden, ist die Bedeutung von Forschung zur Ökonomie von Privatsphäre (engl. *economics of privacy*) seit Beginn des 21. Jahrhunderts gestiegen (Acquisti et al. 2016; Rust et al. 2002). Dabei befasst sich dieser Forschungsstrang vor allem mit dem Trade-off, dem Individuen, Gesellschaft und Unternehmen zwischen dem Preisgeben und der Nutzung von personenbezogenen Informationen sowie dem Schutz dieser, ausgesetzt sind (Acquisti 2010). Die bereits in der Einleitung aufgeworfene Thematik der organisatorischen Datenpraktiken nimmt daher eine zentrale Rolle in diesem Forschungsbereich ein. Schließlich können sich die Praktiken sowohl für die Individuen als auch für die Unternehmen vorteilhaft auswirken, allerdings können diese auch, je nach Kontext der Datenpreisgabe, negative Folgen für die Individuen haben und ihre Privatsphäre-Bedenken schüren, welche das Bedürfnis nach schützenden Maßnahmen weckt (Acquisti et al. 2016; Hui und Png 2006). Vor dem Hintergrund dieses Zielkonfliktes resümieren Acquisti et al. (2016): *„If it is true that information is power, then control over personal information can affect the balance of economic power among parties. Thus, privacy can simultaneously be a source of protection from the economic leverage a data holder could otherwise hold over the data subject (...); as well as be a tool the data subject may strategically use against the nonholder (...). Privacy is not the opposite of sharing−rather, it is control over sharing."* (Acquisti et al. 2016, S. 445).

Auch bei dieser Ausführung zeigt sich wieder, dass weniger der vollkommene Verschluss von Daten angestrebt wird, sondern eher deren angemessener Umgang im Zentrum stehen sollte. Ziel ist daher, dass die involvierten Parteien von der Datenökonomie profitieren können und die Risiken der Datenpreisgabe dennoch begrenzt werden. Vor diesem Hintergrund betrachtet

die Forschung zur Ökonomie von Privatsphäre dieselbe daher als ein handelbares Gut, welches spezielle Eigenschaften besitzt:

1. Obwohl es das Kernziel von Privatsphäre darstellt, kann es herausfordernd sein, einmal freigegebene Daten vor einer Duplizierung oder erneuten Weitergabe zu schützen, was unter anderem daran liegt, dass der Wert von Daten und Privatsphäre stark subjektiv sowie kontext-, zeit- und kombinationsabhängig ist (Acquisti et al. 2015; Acquisti et al. 2016; Nissenbaum 2004). So könnte ein E-Commerce-Nutzer beispielsweise einen Vorteil darin sehen, dass der Händler seine Produktreferenzen kennt, er würde aber wahrscheinlich keine Hinweise über seine Zahlungsbereitschaft für die Produkte preisgeben wollen (Varian 2002).
2. Weiterhin können verstärkt Informationsasymmetrien bestehen, da die Individuen oft nicht vollkommen über die angewendeten Datenpraktiken und Konsequenzen des Datenpreisgebens informiert sind, was dazu führen kann, dass die Vorteile der Preisgabe oft direkter wahrgenommen werden, während die Kosten unklarer und erst zu einem späteren Zeitpunkt erscheinen (Acquisti und Grossklags 2005; Acquisti et al. 2016).
3. Damit verwandt, werden bei dem beschriebenen Trade-off zwischen der Preisgabe und dem Schutz von Informationen oft materielle mit immateriellen Dimensionen vermischt, beispielsweise indem monetäre Vorteile, die mit einer Datenpreisgabe einhergehen können, mit dem Gefühl die Kontrolle über etwas Persönliches zu verlieren, abgewogen werden (Acquisti 2010; Acquisti et al. 2016).
4. Darüber hinaus kann Privatsphäre entweder als eigenständiges Gut angesehen werden, dass für sich selbst einen Wert besitzt, oder auch als intermediäres Gut, dessen Wert sich beispielsweise erst durch den Verlust von Privatsphäre offenbart (Acquisti et al. 2016; Farrell 2012).
5. Ein weiteres Charakteristikum ist die Herausforderung, den Wert von Privatsphäre und personenbezogenen Daten zu bestimmen, was essentiell dafür ist, dass Individuen fundierte Entscheidungen bezüglich der Preisgabe ihrer Daten treffen können (Berthold und Böhme 2010). Mögliche in der Literatur diskutierte Ansätze sind dabei, die potenziellen Kosten der Datenpreisgebenden oder die Profite der Datennutzer als Anhaltspunkte zu verwenden (Acquisti et al. 2016). Wie bereits im einleitenden Kapitel dieser Arbeit erläutert, werden personenbezogene Daten schließlich kontinuierlich zwischen Unternehmen weiterverkauft und auf entsprechenden

Datenmärkten gehandelt (Spiekermann et al. 2015a). Allerdings haben die Datenpreisgebenden in der Regel selbst keinen Zugang zu diesen Märkten, weswegen der sich so ergebende Wert nur Unternehmensinteressen widerspiegelt und die Wertvorstellung der Individuen vernachlässigt. Vor diesem Hintergrund würden Märkte, auf denen Nutzer ihre personenbezogenen Daten offen und transparent an interessierte Käufer verkaufen können, eine angemessenere Wertvorstellung wiedergeben (Acquisti et al. 2016). Allerdings sind zwar, wie bereits in der Einleitung erläutert, in den letzten Jahren bereits entsprechende Datenverkaufsplattformen entstanden, diese befinden sich jedoch noch in frühen Stadien, weswegen die Messung des Wertes von Daten und Privatsphäre anhand des Handels auf den Märkten derzeit noch erschwert wird. Derartige Datenverkaufsplattformen eignen sich jedoch gut als Kontext für die Wertermittlung, weswegen dieser Ansatz im 6. Kapitel vor dem Hintergrund der Bestimmung des Wertes von Daten sowie zur Untersuchung dieser als alternatives Geschäftsmodell genauer analysiert wird. Schließlich misst die bisherige Forschung, wie bereits kurz erläutert, den Wert, den Individuen ihren personenbezogenen Daten zuweisen, indem untersucht wird, welchen Wert Individuen für den Schutz ihrer Daten zu zahlen bereit sind und wie viel sie für den Verkauf ihrer Daten verlangen würden (Grossklags und Acquisti 2007). Das 4. Kapitel dieser Arbeit stellt die Ergebnisse bisheriger Studien zu dieser Thematik mit Hilfe einer strukturierten Literaturrecherche vor, während Kapitel 5 und 6 selbst Studien zur Wertermittlung von personenbezogenen Daten durch Untersuchungen der Bereitschaft von Individuen Daten zu verkaufen, behandeln.

Neben dem Themenfeld der besonderen Charakteristika von Daten und Privatsphäre, sowie der Wertermittlung derselben und Datenmarktplätzen, befasst sich Forschung zur Ökonomie von Privatsphäre darüber hinaus noch mit den thematischen Schwerpunkten der Nutzeridentifizierung und (Preis-)Diskriminierung (z.B. Mikians et al. 2013; Strahilevitz 2008; Taylor 2004; Villas-Boas 2004), der Rolle von Daten-Intermediären, die Informationen von Internetnutzern sammeln und weiterverkaufen (z.B. Bergemann und Bonatti 2015; Hagiu und Jullien 2011) sowie Anbieterstrategien, Marketing-Techniken und E-Commerce (z.B. Chellappa und Shivendu 2010; Hoofnagle et al. 2012; Lambrecht und Tucker 2013; Tang et al. 2008). Sowohl auf theoretischer als auch empirischer Ebene hat sich dabei gezeigt, dass die Effekte oft nicht ganz eindeutig sind und wirtschaftliche Konsequenzen von weniger Privatsphäre und mehr Informationspreisgabe in manchen Fällen vorteilhaft für die involvierten Parteien sind, in anderen allerdings negativ (Acquisti et al. 2016). So kann

Werbung, die auf Grundlage von gesammelten Daten für Individuen maßgeschneidert wurde, für diese informativer sein (Tucker 2012), während sie auf der anderen Seite die Entscheidungsfindung der Werbungsempfänger manipulieren kann (Calo 2014; Hanson und Kysar 1999). Noch deutlicher wird der Trade-off zwischen den potenziellen Vorteilen der Datenpreisgabe und –analyse sowie der damit einhergehenden Risiken in Bereichen wie der Medizin (beispielsweise im Kontext genetischer Tests auf Krebsrisiken (Miller und Tucker 2018)), Versicherungen (Troncoso et al. 2011) oder auf dem Kreditmarkt (Einav et al. 2013).

Es zeigt sich also, dass der Weg zu einem optimalen Gleichgewicht zwischen Datenschutz und Nutzen der Offenlegung nicht eindeutig ist, schließlich haben die verschiedenen Interessensgruppen (Individuen, Unternehmen und sogar Regierungen) teilweise unterschiedliche bis sogar widersprüchliche Zielvorstellungen (Acquisti et al. 2016). Hinzukommt, dass sich sowohl Informationstechnologien als auch Datenschutzbelange ständig weiterentwickeln und stark kontextabhängig sind, sodass statt eines einheitlichen und universellen Ansatzes, je nach Gegebenheiten differenzierte Lösungen zur Balancierung der widerstrebenden Kräfte notwendig sind (Acquisti et al. 2016).

3 Eine Untersuchung der konkurrierenden Anforderungen von Unternehmen im Umgang mit Nutzerdaten und Privatsphäre[2]

Wie im vorausgegangenen Kapitel bereits dargelegt, wurde die bisherige Privatsphäre-Forschung vorwiegend aus der Nutzerperspektive untersucht, während der Unternehmenssicht auf Privatsphäre bislang nur wenig Aufmerksamkeit gewidmet wurde (Bélanger und Crossler 2011; Smith et al. 2011). Vor diesem Hintergrund wird im Folgenden eine Studie vorgestellt, die den Zielkonflikt der Unternehmen untersucht, der sich aus dem Spannungsverhältnis zwischen dem Informationsbedarf der Unternehmen und der Notwendigkeit des Privatsphäre-Schutzes ihrer Nutzer ergibt. Dabei wird analysiert, wie die Unternehmen diesen Konflikt wahrnehmen und damit umgehen.

3.1 Motivation und Relevanz

"The companies that do the best job on managing a user's privacy will be the companies that ultimately are the most successful."

Fred Wilson (2018)

In den letzten Jahren haben immer mehr Unternehmen, die Online-Dienste anbieten, den Wert von Nutzerdaten als eine wichtige Ressource für ihr Geschäft erkannt. Schließlich können Kundeninformationen, wie bereits erwähnt, für Unternehmen einen großen Wettbewerbsvorteil darstellen (z.B. Detwiler 2015; Shapiro et al. 1998), beispielsweise indem sie zur Erstellung personalisierter Angebote genutzt werden, die wiederum die Erfolgsquote von Werbemaßnahmen erhöhen können. Gleichzeitig kann die Erhebung und Nutzung solcher Daten jedoch negative Folgen für Unternehmen haben, da Nutzer scheinbar zunehmend für das Risiko von Datenschutzverletzungen sensibilisiert sind, das mit der Erfassung und Nutzung ihrer Daten einhergeht (Lowry et al. 2017). Diese zweischneidige Natur der Erhebung und Verwendung von Nutzerdaten, die mit Einschnitten in die Privatsphäre der Nutzer verbunden sind, stellt Unternehmen vor große Herausforderungen. Denn einerseits wollen Unternehmen den Wert der Nutzerdaten nicht ungenutzt lassen, da sich dies negativ auf ihre Wettbewerbsstärke auswirken könnte, andererseits würden sie aber gerne auf eine

[2] Die in diesem Kapitel vorgestellte Studie basiert auf Gerlach et al. (2019).

umfangreiche Erfassung und Verwendung verzichten, um keine Nutzer aus Privatsphäre-Gründen zu verlieren. Hierbei ein Gleichgewicht zu finden, kann also, wie in dem einleitenden Zitat von Fred Wilson dargestellt, ein entscheidender Vorteil für Unternehmen sein.

Wie allgegenwärtig dieser Zielkonflikt der Unternehmen hinsichtlich der Privatsphäre ihrer Nutzer sein kann, verdeutlichen die beiden folgenden Beispiele: Wie bereits in der Einleitung dieser Arbeit erwähnt, wurde 2018 bekannt, dass es Dritten möglich war, personenbezogene Daten von Facebook-Nutzern zu erwerben (NewYorkTimes 2018). Als Folge dieses Skandals, entschieden sich einige Nutzer Facebook zu verlassen (NewYorkTimes 2018). Außerdem wurde eine Geldstrafe verhängt (TheGuardian 2018). Dieses Beispiel demonstriert, wie Facebook die negativen Konsequenzen einer Privatsphäre-invasiven Entscheidung tragen muss. Ein Beispiel für den umgekehrten Fall ist Apple. Der starke Fokus auf Datenschutz schränkt die Verwendung von Daten, die zur Personalisierung und Verbesserung des Sprachassistentensystems Siri genutzt werden können ein, weswegen Apple zunehmend Schwierigkeiten hat mit den Fortschritten von Amazon und Google im Bereich intelligenter Sprachsysteme Schritt zu halten (MacRumors 2017).

Trotz der Omnipräsenz dieses Zielkonfliktes, gibt es bislang nur wenig Forschung darüber, wie Unternehmen die Herausforderungen im Zusammenhang mit Nutzerinformationen und Privatsphäre wahrnehmen und damit umgehen. Vielmehr fokussierte sich die Mehrheit der bestehenden Privatsphäre-Studien auf die Nutzerperspektive und unterstreicht damit die Bedeutung des Datenschutzes für Individuen (Hui et al. 2007; Krasnova et al. 2010; Tsai et al. 2011). Dabei scheinen Unternehmen diese Empfehlungen jedoch nicht strikt zu befolgen (Bélanger und Crossler 2011; Lee et al. 2011; Wall et al. 2015). Gründe dafür zeigt die Forschung in den Bereichen der Organisationstheorie, des Marketings und der *Business Intelligence Analytics* auf, in der die Notwendigkeit für Unternehmen betont wird, Informationen zu sammeln und zu nutzen (Chen et al. 2012; Choo 1996; Huber 1990; Moorman 1995). Die Literatur der genannten Felder geht dabei allerdings nicht auf die mit der Privatsphäre verbundenen Herausforderungen in Zusammenhang mit der Erfüllung solcher organisatorischen Informationsbedürfnisse ein. Insgesamt wird in der aktuellen Literatur also nicht ausreichend dargelegt, wie Unternehmen mit den konkurrierenden Anforderungen in Bezug auf Nutzerinformationen und Datenschutz umgehen können, sowie wie sie diese bewältigen können. Vor diesem Hintergrund erforscht diese Studie die folgende Untersuchungsfrage:

Wie nehmen Unternehmen das Spannungsverhältnis zwischen der Notwendigkeit, die Privatsphäre ihrer Nutzer zu verletzen, um den Bedarf an Unternehmensinformationen decken zu können, und der Notwendigkeit, die Privatsphäre ihrer Nutzer zu schützen, um Kunden zu gewinnen und zu binden, wahr und gehen damit um?

Um diese Frage zu beantworten, wurde eine *Grounded Theory* Studie durchgeführt, die auf qualitativen Daten von Online-Dienstanbietern, die Kundeninformationen erheben und nutzen, basiert. Als Meta-Perspektive wird die Ambidextrie-Forschung (engl. *ambidexterity*) zu Grunde gelegt, die sich mit der Fähigkeit von Organisationen beschäftigt, zwei unterschiedliche Ziele gleichzeitig zu verfolgen (Gibson und Birkinshaw 2004). Diese metatheoretische Perspektive hilft dabei, die Privatsphäre-bezogenen Herausforderungen der Unternehmen zu theoretisieren, die sich aus einem ausgeglichenen Verhältnis zwischen den Informationsbedürfnissen eines Unternehmens und der Notwendigkeit, Nutzer zu gewinnen und zu binden, ergeben. Durch die Analyse konnten insgesamt vier kontextspezifische Spannungen identifiziert werden, denen Unternehmen, die mit Nutzerinformationen umgehen, ausgesetzt sind. Als Spannung wird dabei ein Geflecht aus gegensätzlichen Kräften verstanden, das zu widersprüchlichen Auswirkungen führt (Andriopoulos und Lewis 2009; Kreiner et al. 2006; Larson und Pepper 2003). Die in der vorliegenden Studie identifizierten Spannungen sind: (1) **die Datensammlung gegen Nutzergewinnung**, (2) **der Zeitrahmen der Sammlung**, (3) **Image-bezogene Kosten der Nutzerdaten** und (4) **der Verlust von Nutzern durch Datennutzung.** Die Ergebnisse deuten darauf hin, dass Unternehmen angesichts dieser Spannungen und des zusätzlichen kontextuellen Drucks, dem sie ausgesetzt sind, versuchen müssen, ein Gleichgewicht zwischen den konkurrierenden Anforderungen zu erreichen. Die Studie konnte zeigen, dass Unternehmen dies versuchen, indem sie verschiedene Taktiken anwenden, also Wege zum Umgang mit den Spannungen und den damit verbundenen Herausforderungen anwenden. Diese können helfen, das Gleichgewicht im Falle einer Störung aufrechtzuerhalten oder wiederherzustellen. Insgesamt konnte die Studie drei Kategorien von Taktiken identifizieren: (1) **Ersatztaktiken**, (2) **Transparenztaktiken** und (3) **Segmentierungstaktiken**.

Zusammengefasst, trägt die vorliegende Studie also zu einem besseren Verständnis darüber bei, wie Unternehmen die konkurrierenden Anforderungen an Nutzerdaten und Privatsphäre erleben und damit umgehen. Die Studienergebnisse können darüber hinaus als Grundlage für zukünftige Studien dienen, die untersuchen, wie Unternehmen die unterschiedlichen

Bedürfnisse von Unternehmen und Nutzern in Bezug auf die personenbezogenen Daten von Individuen und ihren Privatsphäre-Anforderungen erfüllen können.

Nach diesem einleitenden Kapitel, wird im nächsten Abschnitt der theoretische Hintergrund für diese Studie vorgestellt, indem auf die Bedeutung von Informationen für Unternehmen eingegangen wird und ein Überblick über die organisationsbezogene Privatsphäre-Forschung, als Ergänzung für die im 2. Kapitel bereits dargestellten allgemeinen Grundlagen, gegeben wird. Anschließend wird die Forschungsmethodik der *Grounded Theory* vorgestellt und dargestellt, wie den Prinzipien dieses Ansatzes gefolgt wurde, bevor die Ergebnisse der Studie präsentiert werden. Schließlich werden die Ergebnisse in die bestehende Forschung eingegliedert und die Implikationen der Ergebnisse sowie zukünftige Forschungspotenzial diskutiert.

3.2 Grundlagen der organisationalen Privatsphäre-Forschung und des Informationsbedarfs aus Unternehmensperspektive

3.2.1 Informationsbedarf von Unternehmen

Unternehmen, im Kontext dieser Studie insbesondere Anbieter von Online-Dienstleistungen, können als Organisationen gesehen werden, die Werte schaffen, mit ihrer Umgebung interagieren und ihren Kunden Produkte oder Dienstleistungen anbieten. Die grundlegende Notwendigkeit solcher Organisationen, Informationen von außerhalb der Unternehmensgrenzen zu erfassen und zu nutzen, wurde bereits in vielen Studien thematisiert (z.B. Choo 1996; Cohen und Levinthal 1990; Feldman und March 1981). Auf abstrakter Ebene können Unternehmen demnach als Informationsverarbeitungssysteme betrachtet werden, die Informationen benötigen, um mit unsicheren Begebenheiten umgehen zu können und sie so vorhersehbarer zu machen (Choo 1996). Schließlich müssen Unternehmen Daten sammeln und nutzen, um die Geschwindigkeit und Qualität ihrer Entscheidungen zu verbessern (Huber 1990; McAfee et al. 2012), ihr Umfeld zu verstehen (Choo 1996; Weick 1995), innovative Produkte zu entwickeln (Choo 1996; Cohen und Levinthal 1990), Marketing zu betreiben (Moorman 1995) und idealerweise einen Wettbewerbsvorteil zu schaffen (Evans und Wurster 1997; Porter und Millar 1985). Dieser Betrachtungsweise von Unternehmen als Informationsverarbeitungssysteme ist grundlegend für die *Business Intelligence Analytics*-Forschung, die darauf abzielt, die Informationsverarbeitungsfähigkeiten von Organisationsmitgliedern zu verbessern, um fundierte Entscheidungen treffen zu können (Chen et al. 2012; Davenport 2010; McAfee et al. 2012).

Was in diesen Studien der *Business Intelligence Analytics*-Forschung allerdings fehlt, sind Erkenntnisse darüber, wie Unternehmen mit den Privatsphäre-Herausforderungen, die mit der Erfüllung dieses Informationsbedarfs verbunden sind, umgehen, da schließlich eine Verbindung zwischen der Erfassung und Verwendung personenbezogener Daten und der Privatsphäre der Nutzer besteht. Diese Verbindung wiederum ist in der Privatsphäre-Literatur zwar gut dokumentiert, allerdings ist dort wenig Aufmerksamkeit auf die konkurrierenden Anforderungen und Spannungen bezüglich Nutzerinformationen und Privatsphäre gelenkt worden.

3.2.2 Privatsphäre-Forschung aus Unternehmensperspektive

Wie bereits erwähnt, konzentriert sich die Mehrzahl der bisherigen Privatsphäre-Forschungsstudien auf die Nutzerperspektive. Infolgedessen resultieren die Studien daher oft in Empfehlungen dahingehend, dass Unternehmen die Privatsphäre ihrer Nutzer schützen sollten, beispielsweise indem sie ihre Datenerfassung reduzieren, faire Informationsverarbeitungen anwenden und ihr datenschutzorientiertes Verhalten aktiv kommunizieren (Hui et al. 2007; Krasnova et al. 2010; Pavlou et al. 2007; Tsai et al. 2011). Trotz dieser wertvollen Beiträge lassen sich die Ergebnisse Nutzer-getriebener Studien durch ihre Einseitigkeit nicht einfach auf die Unternehmenspraxis übertragen, da sie die organisatorischen Informationsbedürfnisse, wie in Kapitel 3.2.1 dargelegt, vernachlässigen. Dabei hat Smith (1993) schon vor über zwei Jahrzehnten festgestellt, dass es an Forschung mangelt, die sich auf die Unternehmensperspektive von Privatsphäre-bezogenen Praktiken bezieht. Und auch mehr als zehn Jahre später äußerte Mary Culnan weiterhin, dass Privatsphäre ein Problem für Unternehmen darstellt, das bislang nur unzureichend untersucht wurde (Chan et al. 2005, S. 272). Daher ist es überraschend, dass sich seither trotzdem erst eine Handvoll Studien dieser Forschungslücke angenommen haben (z.B. Greenaway et al. 2015; Lee et al. 2011; Parks et al. 2017; Wall et al. 2015). Die wenigen Studien, die organisationale Privatsphäre-Forschung vorgenommen haben, sind in Tabelle 1 zusammengefasst. Eine Gemeinsamkeit dieser Studien ist, dass der Umgang mit Nutzerdaten und der Schutz der Privatsphäre als eine große Herausforderung für Unternehmen identifiziert wird.

Tabelle 1: Überblick der Privatsphäre-Literatur aus Unternehmensperspektive

Studie	Forschungsziel	Methode	Privatsphäre-bezogene Herausforderungen
Culnan und Williams (2009)	Hervorhebung der moralischen Verpflichtung der Unternehmen, die Privatsphäre ihrer Nutzer zu schützen.	Fallstudie	Unternehmen sollten verpflichtet sein, Vorsichtsmaßnahmen zu ergreifen, da dezentrale Technologien zu Privatsphäre-Verletzungen führen können.
Chan und Greenaway (2005)	Schaffung von theoretischen Perspektiven (z.B. institutioneller Ansatz, ressourcenbasierte Sichtweise), die das Datenschutzverhalten von Unternehmen erklären können.	Konzeptionelle Methode	Privatsphäre-relevante Entscheidungen müssen im Zuge von Unternehmenszielen getroffen werden, die möglicherweise mit dem Datenschutz konkurrieren.
Greenaway et al. (2015)	Unterschiede zwischen den Zielen des Informationsmanagements von Unternehmen und ihren moralischen und rechtlichen Verpflichtungen zum Schutz der Privatsphäre sollen in Einklang gebracht werden.	Konzeptionelle Methode	Der Schutz der Privatsphäre der Nutzer steht im Wettbewerb mit der Erreichung der Unternehmensziele in Bezug auf Nutzerdaten.
Lee et al. (2011)	Untersuchung eines unternehmensinternen Privatsphäre-Kalküls, das die Motive der Unternehmen zum Schutz der Privatsphäre basierend auf einer Bewertung der Vor- und Nachteile des Datenschutzes, erläutert.	Theoretisches Modell	Der Schutz der Privatsphäre der Kunden ist mit Vorteilen wie erweiterten Kundensegmenten und höheren Preisen verbunden, bringt aber Kosten für Investitionen in Personal und Infrastruktur sowie zusätzliche variable Kosten mit sich.
Milberg et al. (2000)	Besseres Verständnis der Zusammenhänge zwischen Kultur, regulatorischen Ansätzen zum Datenschutz, der Verwaltung personenbezogener Daten durch das Unternehmen und den Reaktionen der Verbraucher.	Umfrage	Durch ein internationales Umfeld (z.B. unterschiedliche Erwartungen und Gesetze) können sich Herausforderungen für die Unternehmensführung bei der Verwaltung personenbezogener Daten ergeben.
Parks et al. (2017)	Untersuchung der beabsichtigten und unbeabsichtigten Folgen des Schutzes der Privatsphäre in	*Grounded Theory* Studie	Unbeabsichtigte Folgen der Datenschutzvorkehrungen können die beabsichtigten Folgen überwiegen, was zu

	Unternehmen.		Maßnahmen führen kann, die die Einhaltung der Datenschutzbestimmungen beeinträchtigen.
Smith (1993)	Untersuchung des Prozesses mit dem Datenschutzrichtlinien und -praktiken erstellt werden.	Fallstudie	Externe Bedrohungen zwingen Unternehmen dazu ihre bestehenden Richtlinien und Praktiken zu überprüfen.
Wall et al. (2015)	Untersuchung der Wahrscheinlichkeit, dass Unternehmen sich entscheiden entweder gegen eine Datenschutz- oder eine Sicherheitsregel zu verstoßen.	Theoretisches Modell und Fallstudie	Organisatorische Belastungen und/oder Ressourcenengpässe können Unternehmen zu riskantem Verhalten in Bezug auf Privatsphäre und Sicherheit veranlassen.

Ein wichtiger Aspekt, der weiterer Untersuchung erfordert, ist die Herausforderung der Unternehmen, einerseits personenbezogene Daten zu sammeln und zu nutzen, um den Informationsbedarf aus Unternehmenssicht gerecht zu werden, und andererseits die Notwendigkeit, die Privatsphäre der Individuen zu schützen, um Kunden gewinnen und an das Unternehmen binden zu können. So betonen Bélanger und Crossler (2011, S. 1029) beispielsweise auch, dass die Privatsphäre-Forschung damit beginnen muss, die Anforderungen der Unternehmen in Hinblick auf Nutzerdaten zu berücksichtigen und untersuchen sollte, ob Unternehmen andere Privatsphäre-Interessen als die Dienst-Nutzer haben. Bisher haben sich zwei Studien mit dieser besonderen Herausforderung beschäftigt (Chan und Greenaway 2005; Greenaway et al. 2015). Dabei erklären Chan und Greenaway (2005) mit der ressourcenbasierten Sichtweise, warum Unternehmen mitunter die beiden Anforderungen unterschiedlich gewichten. Sie argumentieren dabei, dass Unternehmen, die durch überlegenes Wissen über ihre Kunden Wettbewerbsvorteile realisieren wollen, den Datenschutz unterordnen, um möglichst viele Nutzerinformationen zu sammeln und zu nutzen (Chan und Greenaway 2005). Im Gegensatz dazu werden Unternehmen, die ihre Wettbewerbsfähigkeit durch überlegene Vertrauenswürdigkeit anstreben, die Nutzung von Kundeninformationen unterordnen und die Privatsphäre ihrer Nutzer stärker schützen (Chan und Greenaway 2005). Greenaway et al. (2015, S. 580) leiten vier Kategorien von Unternehmen ab, die sich durch den Grad an Privatsphäre, den sie ihren Nutzern anbieten, unterscheiden, und erklären so wie sich Unternehmen entlang des Kontinuums bestehend aus „Privatsphäre ignorieren“ als ein Ende zu „Privatsphäre schützen“ als das andere Ende, positionieren. Die beiden Artikel helfen dabei zu verstehen, warum Unternehmen eventuellen Privatsphäre-Einschnitten ihrer Nutzer Vorrang vor dem Schutz ihrer Privatsphäre einräumen

und bieten eine Struktur mit der Unternehmen in Bezug auf ihre Privatsphäre-Niveaus beschrieben werden können (Chan und Greenaway 2005; Greenaway et al. 2015). Obwohl die dargestellten Studien wichtige Beiträge zum Verständnis der Unternehmensperspektive auf Privatsphäre bieten, bleibt unklar, wie Unternehmen die Spannungen wahrnehmen und bewältigen, die sich entweder aus der Priorisierung des Informationsbedarfes (der mit Einschnitten in den Datenschutz der Nutzer einhergeht) oder der Kundengewinnung und -bindung (verbunden mit dem Schutz der Privatsphäre) ergeben. Da die beiden Anforderungen inhärent miteinander verbunden sind, kann die Priorisierung einer der Anforderungen und die Vernachlässigung der anderen negative Folgen für Unternehmen haben. In der vorliegenden Studie, wird deshalb untersucht wie Unternehmen diese konkurrierenden Anforderungen wahrnehmen und damit umgehen.

3.3 Methodik

Die vorhandene Literatur bietet also nur wenige Erkenntnisse darüber wie Anbieter von Online-Diensten die Spannungen zwischen der Notwendigkeit, die Privatsphäre ihrer Nutzer zu verletzen um ihren Informationsbedarf decken zu können sowie der Notwendigkeit die Privatsphäre ihrer Nutzer zu schützen, um Kunden zu gewinnen und binden zu können, wahrnehmen und bewältigen. In solchen Kontexten, in denen die theoretischen Grundlagen weitgehend noch fehlen, kann die *Grounded Theory* Methode ein effektiver Ansatz sein, um dieses aufstrebende Forschungsgebiet zu untersuchen. *Grounded Theory* ist ein induktiver Forschungsansatz, der sich an Theoriebildung (im Gegensatz zur Theorieprüfung) orientiert und es Forschern ermöglicht, vorher entwickelte theoretische Haltungen zu vermeiden, die mögliche Ergebnisse beeinflussen könnten. Vielmehr ermöglicht dieser Ansatz eine aufgeschlossene Erforschung eines Phänomens, vermeidet die Anpassung von Daten an vordefinierte Theorien und lässt aus den Daten sinnvolle Konzepte entstehen (Birks et al. 2013; Charmaz 2014; Urquhart und Fernandez 2013). In der Wirtschaftsinformatik-Forschung, erfreut sich *Grounded Theory* zunehmender Beliebtheit und wurde bereits im Rahmen von Outsourcing-Projekten (Gregory et al. 2013), Unternehmenssystemen (Strong und Volkoff 2010), nachhaltigen Städten (Corbett und Mellouli 2017) und vielen anderen Themengebieten eingesetzt. Im Privatsphäre-Bereich hat eine aktuelle Studie den *Grounded Theory* Ansatz verwendet, um die beabsichtigten und unbeabsichtigten Folgen von Datenschutzmaßnahmen zu untersuchen (Parks et al. 2017).

Auf einer abstrakten Ebene geht die *Grounded Theory* Forschung wie folgt vor (Birks et al. 2013; Charmaz 2014; Urquhart et al. 2010): Nach der Auswahl eines Untersuchungsgebietes

und der Definition des Themas, beginnt der Forscher einen iterativen Prozess, der zwischen Datenerhebung und -analyse wechselt. Dabei wird die gesamte Datenerhebung von einem theoretischen Sampling (engl. *theoretical sampling*) geleitet. Dies bedeutet, dass der Forscher bei der Iteration zwischen Datenerhebung und -analyse aus theoretischen Gründen entscheidet, woher die nächste Probe entnommen wird und was erforscht wird. Ziel davon ist es, Daten zu erhalten, die die theoretischen Fragen beantworten, die zu einem bestimmten Zeitpunkt während des Forschungsprozesses entstanden sind (Birks et al. 2013; Urquhart und Fernandez 2013). Durch den ständigen Vergleich und der Kodierung der Daten im Zuge des *theoretical sampling* entstehen Themen und Kategorien, die schrittweise auf einer konzeptionellen Ebene (engl. *conceptual label*) abstrahiert werden können. Während des gesamten Prozesses schreibt der Forscher umfangreiche Memos, um über die aufkommenden Konzepte und Theorien zu reflektieren (Urquhart et al. 2010). An dem Punkt, an dem eine Sättigung eintritt, also keine neuen Konzepte oder Beziehungen entstehen, beendet der Forscher die Datensammlung und reduziert die entstandenen Konzepte und Beziehungen auf eine sinnvolle Kernmenge - die *Grounded Theory*. Diese Theorie wird dann auf bestehende Theorien bezogen, um zur theoretischen Integration in der Disziplin beitragen zu können. Das Ergebnis ist eine *Grounded Theory*, die fest in den Daten verwurzelt, realitätsnah und von hohem Forschungsinteresse ist, weil sich die Ideen den Weg in die Theorie "verdient" haben (Glaser 1978, S. 8).

In der *Grounded Theory* Forschung gibt es zwei verschiedene Stränge, die sich aus einer Meinungsverschiedenheit zwischen den beiden Mitbegründern über den "richtigen Weg" der Datenkodierung während einer Studie ergeben haben.[3] Die vorliegende Studie folgt dem Ansatz von Birks et al. (2013), die dafür plädieren, dass sich Forscher nicht allzu sehr mit der Art der *Grounded Theory* für eine bestimmte Forschungsarbeit befassen sollten, da diese nur von Elementen ablenkt, die beide Stränge gemeinsam haben und die "weitaus wichtiger" als die Unähnlichkeiten sind (S. 4). Nichtsdestotrotz ist diese Studie mehr auf den *Glaserian* Strang ausgerichtet, da weder die axiale Kodierung noch das Paradigmenmodell verwendet wurden, welche als wichtige Elemente des *Straussian* Strangs angesehen werden (Seidel und Urquhart 2013; Strauss und Corbin 1990). Das Paradigmenmodell wurde von Strauss und Corbin (1990) als Rahmen für die Verwendung in der axialen Kodierungsphase vorgeschlagen. Es bietet eine vordefinierte Struktur, die Forscher dabei unterstützt, auftretende Codes miteinander zu verknüpfen. Der Ansatz wurde von Glaser wegen seiner

[3] Für einen detaillierten Überblick gibt es fundierte Zusammenfassungen dieser Debatte (z.B. Seidel und Urquhart 2013; Urquhart et al. 2010).

begrenzten Sichtweisen auf die Beziehungen zwischen Konzepten kritisiert, die in der Realität existieren könnten (Seidel und Urquhart 2013). In den folgenden Unterabschnitten werden die durchgeführte Datenerhebung und -analyse detaillierter vorgestellt.

3.3.1 Datenerhebung

Mit Hilfe semi-strukturierter Interviews wurden Daten von Online-Dienstleistern erhoben, die personenbezogene Informationen von ihren Nutzern erfassen und verwenden. Da das Forschungsthema von den befragten Unternehmensvertretern als heikel angesehen werden kann, wurden keine zufälligen Unternehmen angefragt, sondern Online-Dienstleister die über persönliche Netzwerke bekannt sind. Auf diese Weise konnten auch Führungskräfte auf Vorstandsebene oder Produktmanager für die Interviews gewonnen werden. Dieser Ansatz gewährleistete zudem ein gewisses Maß an Vertrauen zwischen den Unternehmensvertretern und den Interviewern, was die Ehrlichkeit der von den Interviewten gegebenen Antworten erhöhte. Insgesamt konnten so Interviewdaten von 23 verschiedenen Unternehmen erhoben werden, was einer annehmbaren Stichprobengröße entspricht, zumal die Privatsphäre-Literatur Schwierigkeiten bei der Erhebung von Daten von Unternehmensteilnehmern zum Thema Datenschutz aufgezeigt hat (Bélanger und Crossler 2011).

Die Datenerhebung dieser Studie orientierte sich am Prinzip des *theoretical sampling* (Birks et al. 2013), was sich zum einen dadurch ausdrückt, dass die Stichproben-Wahl zwischen verschiedenen Unternehmen variiert wurde, um so zu untersuchen, ob unterschiedliche Unternehmens- oder Dienstleistungsmerkmale die Art und Weise verändern, wie über die sich ergebende Theorie nachgedacht wurde. So variieren die befragten Unternehmen beispielsweise in ihrer Größe, dabei sind sowohl kleine Start-ups als auch multinationale Konzerne vertreten. Geschäftsbereiche der Unternehmen sind z.B. E-Commerce, Gesundheit & Fitness, Spiele und Dienstleistungen die entweder über Webseiten oder über mobile Apps bereitstellt werden. Die Nutzerbasis der Dienste reichte von einigen Tausend bis zu mehreren Millionen Nutzern pro Monat. Die Unternehmen verlangten von ihren Nutzern ein breites Spektrum an Informationen, das von demographischen Daten über Standortdaten, Einkaufsdaten bis hin zu ID-Kartenscans reicht. Ein Überblick über die Charakteristiken des finalen Samples kann im Anhang 1 eingesehen werden, wobei aus Anonymitätsgründen nur begrenzte Informationen preisgegeben werden.

Das *theoretical sampling* drückt sich weiterhin darin aus, dass Fragen, die von früheren Daten inspiriert waren, verwendet wurden, um die Datenerhebung in den späteren Phasen zu

steuern. So war die Datenerhebung in der Anfangsphase vor allem darauf ausgerichtet, die Spannungen zu untersuchen, die Unternehmen beim Umgang mit Nutzerinformationen begegnen. Später, nachdem bereits ein tieferes Verständnis dieser Spannungen gewonnen werden konnte, verlagerte sich der Schwerpunkt der Datenerhebung auf die Art und Weise, wie die Anbieter diese Spannungen bewältigen und versuchen, in diesem Zusammenhang ein Gleichgewicht zu halten. Dementsprechend wurden die Interviewfragen fokussierter und strukturierter (Eisenhardt und Graebner 2007; Orlikowski 1993). Schließlich wurde die Auswahl neuer Interview-Partner zum Zeitpunkt der Sättigung beendet, als durch zusätzliche Datenerhebung und -analyse keine neuen Erkenntnisse gewonnen werden konnten.

Insgesamt wurden 27 semi-strukturierte Interviews mit Vertretern der 23 bereits erwähnten Unternehmen durchgeführt. Einige der Interviews waren Folgebefragungen, die darauf abzielten, die früher gesammelten Daten mit neuen Perspektiven aus späteren Iterationen der Datenanalyse zu bereichern. Für viele *Grounded Theory* Studien im Bereich der Wirtschaftsinformatik sind Interviews die primäre Datenquelle (Corbett und Mellouli 2017; Gregory et al. 2015; Urquhart et al. 2010), schließlich bieten sie auch den Vorteil, dass den Forschern eine starke Kontrolle über das Gespräch gegeben wird. Wie bereits erwähnt, wurden in den Interviews in der Regel Vertreter der Unternehmen interviewt, die im Management tätig sind, also zum Beispiel Produktmanager in größeren Unternehmen oder CEOs bei Start-ups und mittleren Unternehmen. Hierdurch konnte gewährleistet werden, dass die Befragten an wichtigen Entscheidungen über Dienstleistungen beteiligt sind und daher detaillierte Antworten auf Fragen bezüglich der Erhebung und Nutzung von Kundendaten und die damit verbundenen privatrechtlichen Herausforderungen geben konnten. Alle Interviews begannen mit einer kurzen Vorstellung und einer Einführung, sowie einer Beschreibung des Interviewprozesses und einer Vertraulichkeitszusicherung, in der auch das Interesse am Thema Privatsphäre aus organisatorischer Sicht aufgezeigt wurde. Die Interviews basierten auf einem Interviewleitfaden (siehe Anhang 2), der sich mit Verlauf der Studie iterativ weiterentwickelte. Im Durchschnitt wurde jeder Interviewpartner 48 Minuten lang befragt. Dabei wurden alle Interviews aufgezeichnet und transkribiert. Insgesamt kamen so über 18 Stunden Interviewmaterial zusammen und etwa 320 Seiten Text. Um die Aussagen der Interviewpartner zu validieren und ihre Inhalte zu überprüfen, wurden sekundäre Datenquellen miteinbezogen, indem beispielsweise die für den Dienst notwendigen Nutzerdaten-Abfragen oder die Datenschutzrichtlinien der Dienstleistungen kontrolliert wurden.

3.3.2 Datenanalyse, Kodierung und Memo-Schreiben

Wie in Kapitel 3.3 beschrieben, basiert die Datenanalyse dieser Studie auf dem von Glaser (1978) beschriebenen Kodierungsverfahren, welches mit Hilfe der Software *Atlas.ti* organisiert wurde. Obwohl im weiteren Verlauf dieses Kapitels drei Kodierungsstufen separat beschrieben werden, ist zu beachten, dass die Stufen in der Praxis untrennbar miteinander verbunden waren (Glaser 1978). Durch den ständigen Vergleich verschiedener Daten konnten Ähnlichkeiten und Unterschiede in den Antworten der Befragten identifiziert werden und frühere Codes verfeinert werden, sodass Kategorien zur Beschreibung von Beobachtungen, die miteinander in Beziehung standen, erstellt werden konnten. Auf diese Weise konnte nach und nach das Abstraktionsniveau erhöht werden. Während des gesamten Kodierungsprozesses wurden zudem umfangreiche Memos geschrieben. So wurden von Anfang an Memos verfasst, in denen Ideen für neue Konzepte beschrieben wurden, die im weiteren Verlauf durch Memos ergänzt wurden, welche wiederum zum Überdenken der Beziehungen zwischen den entstehenden Kategorien führten. Es wurden beispielsweise mehrere Diagramme erstellt, die die möglichen Beziehungen zwischen den Kategorien veranschaulichen. Während der Datenanalyse wurden die Memos mehrmals wiederholt und analysiert, um die verschiedenen, separaten Beobachtungen besser zu verstehen.

Die erste Stufe der Kodierung war eine offene Kodierung (engl. *open coding*) der gesammelten Daten, um gemeinsame Themen zu identifizieren und Beobachtungen zu verstehen (Glaser 1978). Zu diesem Zweck wurden die Daten Zeile für Zeile analysiert und konzeptionelle Bezeichnungen zu sinnvollen Texteinheiten, Phrasen, Sätzen, Halbsätzen oder Wörtern hinzugefügt. Um sicherzustellen, dass die Kodierungsergebnisse aus mehreren Perspektiven stammen, wurde der Kodierungsprozess von intensiven Diskussionen zwischen den Autoren begleitet. Diese Diskussionen stimulierten unterschiedliche Denkweisen über die Daten, die dazu führten, dass frühere Kodierungsergebnisse mehrfach überarbeitet und neu kodiert wurden. Basierend auf den offenen Codes, wurde eine selektive Kodierung (engl. *selective coding*) durchgeführt, um aufkommende Codes zu gruppieren, die sich auf ein Kernphänomen konzentrieren, sodass schließlich nur Codes erhalten bleiben, die ausreichend mit diesem Phänomen verbunden sind (Glaser 1978). Angesichts der Forschungsziele dieser Studie wurden die Spannungen, denen die befragten Anbieter ausgesetzt waren, und die Balance, die sie zu erreichen versuchen, als Kernphänomene ausgewählt. Durch Fokus auf diese beiden Phänomene, konnten mehrere Kategorien identifiziert werden, die für Studien von Interesse sind, die untersuchen, wie Anbieter mit Kundeninformationen umgehen. So wurden zum Beispiel mehrere Taktiken identifiziert, mit denen Anbieter ein Gleichgewicht

aufrechterhalten oder wiederherstellen konnten, nachdem es gestört worden war. Zuletzt wurde die theoretische Kodierung (engl. *theoretical coding*) verwendet, um Beziehungen zwischen den Kernkategorien zu identifizieren, die sich aus der selektiven Kodierung ergeben hatten (Glaser 1978). Daraus resultierte eine Theorie, die erklärt, wie Anbieter bestimmte Spannungen überwinden, die bei dem Versuch, ein Gleichgewicht herzustellen, entstehen und wie interner und externer Druck sowie das Verhalten des Unternehmens dieses Gleichgewicht beeinflussen.

Insgesamt führten die ständigen Vergleiche, Iterationen zwischen Datenerhebung und -analyse und umfangreiches Memo-Schreiben zu einer finalen Theorie, die im Folgenden vorgestellt wird. Beim Aufbau dieser Theorie wurde während des gesamten Forschungsprozesses strikt an den Prinzipien der *Grounded Theory* Methodik festgehalten. Tabelle 2 fasst nochmals zusammen, wie die Anforderungen an *Grounded Theory* Studien, wie sie von Birks et al. (2013) vorgeschlagen werden, erfüllt wurden.

Tabelle 2: Überblick über die Einhaltung der Anforderungen an *Grounded Theory* Studien basierend auf Birks et al. (2013)

Anforderungen	Umsetzung in der Studie
Theorie-Entwicklung: Das Ziel der Studie muss die Theorieentwicklung und nicht die Theorieprüfungen sein.	In dieser Studie wurde eine "Typ II"-Theorie entwickelt (Gregor 2006), die erklärt, wie Unternehmen die konkurrierenden Anforderungen, die sich einerseits aus ihrem Informationsbedarf und andererseits aus der Notwendigkeit Nutzer zu gewinnen und an sich zu binden ergeben, balancieren. Dabei wurde keine im Vorhinein entwickelte theoretische Haltung in die Studie mit einbezogen, sondern die Theorie aus den erhobenen Daten selbst entwickelt.
Konstante Vergleiche: Die Beobachtungen müssen ständig verglichen und aus verschiedenen Blickwinkeln betrachtet werden, um neue Kategorien einer strengen Prüfung zu unterziehen.	Es wurden ständig alle Daten mit den neuen Konzepten verglichen, um zu untersuchen, wo die Daten passen und wo theoretische Überlegungen noch unzureichend waren. Weiterhin wurden auch frühere mit späteren Daten sowie Daten von kleinen und großen Unternehmen und Daten aus verschiedenen Geschäftsbereichen miteinander verglichen.
Iterative Kodierung: Die Theorie wird auf Grundlage mehrerer Iterationen der Daten-Kodierung entwickelt.	Die Kodierung verlief iterativ und wurde auf drei verschiedenen Kodierungsebenen (offene, selektive und theoretische Kodierung) durchgeführt, zwischen denen iteriert wurde. Aufgrund der ständigen Vergleiche sowie der intensiven Diskussionen zwischen den Autoren wurden die Daten häufig überprüft und neu kodiert.
Theoretische Stichproben-Wahl: Der Forscher entscheidet aus theoretischen	Die Wahl der Interviewpartner wurde in dieser Studie durch theoretische Überlegungen bestimmt.

Gründen, welche nächste Stichprobe genommen werden soll und woher. Es werden solange neue Datenquellen gesucht, bis die theoretische Sättigung erreicht ist und keine neuen Erkenntnisse mehr entstehen.	Zum einen wurden verschiedene Unternehmen und Dienstleistungen in das Sample einbezogen, um zu analysieren, ob solche Unterschiede in den Beobachtungen die bisherigen Erkenntnisse bereichern oder ihnen widersprechen. Zum anderen wurde der Interviewleitfaden (siehe Anhang 2) schrittweise angepasst, um neue Fragen, die sich im Laufe des Forschungsprozesses ergaben, zu berücksichtigen. Die Datenerhebung wurde an dem Punkt beendet, an dem keine neuen Erkenntnisse aus der zusätzlichen Datenerhebung und -analyse gewonnen werden konnten, also die theoretische Sättigung, erreicht war.
Management von vorgefassten Meinungen: Die Studie wird nicht von bestehenden Theorien bestimmt.	Obwohl es in diesem Bereich einige theoretische Ansätze zur Erforschung des Datenschutzes aus organisatorischer Sicht gab, wurde die Studie ohne vorgefasste Meinungen oder im Vorhinein entwickelte Hypothesen durchgeführt. Vielmehr wurde es ermöglicht, dass aus den Daten Konzepte und Beziehungen entstehen.
Uneingeschränkte Verbindung zwischen Datenerhebung und -analyse: Datenerhebung und -analyse müssen sich abwechseln bis die theoretische Sättigung erreicht ist.	Datenerhebung und -analyse verliefen eng verzahnt. Die zuvor erhobenen Daten wurden analysiert und diskutiert und durch die theoretische Stichproben-Wahl wiederum in neue Datenerhebungen einbezogen.

3.4 Ergebnisse

In diesem Unterkapitel wird die Theorie vorgestellt, die sich aus den erhobenen und analysierten Daten ergeben hat. Die Theorie erklärt, wie Unternehmen die konkurrierenden Herausforderungen im Umgang mit Nutzerdaten erleben und damit umgehen, um einerseits ihren Informationsbedarf zu decken, was mit Einschnitten in die Privatsphäre ihrer Nutzer verbunden ist und andererseits die Privatsphäre schützen wollen, um Nutzer zu gewinnen und zu binden. Im Folgenden werden zunächst verschiedene Spannungsfelder vorgestellt, die sich aus dieser übergreifenden Herausforderung ergeben haben. Jede Spannung definiert dabei Herausforderungen, die Unternehmen im Umgang mit Nutzerdaten beeinflussen. Vor dem Hintergrund dieser Spannungen müssen Unternehmen versuchen ein Gleichgewicht zu schaffen und aufrechtzuerhalten. Aufgrund von internen und externen Druckausübungen stellt der Umgang mit den Herausforderungen an sich häufig selbst eine Herausforderung dar. Im Anschluss werden die beobachteten Taktiken vorgestellt, die Unternehmen zur Wiederherstellung oder proaktiven Aufrechterhaltung eines Gleichgewichts einsetzten.

3.4.1 Spannungen der Anbieter bei der Erhebung und Nutzung von Nutzerdaten

Wie in früheren Forschungsstudien, die übergeordnete, konkurrierende Anforderungen von Unternehmen untersuchten (z.B. Andriopoulos und Lewis 2009; Smith und Tushman 2005), konnten durch die Analyse der Interviewdaten vier verschiedene Kategorien von Spannungen identifiziert werden, die sich auf die Erhebung und Verwendung von Nutzerdaten beziehen. Tabelle 3 fasst die vier Spannungen, die den Kontext definieren, in dem die Unternehmen agieren müssen, graphisch noch einmal zusammen.

Tabelle 3: Durch konkurrierende Anforderungen entstehende Spannungen

Spannungen	Anforderung		Gegensätzliche Anforderung
Spannung 1: Datensammlung gegen Nutzergewinnung	Sammeln von Nutzerdaten	↯	Gewinnen und Binden von Nutzern
Spannung 2: Zeitrahmen der Sammlung	Gegenwärtiges Sammeln von Nutzerdaten	↯	Zukünftiges Sammeln von Nutzerdaten
Spannung 3: Image-bezogene Kosten der Nutzerdaten	Sammeln und Verwenden von Nutzerdaten	↯	Aufrechterhalten eines guten Unternehmensimages
Spannung 4: Verlust von Nutzern durch Datennutzung	Ausweiten des Verwendungszwecks	↯	Gewinnen und Binden von Nutzern

Spannung 1: Datensammlung gegen Nutzergewinnung

Für die Unternehmen ergibt sich eine Spannung aus der Notwendigkeit Nutzerdaten zu erheben, die mit der Anforderung konkurriert, Kunden zu gewinnen und zu binden. Einerseits ist die Erfassung von Nutzerdaten eine Voraussetzung, um vielen organisatorischen Anforderungen gerecht zu werden. So kann beispielsweise das Sammeln von mehr Informationen über Nutzer zu einer Erhöhung der allgemeinen Servicequalität, einer höheren Effektivität von Marketingaktivitäten oder zu besseren strategischen Entscheidungen führen. Auf der anderen Seite kann das Sammeln von mehr Informationen (potenzielle) Nutzer auch abschrecken. Ein interviewter Unternehmensvertreter, der sicherstellen musste, dass auf seiner Plattform keine gefälschten Bewertungen abgegeben wurden, und daher die Nutzer aufforderte, ihre E-Mail-Adressen anzugeben, beschrieb diese Spannung wie folgt (S#14): *„Ich meine, was sie sicherlich verschreckt und was wir auch wissen ist, dass sie sich natürlich in irgendeiner Form validieren müssen. Also zum Beispiel durch Abgabe ihrer E-Mail-Adresse. Also wenn wir da auf die Conversion schauen würden, wäre die natürlich deutlich höher, wenn wir das nicht hätten. Aber das ist dann so bei uns der Trade-off aus Datenqualität versus Conversion.“*

Dieses Zitat veranschaulicht, dass dieses Unternehmen bei der Entscheidung für oder gegen die Erhebung von E-Mail-Adressen ihrer Nutzer ein Opfer bringen muss. In ähnlicher Weise stellten zwei E-Commerce-Anbieter fest, dass das Sammeln von mehr Informationen über ihre Nutzer mit der potenziellen Gefahr einhergeht, Nutzer ganz zu verlieren. So beschrieb einer von ihnen (S#10): *„Genau, wir hatten zum Beispiel mal das Geburtsdatum drin als optionales Feld. Da haben wir ganz klar festgestellt, dass je mehr Daten man angeben muss, besonders das Geburtsdatum, das schreckt die Leute ab.“* Der zweite E-Commerce-Anbieter äußerte sich dazu etwas allgemeiner (S#21): „*Man möchte vielleicht mehr Daten haben, aber man riskiert natürlich, wenn man dem Kunden mehr abverlangt, auch, dass der Kunde sich vielleicht nicht registriert.“*

Aufgrund dieser Spannung müssen Unternehmen ihre Entscheidungen sehr vorsichtig treffen, denn sowohl die Vernachlässigung ihres Informationsbedarfes als auch ihres Bedarfs nach Gewinnung und Bindung von Kunden, könnte einen erheblichen Einfluss auf ihren Gesamterfolg haben.

Spannung 2: Zeitrahmen der Sammlung

Eine weitere Spannung basiert auf der Frage, ob Daten, die zum jetzigen Zeitpunkt nicht verwendet werden, aber in Zukunft benötigt werden könnten, jetzt oder zu einem späteren Zeitpunkt gesammelt werden sollten. Der Anbieter eines Fitnessdienstes, der sich entschieden hat, zum jetzigen Zeitpunkt keine Daten für zukünftige Zwecke zu erheben, gab dazu an (S#05): *„Und dann war für uns eher die Diskussion, wollen wir diesen Wert schon abfragen (...) oder fragen wir den Wert bewusst nicht ab, was für die Conversion in der Regel immer besser ist, je weniger Werte man abfragt. Insbesondere, weil wir den Wert [heute] nicht verwenden.*“

Die Datenerhebung zum gegenwärtigen Zeitpunkt könnte die gleichen negativen Folgen haben wie bei der vorherigen Spannung und zwar Nutzer zu verschrecken, die sich über die Menge der gesammelten Daten Sorgen machen. Dem gegenüber steht die Notwendigkeit von Unternehmen im Voraus zu planen. So können bestimmte Daten, die heute nicht verwendet werden, in Zukunft notwendig werden, wie das nächste Zitat zeigt (S#15): *„Ich möchte den Nutzer nicht direkt am Anfang alles Mögliche abfragen, um ihn möglicherweise bei der Registrierung schon zu verlieren. Nein, wir wollen die Hürde so niedrig wie möglich haben. (....) Aber (...) ich brauche diese Daten irgendwann für bestimmte Fälle.“*

Eine spätere Einholung der Erlaubnis zur Erfassung dieser Daten hätte jedoch ebenfalls negative Auswirkungen, da bestehende Nutzer über Änderungen der Datenschutzrichtlinien oder der Berechtigungen für mobile Anwendungen informiert werden müssen. Dies könnte die Aufmerksamkeit der Nutzer sehr deutlich auf die Datenerfassung lenken und so dazu führen, dass sie den Service nicht mehr nutzen. Ein Anbieter einer mobilen Nachrichten-App erklärt die Schwierigkeit, zu einem späteren Zeitpunkt zusätzliche Daten anzufordern wie folgt (S#03): *„(...) jedes Mal, wenn du mehr willst [mobile App-Berechtigungen], muss man die Bestätigung updaten. Bei Kontaktdaten oder wenn du Push-Notifications brauchst und bei jedem Schritt verlierst du wahrscheinlich 15% deiner Nutzer.“* So stehen Unternehmen vor der schwierigen Entscheidung, ob sie möglicherweise in der Zukunft benötigte Daten bereits zum gegenwärtigen Zeitpunkt erfragen, oder dies auf einen späteren Zeitpunkt verschieben.

Spannung 3: Image-bezogene Kosten der Nutzerdaten

Für Unternehmen ist es ebenfalls wichtig, über die unmittelbaren Auswirkungen ihrer Praktiken auf den Erfolg ihrer Dienstleistungen hinauszuschauen. Unternehmen, die mehr als einen Service anbieten oder eine mobile App beziehungsweise Webseite zur Ergänzung ihres Kerngeschäfts haben, müssen sich der Auswirkungen bewusst sein, die ihr Umgang mit Nutzerdaten auf ihr Unternehmens- oder Markenimage haben können. Die Erhebung weiterer Nutzerdaten oder die Nutzung von Daten für zusätzliche Zwecke, könnte auf Kosten dieses Images gehen - zum Beispiel, wenn eine Marke oder ein Firmenname mit Vertrauen und Verantwortung verbunden war und dieses nun geschwächt wird. In diesem Zusammenhang beschrieb ein E-Commerce-Dienstleister seine Ängste davor, dass die Erhebung zu vieler Daten das Image des Unternehmens schädigen könnte, wie folgt (S#21): *„Ja, wir von [großer E-Commerce-Service] haben ganz viel Angst, dass unser Image durch so etwas [das Sammeln von zu vielen Daten] beschädigt wird. Deshalb sind wir ja auch sehr vorsichtig an der Ecke.“*

Ebenso war es einem Unternehmen, das neben seinen stationären Geschäften auch einen Online-Shop anbiete, ein großes Anliegen, das positive Markenimage zu erhalten, da die Marke im Offline-Kanal sehr beliebt ist (S#23)*: „[Es ist] eine sehr große Herausforderung. Weil unser Unternehmen extrem darauf angewiesen ist, auf das positive Image. Dadurch, dass die Marke seit 30 Jahren besteht (...) wäre es natürlich in dem Fall ein Riesen-Fauxpas wenn da rauskommen würde „Ach die sind ja doch nur Amazon, wie Amazon“, so ungefähr, oder „wie die großen, die [Daten] sammeln [und] sammeln“ (...) das wäre natürlich ein Riesenproblem für uns und das hat man definitiv auf dem Schirm.“*

In einem anderen Fall wurde der Online-Service von einer Tochtergesellschaft eines größeren Unternehmens bereitgestellt. Die Entscheidungen dieser Tochtergesellschaft könnten auf das Image des Hauptkonzerns übergreifen, und das musste berücksichtigt werden:

Interviewer: *„Ist das bei Ihnen in der Diskussion, das bestimmte Nutzungsarten oder Sammlung von Daten irgendwie ein Risiko für das Unternehmensimage sein könnte?“*

S#14: *„(....) das ist natürlich bei uns auch nochmal die Herausforderung, wir sind ja eine hundertprozentige Tochter von [Name der Muttergesellschaft].“*

Aber auch hier würde das Nicht-Erheben oder Verwenden von Daten bedeuten, dass das Unternehmen seinen Bedarf nach einer besseren Entscheidungsfindung und Vermarktung vernachlässigen müsste, was es unter anderem vor die Herausforderung stellt, diese Bedarfe gegen das Unternehmens- oder Markenimage abzuwägen.

Spannung 4: Verlust von Nutzern durch Datennutzung

Die vierte identifizierte Spannung besteht darin, dass entschieden werden muss, wie ein Unternehmen zuvor erfasste Nutzerdaten verwenden kann. Diese Spannung unterscheidet sich konzeptionell von der ersten Spannung, die mit der Frage der Informationsbeschaffung verbunden ist, da es hier um die Nutzung und Verarbeitung von bereits erfassten Informationen geht (Culnan 1993; Kettinger und Marchand 2011; Moorman 1995). Die befragten Unternehmen fühlten sich oft darin eingeschränkt, bereits zur Verfügung stehende Daten zu nutzen, da eine vielfältige Verwendung dieser Daten Nutzer verunsichern könnte, die sich in ihrer Privatsphäre verletzt fühlen. Allerdings sehen sich die Unternehmen auch dem Druck ausgesetzt, mit der Konkurrenz Schritt zu halten und deshalb genötigt, den Wert ihrer bereits vorhandenen Daten zu maximieren, indem sie mehr über ihre Nutzer erfahren, um so ihre Effizienz steigern zu können. So hatte der Anbieter eines Nachrichtenportals beispielsweise mit einem Verlag vereinbart, dass personenbezogene Daten von Nutzern, die dieser Praxis zustimmen, an diesen weitergegeben werden. Diese zusätzliche Art der Nutzung personenbezogener Daten könnte aber auf Kosten des Verlustes von Nutzern gehen, die dieser Praxis nicht zustimmen (S#03): *„Also zum Beispiel haben wir jetzt ein neues Projekt mit einem Verlag gestartet und da geht es darum, dass am Ende des Projekts Nutzerdaten übertragen werden müssen. Das ist also Teil des Vertrags. Und da, also in dem Fall, müssen wir einfach, nach sechs Monaten das User Agreement updaten. Die Nutzer müssen dem zustimmen. Diejenigen, die nicht zustimmen, die müssen wir leider wahrscheinlich wegschmeißen, oder, nicht wegschmeißen, aber wir dürfen die nicht übertragen.“*

Aus Unternehmensperspektive muss also ein Teil der Privatsphäre der Nutzer geopfert werden, um den Geschäftszweck erfüllen zu können. Ein vollständiger Privatsphäre-Schutz für jeden Nutzer wurde daher aus Sicht der Unternehmen in der Regel als nicht realisierbar angesehen. Der Anbieter eines Fitnessdienstes erklärte die Notwendigkeit mit Drittanbietern zusammenzuarbeiten, um Umsätze zu generieren, wie folgt (S#09): *„Das würden wir dann bei uns schon machen [personalisierte Werbeanzeigen für Dritte schalten], aber halt ohne das irgendwie weiterzugeben. Da sind wir halt der Meinung, irgendwo müssen die Leute dann auch Verständnis haben, dass wir auch Geld verdienen müssen und wer das halt komplett kostenfrei nutzen will, irgendwo müssen wir das Geld dann auch herholen."*

Dieses Spannungsverhältnis zwingt die Unternehmen sorgfältig darüber nachzudenken, ob verschiedene Arten der Datennutzung den Anbietern auf lange Sicht tatsächlich zugutekommen, oder ob die negativen Folgen der von den Nutzern wahrgenommenen Datenschutzrisiken überwiegen. Schließlich können Änderungen an einem Service, die auf einer zusätzlichen Nutzung von Kundeninformationen beruhen, zu Nutzerverlusten führen, wie das folgende Zitat verdeutlicht (S#22): *„Also wir sehen ja, wenn wir irgendwas in der App (basierend auf Kundendaten) machen, was problematisch ist, dann sehen wir häufig, dass die Apps deinstalliert werden."*

Weitere Zitate für alle vier in diesem Abschnitt vorgestellten Spannungen sind in Anhang 3 einzusehen. Insgesamt werden die identifizierten Spannungen von den Unternehmen als große Herausforderung empfunden und definieren den Kontext, in dem die Organisationen agieren und Entscheidungen treffen müssen.

3.4.2 Ambidextrie als Meta-Theorie

Die im vorausgegangenen Unterkapitel beschriebenen Spannungen bestimmen den Kontext des sich ständig verändernden Umfeldes, in dem Unternehmen agieren und mit dessen konkurrierenden Anforderungen sie jonglieren müssen. Ein einseitiges Handeln bringt die Vernachlässigung der anderen Seite mit sich. Basierend auf diesen Erkenntnissen wurde Ambidextrie als metatheoretische Perspektive übernommen, um die Erkenntnisse zu unterstützen und zu bereichern. Wie oft bei *Grounded Theory* Studien, hat sich diese Perspektive im gesamten Forschungsprozess als relevant erwiesen (Urquhart und Fernandez 2013).

Unternehmensbezogene Ambidextrie bezieht sich im Allgemeinen auf die Fähigkeit eines Unternehmens, zwei verschiedene Dinge gleichzeitig zu verfolgen (Gibson und Birkinshaw

2004, S. 210). Forschung zur unternehmensbezogenen Ambidextrie geht dabei davon aus, dass Anforderungen an Unternehmen immer, bis zu einem gewissen Grad, im Widerspruch stehen und daher Kompromisse eingegangen werden müssen (Gibson und Birkinshaw 2004; Raisch und Birkinshaw 2008). Beispiele für solche Konflikte sind die zwischen Effizienz und Flexibilität (Adler et al. 1999), Exploration und Exploitation (Andriopoulos und Lewis 2009; March 1991) sowie Differenzierungs- und Niedrigkostenstrategien (Porter 1996). In der vorliegenden Studie sind die "zwei verschiedenen Dinge" die Notwendigkeit eines Unternehmens, seinen Informationsbedarf zu decken, was mit einer Verletzung der Privatsphäre seiner Nutzer einhergeht, sowie die Notwendigkeit, die Privatsphäre seiner Nutzer zu schützen, um neue Kunden zu gewinnen und bestehende an sich zu binden.

Um solche konkurrierenden Anforderungen in Einklang bringen zu können, müssen Unternehmen einen Weg finden, mit den gegensätzlichen Kräften umzugehen, wobei das ideale Ergebnis als Gleichgewicht beschrieben wurde (March 1991; Raisch und Birkinshaw 2008; Ramesh et al. 2012). Obwohl Kompromisse nie vollständig beseitigt werden können, ist die Erreichung eines Gleichgewichts mit überlegener Leistung und langfristiger Wettbewerbsfähigkeit verbunden (Gibson und Birkinshaw 2004; March 1991; Raisch und Birkinshaw 2008). Diese Gleichgewichts-Perspektive passt gut zu den empirischen Beobachtungen dieser Studie, sodass Ambidextrie als Meta-Theorie angemessen erscheint. So sagte zum Beispiel der Manager eines Nachrichtenportals (S#22): *„Wir versuchen immer genau zu steuern und man steuert da mal ein bisschen in die eine, in die andere Richtung, aber grundsätzlich versuchen wir natürlich genau da eine Balance zu finden."*

Andere Interviewte benutzten ähnliche Ausdrücke, um auf die Notwendigkeit zum Ausgleich konkurrierender Anforderungen hinzuweisen und beschrieben sie beispielsweise mit „*in einem gesunden Verhältnis stehen*" (S#14), „*einen Spagat*" (S#12) zwischen den beiden gegensätzlichen Kräften erreichen, „*den Mittelweg zu finden*" (S#21) und das Sicherstellen „*dass man den Bogen nicht überspannt*“ (S#18). Dabei ist wichtig zu beachten, dass das, was eine effektiv ausgewogene Konfiguration von Aktivitäten darstellt, vom Kontext und der Situation abhängt (Auh und Menguc 2005; Cao et al. 2009; Raisch und Birkinshaw 2008). So können beispielsweise dieselben explorativen oder exploitativen Maßnahmen in ihrer Wirksamkeit variieren, je nach Umfeld, in dem ein Unternehmen tätig ist (Auh und Menguc 2005). Weiterhin können die Effekte, die das Gleichgewicht oder Ungleichgewicht auf die Unternehmensergebnisse haben, durch Kontextfaktoren wie die Unternehmensgröße oder Umweltfreundlichkeit variieren (Cao et al. 2009). In ähnlicher Weise können auch zwei

Individuen unterschiedliche Vorstellungen davon haben, wie ihr Arbeits- und Privatleben ausbalanciert sein kann (Kreiner et al. 2006). Das Gleichgewicht ist also dynamisch und kann sich sowohl mit der Zeit als auch situationsbedingt ändern und unterschiedliche Ausprägungen annehmen (Cardinal et al. 2004, S. 412). Auch in dieser Studie zeigte sich, dass die befragten Unternehmen die Gleichgewichtszustände unterschiedlich wahrnehmen. Ein Zustand, den ein Unternehmen als ausgewogen empfindet, kann von einem anderen als unausgewogen wahrgenommen werden.

3.4.3 Aufrechterhaltung des Gleichgewichts in dynamischen Kontexten

Im Folgenden wird aufgezeigt, wie die befragten Unternehmen versuchen, die konkurrierenden Anforderungen, denen sie ausgesetzt sind, auszugleichen, und Taktiken präsentieren, mit denen sie das Gleichgewicht aufrechterhalten oder wiederherstellen, wenn es gestört wird. Abbildung 2 gibt einen Überblick über die diesbezüglichen Erkenntnisse und zeigt, wie das Gleichgewicht eines Unternehmens durch interne und externe Faktoren gestört werden kann, die das Unternehmen dazu veranlassen, seine Datenpraktiken zu ändern. Schließlich können Änderungen im Umgang mit Daten zu einem Ungleichgewicht führen. Eine Entscheidung über eine neue Datenpraktik in Form von Sammlung oder Nutzung von Informationen würde einen gewissen Grad an Privatsphäre-Verletzungen mit sich bringen, was das Risiko eines Nutzer- oder Imageverlustes birgt. Die Ablehnung einer Praktik würde zwar die Privatsphäre der Nutzer schützen, aber die Informationsbedarfe des Unternehmens vernachlässigen. Ein Mittelweg könnte daher als Kompromiss dienen. Abhängig von den getroffenen Entscheidungen verwenden die Unternehmen drei Kategorien von Taktiken, um ein Gleichgewicht wiederherzustellen oder proaktiv aufrechtzuerhalten, auf die im Folgenden detailliert eingegangen wird.

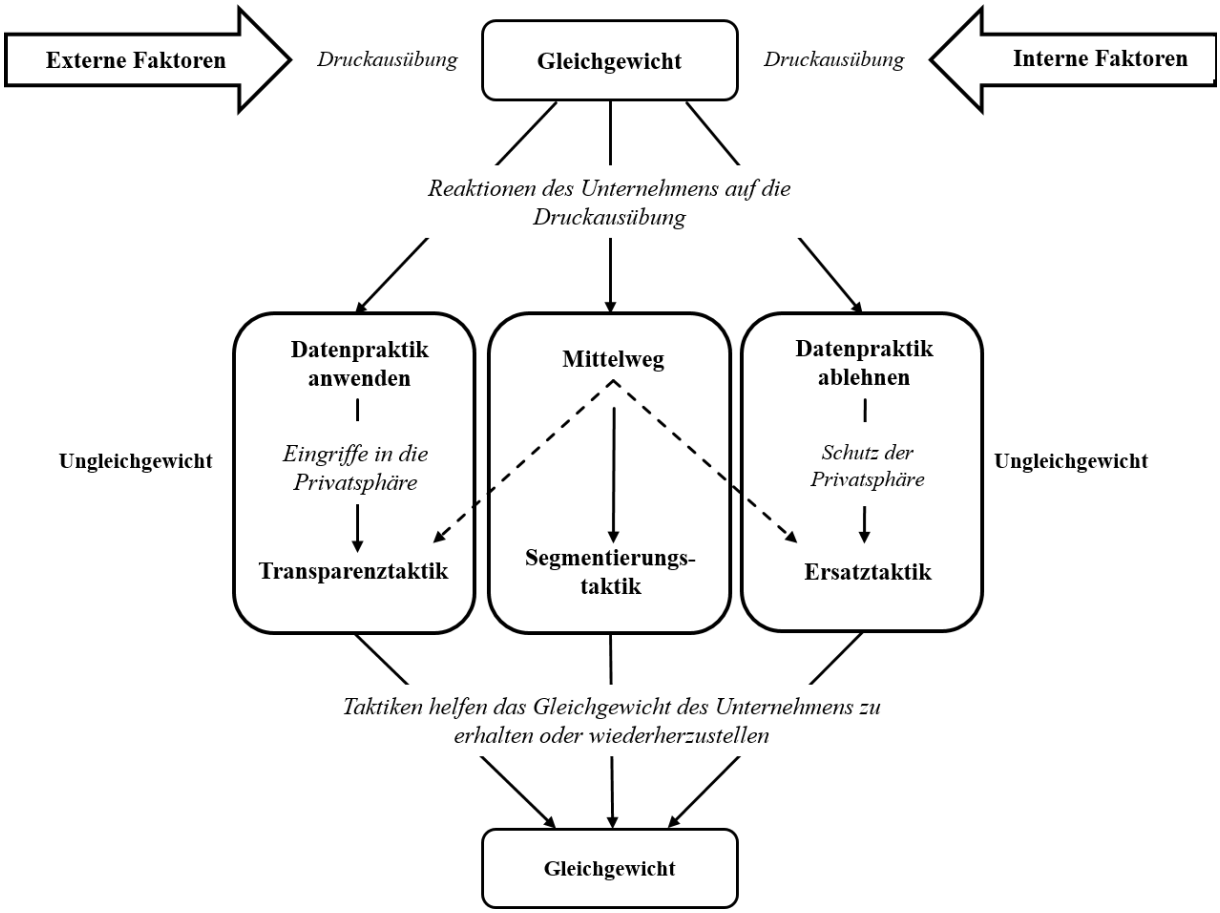


Abbildung 2: Prozessbeschreibung der Aufrechterhaltung des Gleichgewichts in dynamischen Kontexten

Gleichgewichtsstörender Druck und die Notwendigkeit, das Gleichgewicht zu halten

In dynamischen Umgebungen, wie denen von Unternehmen, sind dauerhafte Gleichgewichtszustände schwer zu schaffen und zu erhalten, da Ereignisse und das Ausüben von Druck diese Zustände stören und zu Ungleichgewichten führen können (Cardinal et al. 2004; Gregory et al. 2013; Raisch et al. 2009). Die in den Interviews beschriebenen Gleichgewichtszustände werden dabei oft durch Entscheidungen über die Erhebung oder Verwendung von Nutzerdaten gestört, die durch externe oder interne Druckausübungen auf das Unternehmen ausgelöst wurden. In diesem Zusammenhang konnten verschiedene kontextuelle Faktoren identifiziert werden, die einen ausgleichsstörenden Druck ausüben und die Entscheidungen der Unternehmen über bestimmte Datenpraktiken beeinflussen. Da eine vollständige Darstellung des Wirkmechanismus der Faktoren den Rahmen der vorliegenden Arbeit sprengen würde, wird nur ein kurzer Überblick über die Faktoren gegeben, die sich durch die Daten offenbart haben.

Diese Faktoren können in zwei übergeordnete Kategorien eingeteilt werden: Eine Kategorie fasst dabei die Faktoren **außerhalb** des Unternehmens zusammen und die andere, die mit den **internen** Faktoren des Unternehmens und seinen Aktivitäten selbst zusammenhängen. Da der Forschungsschwerpunkt der vorliegenden Studie auf andere Fragestellungen gelegt wurde, wird kein Anspruch auf Vollständigkeit der Faktoren erhoben und zudem muss nicht jeder Faktor in jedem Kontext relevant sein. Sie bieten allerdings großes Potenzial für zukünftige Untersuchungen, bei denen die vorliegende Auflistung der Online-Services als Ausgangspunkt dienen kann.

Zum einen konnten Faktoren identifiziert werden, die innerhalb eines Unternehmens oder seiner Dienstleistung liegen und die eine bestimmte Datenpraktik erforderlich machen, wie beispielsweise die Ziele eines Unternehmens, seine verfügbaren Ressourcen, der Geschäftswert einer Datenpraktik, die Sensibilität der beteiligten Informationen und die Nutzererfahrung des Dienstes. Im Hinblick auf die Ziele der Unternehmen hatten einige Anbieter beispielsweise eine klare Priorisierung zum Aufbau einer starken Nutzerbasis vorgenommen, während der Aufwand für die Datenerfassung auf ein Minimum reduziert wurde. Ein Interviewter fasste die Notwendigkeit zur Verfolgung der aktuellen Ziele wie folgt zusammen (S#05): „*Also da muss man, glaube ich, immer abwägen, in welcher Situation ist das Unternehmen und was ist gerade das Ziel."* Weiterhin schränken die verfügbaren Ressourcen der Unternehmen oft die Machbarkeit bestimmter Praktiken ein, sodass sie sich gegen ihre Umsetzung entscheiden müssen (S#01): *„Das trifft halt einfach eher die Priorisierung. Wir haben halt sehr knappe Ressourcen hier und können natürlich nicht alles gleichzeitig machen."* Darüber hinaus spielt der Geschäftswert, der sich aus der Erhebung oder Verwendung eines bestimmten Datenelements ergibt, eine zentrale Rolle bei den Entscheidungen der Unternehmen ob sie bestimmte Praktiken anwenden. Ein Befragter aus einem Unternehmen, das eine mobile Nachrichten-App anbietet, reflektiert die Entscheidung des Unternehmens gegen das Sammeln der E-Mail-Adressen seiner Nutzer wie folgt (S#01): „*Und dann haben wir uns erstmal überlegt, vielleicht ist das gar nicht so wichtig diese E-Mail-Adresse überhaupt zu haben, sondern wichtig ist überhaupt erstmal, dass die Leute auf uns aufmerksam werden und das System ausprobieren können."* Darüber hinaus müssen Unternehmen auch die Sensibilität der betreffenden Informationen berücksichtigen, wenn sie Entscheidungen über bestimmte Praktiken treffen. Ein E-Commerce-Unternehmen klassifizierte beispielswiese manche Daten in bestimmten Produktkategorien als sensibler im Vergleich zu anderen und verzichtete daher darauf, personalisierte Angebote einschließlich dieser Daten an die Nutzer zu senden (S#10): *„Deswegen machen wir natürlich bei den*

Kategorien oder bei den Produktkategorien durchaus Unterschiede und senden nicht zu jedem Produkt was [personalisierte Angebote] raus." Schließlich kann das Sammeln oder Verwenden von Nutzerdaten auch die Benutzerfreundlichkeit eines Dienstes beeinträchtigen; ein weiterer Faktor, der bei den Überlegungen der Unternehmen eine Rolle spielt. Das folgende Zitat unterstreicht, dass die Sammlung von Daten für die Nutzer irgendwann ärgerlich werden kann, was zu höheren Abbruchquoten führt (S#17): *„Dann, was noch wichtig ist, die Usability, beziehungsweise ob es dann hohe Abbruchraten an der Stelle gibt, wenn man irgendwelche Daten abfragt. Also, wenn man Daten abfragt und die Benutzer sagen „das ist jetzt schon die fünfte Seite, die ich jetzt mit Formularfeldern voll hab“ oder wenn Benutzer das Gefühl haben, diese Daten sind eigentlich gar nicht das Minimum das man braucht für die Bedienung dieser Funktion."*

Neben internen Faktoren konnten auch Faktoren identifiziert werden, die außerhalb der Unternehmen liegen und diese einem Druck aussetzen, der zu gleichgewichts-störenden Entscheidungen führen kann: externe Bedrohungen, Wettbewerb, das rechtliche Umfeld des Unternehmens und die Präferenzen seiner Nutzer. So können beispielsweise externe Bedrohungen wie das Risiko von Cyberangriffen beeinflussen, ob ein Datenelement erfasst wird. Ein Unternehmen in der Gesundheitsbranche hat sich aus diesem Grund beispielsweise gegen die Erfassung identifizierbarer Nutzerdaten entschieden (S#07): *„Das war auch so die initiale Überlegung, weil wir eben mit Angriffen auf Hackerseite Probleme bekommen könnten. (...) Bei uns war da, denke ich, eine Abwägung aus was kann uns passieren, was können wir daraus für einen Nutzen ziehen. Und [wir] haben uns darauf dann eben entschieden, ja, wir anonymisieren die Daten. Wir ziehen nur so viel, wie wir unbedingt brauchen um diese Analysen zu ermöglichen.“*

Einige Unternehmen sahen es auch als notwendig an, mit den Wettbewerbern gleichzuziehen und neue Wege zur Gewinnung und Nutzung von Nutzerdaten zu gehen. Ein Interviewter gab beispielsweise an (S#12): *„Es heißt überall im Netz höher, weiter, schneller, besser sein. Die Konkurrenz schläft ja nun auch nicht und es wird ja auch tendenziell immer mehr Konkurrenz im Internet. Und insofern versucht man neue Möglichkeiten zu erschließen und da ist man natürlich schon regelmäßig mal am meeten und schaut, "Wo habe ich noch neue Möglichkeiten?““.*

Darüber hinaus kann auch das rechtliche Umfeld eines Unternehmens bestimmte Praktiken fördern oder einschränken. Kurz vor dem Interview mit einem Anbieter einer Finanzdienstleistung ist ein neues Gesetz zur Geldwäsche in Kraft getreten, und in Folge

dessen forderte ein starker Bankpartner des Serviceanbieters, dass dieser, zusätzliche Informationen über seine Nutzer erheben sollte. Das folgende Zitat veranschaulicht, wie dies das Gleichgewicht, welches das Unternehmen zu erhalten versuchte, gestört hat (S#17): *„Und das ist etwas aus der Balance geraten, also wir haben das umgesetzt, weil wir diesen wirtschaftlichen oder auch rechtlichen Druck von der Bank hatten sozusagen, aber wir stehen da in sehr engem Kontakt über den Lenkungsausschuss und versuchen darauf hinzuwirken, dass wir diese Daten wieder loswerden, um da wieder ein Gleichgewicht herzustellen."*

Schließlich können auch Präferenzen der Nutzer hinsichtlich ihrer Privatsphäre und Informationsnutzung heterogen sein und somit die Unternehmen bei ihren Entscheidungen beeinflussen. Wie das folgende Zitat zeigt, erforderte ein heterogener Kundenstamm, dass das Unternehmen differenzierte Ansätze in Bezug auf Datenerhebung und -nutzung in Betracht zieht (S#22): *„Das ist die Hälfte [der Nutzer], die das sehr kritisch sehen und oft sehr, da dann auch sogar drauf aggressiv Feedback gaben, und es gibt aber auch Leute, eben, so 30%, die sagen, "Ich kann mir das gut vorstellen und wir würden das [den persönlichen Service] auch nutzen."“*

Insgesamt übten alle diese Faktoren auf die Unternehmen Druck aus, da sie Entscheidungen in Bezug auf die Daten und Privatsphäre von Nutzern erfordern, die das Gleichgewicht der Unternehmen stören können und sie vor die Herausforderung stellen, mit den Nachteilen der Entscheidung für oder gegen die Erhebung oder Nutzung von Daten umzugehen. In solchen turbulenten und sich ständig verändernden Kontexten ist es immer wieder notwendig auszubalancieren und Aktionen auf die Kernziele auszurichten (Gregory et al. 2013). Die Akteure versuchen daher, das Gleichgewicht durch ein Ausbalancieren wiederherzustellen und zu erhalten, was zu Sequenzen aus Gleichgewichts- und Ungleichgewichts-Zuständen führen kann (Cardinal et al. 2004; Kreiner et al. 2006). Um das Gleichgewicht wiederherzustellen oder aufrecht zu erhalten, haben die interviewten Unternehmen verschiedene Taktiken angewandt, um die negativen Auswirkungen ihrer Entscheidungen und Praktiken abzumildern. Es konnten dabei drei Kategorien von Taktiken identifiziert werden: **Ersatztaktiken**, **Transparenztaktiken** und **Segmentierungstaktiken**. Diese entsprechen den drei möglichen Entscheidungen über die Erfassung und/oder Nutzung von Nutzerdaten: die Datenpraktik kann übernommen oder abgelehnt werden oder es kann ein Mittelweg einschlagen werden. Im Folgenden werden die Taktik-Kategorien genauer vorgestellt. Im Anhang 4 können zusätzliche Zitate für jede Taktik eingesehen werden.

Ersatztaktiken zum Ausgleich vernachlässigter Informationsbedarfe

Um den negativen Folgen der Ablehnung einer Datenpraktik, also der Vernachlässigung des unternehmensbezogenen Informationsbedarfs entgegenzuwirken, tendieren einige Unternehmen dazu, zwei Taktiken zu verwenden, die unter dem Begriff der Ersatztaktiken zusammengefasst werden können. Bei der Entscheidung gegen die Erhebung oder Verwendung personenbezogener Daten zielt die Ersatztaktik darauf ab, den potenziellen Nutzen, den die Unternehmen aufgeben würden, zu kompensieren. Durch die Datenanalyse konnten zwei verschiedene Formen der Ersatztaktik identifiziert werden: **die Verwendung verfügbarer Daten** und **die Suche nach einer weniger aufdringlichen Alternative**.

Wenn das Unternehmen eine Praktik ablehnt, die darauf abzielte, bestimmte Erkenntnisse über die Nutzer zu gewinnen, versuchen einige Unternehmen dieses Ziel dennoch zu erreichen, indem sie sich auf Daten stützen, die ihnen bereits zur Verfügung stehen und somit keine Erhebung neuer Daten erfordern. Die verfügbaren Daten können dabei Elemente umfassen, die von den Unternehmen bereits erhoben wurden, zu denen die Nutzer ihre Erlaubnis zur Verwendung schon früher abgegeben haben, oder die mit technischen Mitteln erfasst werden können, ohne dass der Nutzer seine explizite Zustimmung abgeben muss. So können beispielsweise Daten, die von den Webbrowsern der Nutzer übertragen werden, helfen, das Angebot trotz fehlender, spezifischer Daten zu personalisieren (S#13): *„Was schon relevant ist, ist zum Beispiel zu überlegen, nutzt der [Benutzer] Internet Explorer 7 oder nutzt er Chrome in der neuesten Version. Denn auf Basis dessen, können wir dann natürlich wieder Korrelationen bilden bzw. diese Information nutzen, um zum Beispiel zu vermuten wie alt du bist. Und letztendlich sind alle Informationen relevant, die statistisch valide sind.“*

Die zweite Taktik dieser Kategorie besteht darin, alternative Daten zu finden, die in Bezug auf die Privatsphäre der Nutzer weniger einschneidend sind. In bestimmten Kontexten können Unternehmen ihre Ziele auch mit anderen Mitteln erreichen, ohne zusätzliche Nutzerdaten zu erheben, oder sehr sensible Daten zu verwenden. Der Vertreter eines E-Commerce-Dienstes beschrieb beispielsweise wie der Mangel an Nutzerdaten zur Erstellung personalisierter Newsletter durch eine Idee kompensiert werden konnte und so eine Alternative gefunden wurde, die nicht auf personenbezogene Daten angewiesen ist (S#12): *„Wenn ich natürlich die Info habe, "Was ist deine Lieblingsfarbe", dann kann ich meinen Newsletter entsprechend auf diesen Farben aufbauen. Dann bekommt die eine Gruppe blau primär. Die andere bekommt primär einen grünen Newsletter. Aber warum? Da muss man sich halt vorher ein bisschen*

besser hinsetzen und sagen, "Ok, wie bekomme ich es hin, einen zu machen, der alle anspricht". Und da liegt dann die Kür.“

Unternehmen tendieren also zu Ersatztaktiken, wenn sie sich gegen eine bestimmte Praktik entscheiden und die Privatsphäre ihrer Nutzer schützen wollen. Es bedarf dann einer gewissen Kreativität, um die ursprünglichen Ziele zu erreichen und die organisatorischen Informationsbedarfe zu erfüllen.

Transparenztaktiken zur Vermeidung von Nutzer- oder Imageverlusten

In den Fällen, in denen sich Unternehmen für eine bestimmte Praktik entscheiden, die die Erfassung oder Verwendung von Kundendaten beinhaltet, müssen sie sich irgendwie mit den negativen Folgen der Verletzung der Privatsphäre ihrer Nutzer, beispielsweise in Form von Nutzer- oder Imageverlusten, auseinandersetzen. Die Datenanalyse hat dabei ergeben, dass Unternehmen den Grad der Transparenz, mit dem sie die von ihnen durchgeführten Aktivitäten kommunizieren, variieren. Insbesondere variiert das Ausmaß, mit dem Unternehmen das „was“, „wie“ und „warum“ ihrer Aktivitäten mit Nutzerdaten kommunizieren. Diese Transparenztaktiken können zwei verschiedene Formen annehmen: **Vermeidung von Überbetonung** (weniger Transparenz) und **Erklärung** (mehr Transparenz).

Manchmal entschieden sich Unternehmen für bestimmte Datenpraktiken, betonen diese aber nicht so stark. So gehen einige der befragten Unternehmen beispielsweise davon aus, dass Internetnutzer bereits an eine bestimmte Art der Nutzung oder Erfassung ihrer Daten gewöhnt sind, da diese Praktik auch bei anderen Unternehmen weit verbreitet ist. Darüber hinaus sind die Unternehmen oft der Meinung, dass bestimmte Aktivitäten nichts sind, woran ihre Nutzer von sich aus denken. In diesen Fällen haben sich einige Unternehmen dazu entschieden, eine Überbetonung dieser Aktivitäten zu vermeiden, um nicht unnötig auf sie aufmerksam zu machen. So berichtete ein Anbieter eines Nachrichtenportals im Interview beispielsweise, wie er eine Korrektur in der Betonung einer Aktivität vorgenommen hat (S#22): *„Es gibt den Disclaimer, den man üblicherweise drin hat in den AGBs, zu Datenschutz und so. Und den haben wir einmal sehr, sehr prominent platziert. Dann haben sich wirklich sehr viele Leute das auch durchgelesen und die haben dann Angst da drin gehabt und so weiter und so fort und haben dann eher das deinstalliert. (...) Und dann haben wir den runtergenommen einfach. Also der User, der das sucht, natürlich weiterhin findet, aber das man das nicht den Leuten auch wirklich nicht nochmal unter die Nase hält.“* Auf diese Weise versuchte das

Unternehmen, die Nutzer davon abzuhalten darüber nachzudenken, wie die Daten von dem Unternehmen verwendet, und welche Informationen gesammelt werden.

In anderen Fällen hatten sich Unternehmen bewusst für eine bestimmte Datenpraktik entschieden, die die Aufmerksamkeit ihrer Nutzer auf sich zieht. Dies können Aktivitäten sein, die eher ungewöhnlich sind, die sehr sensible Daten betreffen oder von Natur aus sichtbar sind, wie beispielsweise Formularfelder, die Informationen auf einer Webseite anfordern. Infolgedessen müssen die Unternehmen verhindern, dass Nutzer von dem betroffenen Service abwandern, weil sie ein Risiko für ihre Privatsphäre sehen. Es zeigte sich dabei, dass Unternehmen versuchen, Informationsasymmetrien zu ihren Gunsten zu reduzieren, indem sie das „was“, „warum“ und „wie“ ihres Umgangs mit Nutzerdaten klar kommunizieren. Ein Beispiel dafür ist das folgende Zitat eines Finanzservice-Anbieters, dessen Unternehmen durch gesetzliche Anforderungen zusätzliche Daten erheben muss, und dies seinen Nutzern gegenüber offen kommuniziert (S#17): *„Wir informieren unsere Benutzer, dass wir diese Daten jetzt zusätzlich abfragen müssen, auch unsere Bestandskunden, und sagen ihnen, dass das aus rechtlicher Sicht so ist und nicht, dass wir jetzt einfach mehr Daten haben wollen, um die wirtschaftlich auszuwerten.“* Dabei hoffen einige Unternehmen, dass die Nutzer zu keinen falschen Schlussfolgerungen kommen.

Die bisher vorgestellten Taktiken scheinen bei klaren Entscheidungen für oder gegen eine bestimmte Praktik geeignet zu sein. Wie allerdings bereits erwähnt, verzichteten Unternehmen oft auf solche binären Entscheidungen, da die Präferenzen ihrer potenziellen Nutzer unterschiedlich sein können.

Der Mittelweg: Segmentierungstaktiken

Aufgrund individueller Unterschiede zwischen den Nutzern war es oft keine selbstverständliche Entscheidung auf die Erhebung oder Nutzung von Informationen zu verzichten oder nicht, da die Unternehmen Angst hatten, dass sie auf Möglichkeiten verzichten würden, mit ihrer Konkurrenz Schritt zu halten oder attraktive Dienstleistungen anzubieten. So wie die Festlegung eines Einheitspreises für ein Produkt oder eine Dienstleistung einen möglichen Überschuss aufgrund unterschiedlicher Zahlungsbereitschaft ungenutzt lassen kann, könnte ein einheitlicher Ansatz für die Datenpraktiken von Unternehmen auch zu suboptimalen Ergebnissen führen. Infolgedessen konnten bei der Datenanalyse Unternehmen beobachtet werden, die Taktiken anwenden, die darauf abzielen, dieses Problem anzugehen. Insbesondere versuchen einige Anbieter von Online-Diensten, ihre Nutzer im Hinblick auf individuelle Präferenzen zum Datenschutz zu segmentieren.

Insgesamt wurden drei verschiedene Arten von Segmentierungstaktiken identifiziert: **freiwillige Beiträge**, **funktionale Versionierung** und **Diskriminierung ohne Selbstauswahl**.

Die Taktik der freiwilligen Beiträge scheint dabei die einfachste Form zu sein. Die Nutzer wurden hierbei vor die Wahl gestellt, ob sie auf freiwilliger Basis und je nach Präferenz bestimmte Daten zur Verfügung stellen oder einer bestimmten Praktik zustimmen. Der Anbieter eines Kundenbindungsdienstes beschrieb den Versuch, detailliertere Informationen für Nutzerprofile zu erhalten, wie folgt (S#13:) *„Wir fragen den User im Onboarding auch noch, ob er [Online-]Shops hat, die er relevant findet. (…) Dann wissen wir natürlich, dass er eine bestimmte Art von Shop mag. Natürlich auch nicht unrelevant, aber das ist jetzt nichts, was für den Sign-Up erforderlich ist, wiederum. Das ist ein optionaler Schritt.“* In ähnlicher Weise bieten andere Unternehmen ihren Nutzern die Möglichkeit Newsletter zu erhalten oder ein Konto für die Nutzung eines Dienstes zu erstellen.

Die Taktik der funktionalen Versionierung folgt einer ähnlichen Logik. Sie motiviert die Nutzer dazu, zusätzliche Informationen bereitzustellen oder zusätzlichen Verwendungszwecken zuzustimmen, wodurch der Service mehr Funktionalität bietet. Analog zu Premium-Versionen von Softwareprodukten, wird den Nutzern die Möglichkeit geboten, mehr von ihren Daten zu geben, um im Gegenzug zusätzliche Funktionen zu erhalten. Der Anbieter eines Nachrichtenportals erklärte dies wie im Folgenden dargelegt (S#01): *„Also er muss nicht persönliche Daten angeben um die App zu nutzen. Natürlich hat er einen Vorteil dabei, wenn er die angegeben hat. Also wir bauen da momentan diverse Features, die es dem Nutzer schmackhaft machen sollen sich anzumelden mit E-Mailadresse, weil natürlich E-Mail ist ein Vorteil für uns, weil wir direkt mit den Leuten kommunizieren können.“*

Schließlich planen weiterhin einige Anbieter ihre Nutzer auf der Grundlage eigener Analysen zu segmentieren und verfolgen daher die Taktik der Diskriminierung ohne Selbstauswahl. Dabei versuchen einige Unternehmen, individuelle Unterschiede zwischen ihren Nutzern auf Grundlage eigener Einschätzungen vorherzusagen. Infolgedessen sprechen bestimmte Praktiken nur jene Teilmenge von Nutzern an, die als offen für solche Aktivitäten eingeschätzt werden. Basierend auf diesen Beobachtungen, erfordert diese Taktik präzise statistische Analysen, um zu aussagekräftigen Kundensegmenten zu gelangen. Ein Befragter erklärte diesen Mechanismus wie folgt (S#14): *„Also wir sind auch da natürlich dran [unsere Kunden] zu segmentieren. Und eigentlich genau zu schauen, welche Nutzer sind eigentlich die, die scheinbar einen Vorteil daraus ziehen, die auch mit uns interagieren, die die E-Mails*

[Newsletter] öffnen. Und ich sag mal, heute gibt es verschiedene Testgruppen und es gibt quasi die Möglichkeit null und eins. Aber es ist auf jeden Fall auch das Zukunftsszenario quasi sehr viel stärker zu messen und zu schauen, welche Nutzer scheinen daraus einen Vorteil zu ziehen und welche nicht. Und dann natürlich auch nur die zu bespielen, die auch einen Vorteil daraus haben.“

Die drei Segmentierungstaktiken können von Vorteil sein, wenn ein *One-size-fits-all*-Ansatz Vorteile ungenutzt lässt. Interessanterweise zeigten die Interviews allerdings auch, dass manche Unternehmen ihre Segmentierungstaktik durch den gleichzeitigen Einsatz von Ersatz- oder Transparenztaktiken ergänzen. So könnte beispielsweise die Taktik der freiwilligen Beiträge durch die Transparenztaktik mit Erklärungen ergänzt werden, um die Nutzer zu ermutigen, ihre Daten freiwillig anzugeben.

3.5 Diskussion der Ergebnisse

Die vorliegende Studie stellt eine Theorie vor, die erklärt, wie Unternehmen die konkurrierenden Anforderungen, bestehend aus ihrem Informationsbedarf einerseits und ihrem Bedürfnis Nutzer zu gewinnen und zu binden, andererseits, ausgleichen. Die Theorie kann nach der Klassifizierung von Gregor (2006, S. 624) als "Typ-II“-Theorie bezeichnet werden, die darauf abzielt aufzuzeigen, wie die Welt in einer bestimmten Weise wahrgenommen werden kann. Dies stellt ein gültiges Ergebnis für *Grounded Theory* Studien in der Wirtschaftsinformatik-Forschung dar (Seidel und Urquhart 2013). Im Folgenden wird die erarbeitete Theorie in die bestehende Forschung integriert, sodass der theoretische Beitrag ersichtlich wird. Anschließend wird auf den praktischen Beitrag eingegangen und Limitationen sowie zukünftige Forschungsmöglichkeiten werden aufgezeigt.

3.5.1 Integration in bestehende Forschung und theoretischer Beitrag

Auf höchster Ebene leistet die vorliegende Studie einen theoretischen Beitrag, indem sie erklärt, wie Unternehmen die konkurrierenden Anforderungen bezüglich der Daten und Privatsphäre ihrer Nutzer erleben und handhaben; ein Thema, bei dem trotz der Fülle und Relevanz bestehender Privatsphäre-Forschung, noch kein ausreichendes Verständnis erreicht werden konnte (Bélanger und Crossler 2011). So fördert die Studie ein "*understanding of how things are or why they are as they are*" (Gregor 2006, S. 624). In diesem Sinne wurden die Herausforderungen der Unternehmen untersucht und der Umgang mit Nutzerdaten und Privatsphäre als neuer, wichtiger Kontext aufgedeckt, in dem unternehmensbezogene Ambidextrie erforderlich ist. Daher erweitert die Studie auch die bisherige Ambidextrie-

Forschung (z.B. Andriopoulos und Lewis 2009; Gibson und Birkinshaw 2004; Gregory et al. 2015). Diese übergeordnete Erkenntnis unterstreicht, dass eine rein nutzerorientierte Perspektive auf Privatsphäre eine nur unvollständige Grundlage für die Abgabe von Empfehlungen für die Unternehmenspraxis ist (Bélanger und Crossler 2011). Stattdessen muss die Privatsphäre-Forschung berücksichtigen, dass aus Unternehmenssicht Ambidextrie erforderlich ist, um den Herausforderungen rund um die Daten und Privatsphäre der Nutzer zu begegnen.

Die Studie konzeptualisiert den Begriff der Ambidextrie beim Umgang von Unternehmen mit Nutzerdaten und der Privatsphäre der Nutzer und bietet daher spezifische Konzepte, die die zukünftige Forschung beeinflussen können. Wie Ambidextrie-Studien in anderen Kontexten, die mit einer übergreifenden Herausforderung begonnen haben (z.B. Andriopoulos und Lewis 2009; Smith und Tushman 2005), trägt auch diese Studie zu einem besseren Verständnis über das untersuchte Thema bei, indem vier Spannungen identifiziert wurden, die die Bedingungen definieren, unter denen Unternehmen beim Umgang mit Nutzerdaten agieren müssen: 1) Datensammlung gegen Nutzergewinnung, 2) Zeitrahmen der Sammlung, 3) Image-bezogene Kosten der Nutzerdaten und 4) Verlust von Nutzern durch Datennutzung. Die Spannungen können als Rahmen für zukünftige Unternehmensbezogene Forschung dienen, die darauf abzielt, die Herausforderungen der Unternehmen zu untersuchen, die im Umgang mit Nutzerdaten und Privatsphäre entstehen. Diese Spannungen liefern dabei nützliche Informationen darüber, „was“ ausgewogen sein muss, um Ambidextrie im Rahmen von Privatsphäre zu erreichen. Die Spannungen beziehen sich auf die bestehende Privatsphäre-Theorie, gehen aber auch darüber hinaus. So bietet die Theorie des bereits im Kapitel 2.2 beschriebenen Privatsphäre-Kalküls, beispielsweise eine Begründung dafür, warum diese Spannungen bestehen. Schließlich können Nutzer, wenn sie die Vorteile und Risiken der Offenlegung von Daten vor Verwendung eines Dienstes abwägen, aufgrund erhöhter Risikowahrnehmung abgeschreckt werden, wenn sie einer zusätzlichen Datenerhebung oder -nutzung zustimmen müssen (z.B. Choi et al. 2018; Kehr et al. 2015; Kordzadeh und Warren 2017; Ozdemir et al. 2017). Aufgrund der nutzerorientierten Perspektive berücksichtigt diese Theorie jedoch nicht den eigenen Informationsbedarf der Unternehmen und vernachlässigt daher die daraus resultierenden Spannungen für Unternehmen, die ihren Nutzern Dienstleistungen anbieten.

Bisherige unternehmensorientierte Privatsphäre-Forschung hat zu Untersuchungen über die Strategien aufgerufen, die Unternehmen anwenden, um mit den Privatsphäre-

Herausforderungen umzugehen (Chan und Greenaway 2005). Dieser Forschungsaufruf wird mit der vorliegenden Studie adressiert, indem die Gleichgewichts-Perspektive eingeführt wird. Die Schaffung eines Gleichgewichts hat sich bereits in anderen Kontexten wie Kontrolle, Lernen und Leistung als wichtige Unternehmensaktivität erwiesen (z.B. Auh und Menguc 2005; Eisenhardt et al. 2010; Gregory et al. 2013). Die vorliegende Studie erweitert die Ergebnisse dieser Forschung auf den Kontext der Verwaltung von Nutzerdaten und Privatsphäre und gibt Einblicke in die verschiedenen Taktiken, die die Unternehmen einsetzen um dem entgegenzuwirken. Dabei konnten drei Kategorien von Taktiken und mehrere Ausprägungen für jede dieser Kategorien identifiziert werden. Die Beobachtungen deuten darauf hin, dass diese Taktiken von den Anbietern angewandt wurden, um mit den negativen Auswirkungen ihrer Entscheidungen über die Erhebung und Verwendung von Nutzerdaten umzugehen. Die identifizierten Taktiken können als Grundlage für weitere Forschung über unternehmensbezogene Datenschutzpraktiken dienen.

Eine der identifizierten Ersatztaktiken, bei der bereits verfügbare Daten genutzt werden, deutet darauf hin, dass Unternehmen eine Form von *Bricolage* betreiben - die Fähigkeit bei Ressourcenengpässen alles zu nutzen, was zur Verfügung steht (Baker und Nelson 2005). Darüber hinaus konnten Transparenztaktiken entdeckt werden, die helfen können, mit den nachteiligen Folgen der Erfassung und Nutzung von Nutzerdaten umzugehen. Obwohl der Begriff der Transparenz bereits in früheren Studien diskutiert wurde (z.B. Awad und Krishnan 2006; Venkatesh et al. 2016), ist die Forschung über die Strategien der Unternehmen in Bezug auf die Transparenz begrenzt und Erweiterungen wurden in der Literatur bereits gefordert (Granados und Gupta 2013). Die Erkenntnisse dieser Studie über die Transparenztaktiken, gehen auf diese Forderung ein und erklären, warum Unternehmen nicht immer das höchstmögliche Transparenz-Level verfolgen sollten, wie dies in bisheriger Forschung vorgeschlagen wird (Krasnova et al. 2010; Malhotra et al. 2004). Tatsächlich konnte diese Studie zeigen, dass Unternehmen versuchen, die Transparenz in einigen Fällen zu verringern, indem sie eine Überbetonung bestimmter Praktiken vermeiden - eine Strategie der Verheimlichung von Informationen, wie sie bereits von Granados und Gupta (2013) vorgeschlagen wurde. Segmentierungstaktiken helfen Unternehmen dabei, die Heterogenität der Präferenzen ihrer Nutzer anzugehen, wie bereits von der nutzerorientierten Privatsphäre-Forschung vorgeschlagen (z.B. Ozdemir et al. 2017; Smith et al. 2011). Interessanterweise ähneln diese Segmentierungstaktiken der so genannten traditionellen Preisdiskriminierung für Produkte und digitale Dienstleistungen (z.B. Lehmann und Buxmann 2009; Shapiro et al. 1998). Schließlich generieren die Anbieter von Online-Diensten, wie bereits in dieser Arbeit

beschrieben, oft Einnahmen, indem sie Nutzerdaten monetarisieren und ihre Dienstleistungen nicht gegen Geld, sondern gegen Privatsphäre handeln (Steinfeld 2015). Die in dieser Studie vorgestellten Beobachtungen zu den Segmentierungstaktiken integrieren sich daher in die traditionelle Literatur zur Preisdiskriminierung.

3.5.2 Praktikscher Beitrag

Die gewonnenen Erkenntnisse können Anbietern von Online-Diensten helfen, Entscheidungen über den Umgang mit Nutzerdaten zu treffen. Die Ambidextrie-Theorie legt nahe, dass Unternehmen bei konkurrierenden Anforderungen nach einem Gleichgewicht zwischen den gegensätzlichen Kräften streben sollten, da dies mit überlegener Leistung und langfristiger Wettbewerbsfähigkeit verbunden ist (Gibson und Birkinshaw 2004; March 1991; Raisch und Birkinshaw 2008). In dem vorliegenden Kontext bedeutet dies, dass Unternehmen die Forderungen ihrer Nutzer nach Privatsphäre - wie sie durch die bisherige Privatsphäre-Literatur gefordert wird - nicht vernachlässigen sollten, zeitgleich sollten sie aber auch ihren eigenen Informationsbedarf, der mit einem gewissen Grad an Privatsphäre-Einschnitten einhergeht, nicht außer Acht lassen, wenn sie wettbewerbsfähig bleiben wollen. Wenn Entscheidungen bezüglich einer Aktivität den Gleichgewichtszustand eines Unternehmens stören, sollten Wege gefunden werden, dieses Gleichgewicht wiederherzustellen. Die Spannungen und Taktiken, die in dieser Forschung identifiziert wurden, können in dieser Hinsicht hilfreich sein.

Die in dieser Studie identifizierten Spannungen können der Diskussion der Unternehmen über die Herausforderungen, denen sie in Bezug auf ihre Datenpraktiken gegenüberstehen, mehr Struktur verleihen. Wenn es beispielsweise um die Einführung einer neuen Praktik, wie die Erfassung zusätzlicher Nutzerdaten oder einer zusätzlichen Verwendung bereits vorhandener Daten geht, können Anbieter anhand der identifizierten Spannungen die mit diesen Praktiken verbundenen Nachteile diskutieren. Ebenso können sowohl Start-ups als auch etablierte Unternehmen, die planen, neue Online-Dienste anzubieten, bei der Erstellung und Bewertung ihrer Businesspläne von Anfang an auf das Wissen über diese Spannungen zurückgreifen. Auf diese Weise können sie mögliche Herausforderungen bei der Erfassung und Nutzung von Nutzerdaten im Vorfeld erkennen und vorausplanen.

Wenn das Gleichgewicht eines Unternehmens gefährdet oder bereits gestört ist, können die identifizierten Taktiken dem Unternehmen helfen, das Gleichgewicht zu erhalten oder wiederherzustellen. Die Ablehnung einer Praktik kann dazu führen, dass Anbieter einen

unerfüllten Bedarf an Informationen haben, was wiederum einen Nachteil für diese Unternehmen in Bezug auf die Optimierung ihres Geschäfts, ihrer Marketingeffektivität, ihres Kundenservice usw. darstellt. Alternativ können Unternehmen deshalb nach Ersatztaktiken suchen, um den Nachteilen ihrer Entscheidung zu begegnen. So können beispielsweise Unternehmen, die bereits Daten über ihre Nutzer besitzen, diese wieder aufgreifen und versuchen, auf Grundlage dieser verfügbaren Daten Erkenntnisse zu gewinnen, anstatt zusätzliche Informationen explizit abzufragen. Auf der anderen Seite kann die Einführung einer neuen Datenpraktik Unternehmen vor das Risiko stellen, Nutzer zu verlieren oder ihr Image aufgrund von Datenschutzbedenken ihrer Nutzer zu schädigen. Transparenztaktiken können helfen, diesen Herausforderungen zu begegnen, indem sie entweder Praktiken, die für ihre Nutzer weniger ersichtlich sind, nicht überbetonen oder indem sie ihre Praktiken detailliert erklären und begründen. Ein Beispiel für die Anwendung einer Taktik zur Erhöhung der Transparenz ist die Ankündigung von Facebook, 2018 erstmals seine Datenschutzgrundsätze zu veröffentlichen, um mehr Details über den Umgang des Unternehmens mit personenbezogenen Daten preis zu geben (CNBC 2018). Schließlich können Unternehmen auch Segmentierungstaktiken nutzen, wenn sie mit heterogenen Nutzerpräferenzen, wie sie bereits im 2. Kapitel angesprochen wurden, konfrontiert sind. Ein Beispiel dafür sind Unterschiede in der Einstellung zur personalisierten Werbung. Während eine Gruppe von Nutzern eine positive Einstellung zu Benachrichtigungen über relevante Produkte oder Dienstleistungen haben könnte, könnte eine andere Gruppe besorgt sein, dass Unternehmen ihre Präferenzen verfolgen und analysieren.

Zum Abschluss der praktischen Implikationen, soll noch ein Wort der Vorsicht in Bezug auf den Einsatz von Taktiken im Allgemeinen und besonders von Transparenztaktiken sowie zu langfristigen Ungleichgewichtszuständen gegeben werden: Da der Fokus dieser Studie auf der Erforschung des „Was ist?“ und nicht des „Was ist das Beste?“ gelegt wurde, kann keine Einschätzung zur langfristigen Wirksamkeit der hier vorgestellten Taktiken abgeben werden. Des Weiteren könnte aus den Ergebnissen dieser Studie interpretiert werden, dass Unternehmen Privatsphäre-intrusive Praktiken vor ihren Nutzern verbergen könnten. Von solchen Methoden distanziert sich diese Studie jedoch klar. Die Ergebnisse sollen vielmehr dazu dienen, Unternehmen zu helfen, Erkenntnisse darüber zu entwickeln, wann sie von der Erklärung einer Datenpraktik profitieren können, weil die Praktik von den Nutzern erwartet oder toleriert wird und wann sie Nutzer abschrecken könnten. Nutzern zu schädigen ist jedoch niemals ratsam, und es gibt andere Wege die helfen Informationsasymmetrien zu reduzieren und dadurch Datenpraktiken transparent zu machen. Ein aktuelles Beispiel ist die Fitness-App

Runkeeper, die die Bewegungsdaten ihrer Nutzer an ein fremdes Werbenetzwerk übermittelt, selbst wenn die App inaktiv ist. Dieses Beispiel zeigt, wie schnell Massenmedien schädliche Praktiken offenlegen können (DigitalTrends 2016; Fortune 2016). Zu guter Letzt, lag der Fokus dieser Studie, wie bereits erwähnt, nicht auf den möglichen Folgen langfristiger Ungleichgewichtszustände. Deshalb muss beachtet werden, dass ein ignorierter Ungleichgewichtszustand über einen längeren Zeitraum erhebliche negative Folgen für ein Unternehmen und seine Kunden haben kann, die nicht sofort eintreten.

3.5.3 Limitationen und weiterer Forschungsbedarf

Wie alle Studien, hat auch diese ihre Limitationen, wodurch sich weitere Möglichkeiten für zukünftige Forschung ergeben. Erstens basiert diese explorative Studie auf Eigenberichten der Interviewten, was immer mit dem Risiko sozial erwünschter Antworten einhergeht. Weiterhin basiert die Studie auf einer Stichprobe, deren Unternehmen aus dem persönlichen und beruflichen Netzwerk der Autoren ausgewählt wurden. Einerseits bringt dies den Vorteil, dass ein gewisses Maß an Vertrauen im Interview besteht, was vor allem bei sensiblen Themen wie Nutzerdaten und Privatsphäre günstig sein kann. Dies kann auch dazu beigetragen haben, das Problem der sozialen Erwünschtheit der Antworten bis zu einem gewissen Grad zu verhindern oder zu reduzieren. Andererseits hätte eine repräsentativere Stichprobe zusätzliche Aspekte aufdecken können, die in dieser Forschung so nicht berücksichtigt wurden. Trotz der persönlichen Auswahl des Samples, besteht die Stichprobe dennoch aus heterogenen Quellen, mit mehreren etablierten Unternehmen mit langjähriger Erfahrung, sowie kleineren Start-ups in unterschiedlichen Reifegraden. Auch die Nutzerzahlen der Unternehmen in der Stichprobe variieren und umfassen teilweise bis zu 19 Millionen Nutzer pro Monat.

Eine zweite Limitation kann darin gesehen werden, dass die Theorie keine möglichen Unterschiede in der Relevanz der vier Spannungen für verschiedene Unternehmen erklärt. Es erscheint wahrscheinlich, dass die Relevanz jeder Spannung für ein Unternehmen vom Kontext desselben abhängt und es konnte auch beobachtet werden, dass die Wahrnehmung des Gleichgewichts zwischen den Unternehmen variieren kann. Was von einem Unternehmen als ausgeglichener Zustand betrachtet wird, könnte von einer anderen Firma als Ungleichgewicht wahrgenommen werden. Zukünftige, groß angelegte, quantitative Studien sind angesichts des begrenzten Stichprobenumfangs dieser qualitativen Studie besser geeignet, diese Probleme zu lösen. Solche Studien können Unternehmens- und Dienstleistungsmerkmale strukturierter und quantitativer bewerten und potenzielle Cluster von Unternehmen identifizieren, die sich darin ähneln, wie die verschiedenen Spannungen

abgewogen werden und wo das optimale Gleichgewicht liegt. Solche Cluster oder Unternehmenskategorien wiederum könnten zukünftigen Studien dienlich sein, indem sie Unterschiede in den Aktivitäten, Strategien und Erfolgen von Unternehmen erklären.

Die vorliegende Forschung stellt nur einen kleinen Schritt bei der Untersuchung der unternehmensbezogenen Herausforderungen im Umgang mit Nutzerdaten und Privatsphäre dar. Angesichts der Wichtigkeit des Themas und der mangelnden Privatsphäre-Forschung aus Unternehmenssicht sind weitere Studien erforderlich, für welche die in dieser Studie vorgestellten Ergebnisse eine Grundlage darstellen. So bleiben diese Ergebnisse beispielsweise auf einem relativ abstrakten Niveau und identifizieren lediglich den Gesamtmechanismus und die Konzepte, die sich auf die Gleichgewichtsschaffung von Unternehmen rund um ihre Informationsbedarfe und die Privatsphäre beziehen. Detaillierte Fallstudien könnten unterschiedliche Unternehmen vergleichen, um die Bedingungen für ihre Gleichgewichtswahrnehmung näher zu ergründen. Wie in früheren Forschungen, die organisatorische Spannungen untersucht haben, könnte die Ambidextrie-Theorie in zukünftigen Studien ebenfalls als theoretische Grundlage dienen (Adler et al. 1999; Andriopoulos und Lewis 2009).

Darüber hinaus kann die Identifizierung des Spannungsfeldes zwischen dem Sammeln und Verwenden von Nutzerdaten auf der einen Seite und der Aufrechterhaltung des Unternehmensimages auf der anderen Seite zukünftige Forschung, die Determinanten auf das Unternehmens- oder Markenimage untersuchen, bereichern. Schließlich deutet die vorliegende Studie darauf hin, dass der Umgang eines Unternehmens mit Nutzerdaten berücksichtigt werden sollte, da er das Image beeinflussen könnte. Die *Brand Equity Theory* könnte dabei verwendet werden, um das Image zu konzeptionieren und Einblicke in potenzielle Determinanten zu geben (Dawar und Pillutla 2000; Keller 1993).

Zukünftige Studien könnten sich weiterhin dem großen Forschungspotenzial annehmen, dass sich aus den identifizierten Kontextfaktoren ergibt, die Druck ausüben und die Entscheidungen der Unternehmen über die Erhebung und Nutzung von Nutzerdaten beeinflussen. Die identifizierten Faktoren könnten beispielsweise in Studien verwendet werden, die ein besseres Verständnis dafür suchen, warum und wie Entscheidungen für oder gegen bestimmte Datenpraktiken getroffen werden und wie sich diese Faktoren auf die Gleichgewichtswahrnehmung und das Niveau der Ambidextrie auswirken. Dabei könnten Theorien der organisatorischen Entscheidungsfindung als theoretische Grundlage dienen (Eisenhardt 1989; Nutt 1998).

Die vorliegende Arbeit eröffnet also einige weitere Forschungsmöglichkeiten zur Untersuchung des Umgangs von Unternehmen mit personenbezogenen Nutzerdaten, die den Beitrag dieser Arbeit ergänzen können. Im weiteren Verlauf der Arbeit werden die bislang gewonnenen Erkenntnisse zur Bedeutung von Privatsphäre aus organisationaler Perspektive durch Untersuchungen der Nutzerperspektive erweitert.

4 Eine strukturierte Literaturrecherche zum Wert von Daten aus Nutzerperspektive[4]

Nachdem im vorausgegangenen Kapitel die Unternehmensperspektive auf personenbezogene Nutzerdaten und Privatsphäre untersucht und dabei aufgezeigt wurde, wie schwer es Unternehmen fällt das Gleichgewicht zwischen der Notwendigkeit zur Verwendung dieser Daten und der Notwendigkeit des Privatsphäre-Schutzes herzustellen und zu halten, wird in dem 4. Kapitel der vorliegenden Arbeit die Nutzerperspektive auf Daten und Privatsphäre analysiert. Dabei wird der monetäre Wert, den Nutzern ihren Daten zuweisen näher untersucht, indem die bisherigen Studien zu diesem Thema in einer strukturierten Literaturrecherche zusammengefasst und miteinander verglichen werden.

4.1 Motivation und Relevanz

"There is a saying that if you get something for free, you should know that you're the product. It was never more true than in the case of Facebook and Gmail and YouTube. You get free social-media services, and you get free funny cat videos. In exchange, you give up the most valuable asset you have, which is your personal data."

Yuval Noah Harari (Time 2017)

Wie bereits in dem Zitat von Yuval Harari thematisiert, besteht mittlerweile wohl Einigkeit darüber, dass Unternehmen, insbesondere Onlinedienstleister wie Google oder Facebook, die Privatsphäre ihrer Nutzer in Form von deren personenbezogenen Daten monetarisieren (Steinfeld 2015). Schließlich geben Individuen nach dem Prinzip, dass sie das „Produkt" für die Anbieter von Services sind, ihre Daten preis, um dafür im Gegenzug bestimmte Vorteile, wie die Nutzung des Dienstes (Chellappa und Sin 2005) oder finanzielle Belohnungen (Hann et al. 2002), zu erhalten. Ob die Individuen sich dabei tatsächlich für eine Preisgabe ihrer Daten entscheiden, hängt von dem bereits vorgestellten Privatsphäre-Kalkül ab, also der Abwägung zwischen den Risiken der Datenaufgabe sowie den Vorteilen, die durch die Datennutzung entstehen können (Dinev und Hart 2006). Personenbezogene Daten werden

[4] Die in diesem Kapitel vorgestellte strukturierte Literaturrecherche basiert auf Wagner et al. (2018).

demnach nur preisgegeben, wenn der Nutzen, der mit der Offenlegung der Daten einhergeht, höher als die wahrgenommenen Risiken ist (Rust et al. 2002; Xu et al. 2011).

Um fundierte Abwägungsentscheidungen treffen zu können, ist es daher für die Individuen wichtig, den Wert ihrer Daten besser einschätzen zu können. Auch für die Unternehmen sind die Erkenntnisse, welchen Wert Individuen ihren personenbezogenen Daten zuweisen wesentlich, um die Dienste entsprechend gestalten und erbringen zu können. Schließlich hat das vorausgegangene 3. Kapitel bereits gezeigt, wie schwer der Umgang mit personenbezogenen Nutzerdaten für Unternehmen ist. Die Wertermittlung personenbezogener Daten und damit der Privatsphäre aus Nutzerperspektive ist jedoch nicht trivial, sondern in der Regel ist es für Individuen schwer einzuschätzen und zudem im Allgemeinen subjektiv (Grossklags und Acquisti 2007). Darüber hinaus verfügen Individuen nur über unvollständige Informationen darüber, wie ihre personenbezogenen Daten von Unternehmen verwendet werden (Acquisti et al. 2009), was die Bewertung zusätzlich erschwert.

Um die Wertermittlung operationalisieren zu können, stützen sich bisherige Forschungsarbeiten auf Umfragen (z.B. Rose 2005) oder Experimente (z.B. Steinfeld 2015), um die Bereitschaft der Individuen zur Preis- beziehungsweise Weitergabe der personenbezogenen Daten an Dritte zu messen (Hann et al. 2007; Krasnova et al. 2009; Tsai et al. 2011). Konkret untersuchen die Studien, welche Determinanten Individuen in ihrer Bewertung der Privatsphäre beeinflussen und in welchen Werten diese resultieren, indem sie entweder die Zahlungsbereitschaft der Individuen für einen erhöhten Schutz der Daten oder ihre Verkaufsbereitschaft für Daten messen (Grossklags und Acquisti 2007). Daher wird der Wert von Privatsphäre im Folgenden dieser Arbeit mit dem Wert von personenbezogenen Daten gleichgesetzt.

Die Zahlungsbereitschaft für einen erhöhten Datenschutz, englisch *willingness-to-pay (WTP) for privacy*, untersucht dabei inwiefern Individuen bereit sind, eine Gebühr für privatsphärenfördernde Funktionalitäten zu zahlen. Es kann also als eine Art Datenschutzprämie (engl. *privacy premium*) verstanden werden, die typischerweise von Unternehmen als *Freemium*-Produkt angeboten wird. Demnach stellen Unternehmen ihre Basisprodukte kostenlos zur Verfügung und bieten darüber hinaus kostenpflichtige Zusatzleistungen an (Schreiner und Hess 2015), welche die Privatsphäre der Nutzer besser schützen als es vom Basisprodukt her vorgesehen ist.

Im Gegensatz dazu steht die Bereitschaft der Individuen ihre personenbezogenen Daten gegen eine monetäre Vergütung zu verkaufen (Acquisti et al. 2009). Der Begriff leitet sich dabei aus

dem englischen *willingness-to-sell (WTS) personal data* beziehungsweise dem als Synonym zu verwendenden *willingness-to-accept (WTA) privacy invasion* ab (Grossklags und Acquisti 2007). Dieser Ansatz untersucht also, wie Individuen auf wirtschaftliche Anreize reagieren, wenn sie darüber entscheiden, ob sie ihre personenbezogenen Daten an Unternehmen weitergeben sollen (Grossklags und Acquisti 2007).

Die Ergebnisse bisheriger Studien zur Untersuchung der Zahlungs- und Verkaufsbereitschaft fallen dabei sehr unterschiedlich aus, und teilweise sogar widersprüchlich: So zeigten manche Resultate beispielsweise, dass die Befragten sehr datenschutzbewusst sind und ihre Daten daher sehr hoch bewerteten (z.B. Barak et al. 2013; Huberman et al. 2005), während andere Studien zu dem Ergebnis kamen, dass die Teilnehmer ihre Privatsphäre überhaupt nicht wertschätzten (z.B. Bauer et al. 2012; Grossklags und Acquisti 2007). Selbst für den gleichen Datentyp sind die Ergebnisse teilweise sehr unterschiedlich. Huberman et al. (2005) zeigten zum Beispiel, dass die Studienteilnehmer ihre Gewichtsinformationen für durchschnittlich 74,06 US-Dollar verkaufen würden, während die Studie von Grossklags und Acquisti (2007) zu einem Preis von 31,80 US-Dollar für die gleiche Art von Informationen führte. Weiterhin wurden mit einer anderen Messmethode von dem gleichen Sample sogar Angebote von 25 Cent für Gewichtsinformationen angenommen (Grossklags und Acquisti 2007). Darüber hinaus zeigten Schreiner und Hess (2015), dass Facebook-Nutzer durchschnittlich 0,63 Euro für eine Premium-Version des sozialen Netzwerkes zahlen würden, während die Studie von Krasnova et al. (2009) zu einer monatlichen Gebühr von 1,20 Euro beziehungsweise 1,40 Euro für soziale Netzwerke führte.

Da die Ergebnisse bisheriger Forschung so verstreut sind, ist es wichtig, die Unterschiede zwischen den Studien zu untersuchen, um Einblicke in die Wertvorstellungen von Nutzern bezüglich ihrer Privatsphäre zu erhalten und zu verstehen, wie diese beeinflusst werden. Darüber hinaus fehlt bisher ein systematischer Ansatz zur umfassenden Beschreibung des aktuellen Forschungsstandes, obwohl dieser für ein umfassendes Verständnis der Bewertung der Privatsphäre aus Nutzerperspektive wichtig ist. Weiterhin können sich Unternehmen bei der Erbringung von Dienstleistungen, welche die Privatsphäre-Belange ihrer Kunden betreffen, nur teilweise auf bisherige Forschungserkenntnisse verlassen. Um dieses praktische und theoretische Problem zu lösen, wurde die hier vorliegende strukturierte Literaturrecherche durchgeführt. Ziel ist es einen narrativen, theoretischen Überblick und Vergleich der bisherigen Literatur zu bieten. Dabei wird die folgende Untersuchungsfrage beantwortet:

Was beeinflusst den monetären Wert, den Individuen ihren personenbezogenen Informationen beimessen und wie können die bestehenden Ansätze und Ergebnisse einheitlich konzeptualisiert werden?

Auf Basis etablierter Methoden der strukturierten Literaturrecherche (Vom Brocke et al. 2009; Webster und Watson 2002), die im nächsten Abschnitt genauer vorgestellt werden, wurden 37 empirische Studien, die in verschiedenen Journalen, Konferenzbeiträgen und Workshops veröffentlicht wurden, analysiert und zusammengefasst. Dabei wurden sowohl die Messmethoden, als auch die Faktoren, die einen Einfluss auf die Bewertung der Daten haben, kodiert. Die Ergebnisse sind in den Kapiteln 4.3.1 und 4.3.2 detaillierter beschrieben. Zusätzlich werden diese in tabellarischer Form (siehe Anhang 5) sowie in einem integrativen, theoretischen Framework (siehe Abbildung 4) zusammengefasst, durch welche die zugrundeliegenden Unterschiede sichtbar werden (Baumeister und Leary 1997). Neben den Einflussfaktoren werden auch exemplarisch Ergebnisse der Zahlungsbereitschaft für einen erhöhten Datenschutz sowie für die Bereitschaft Daten zu verkaufen als die beiden Facetten, durch die der Wert von Daten gemessen werden kann, detaillierter vorgestellt (Kapitel 4.3.3). Aus Gründen der Vereinfachung, werden diese Facetten im weiteren Verlauf der Arbeit mit Zahlungs- und Verkaufsbereitschaft abgekürzt und auf den Zusatz des Daten- und Privatsphäre-Kontextes verzichtet. Das Ende dieses Kapitels bildet die Diskussion der wichtigsten Ergebnisse, in welcher die Limitationen zusammengefasst und ein Ausblick auf mögliche zukünftige Forschungsrichtungen gegeben wird.

4.2 Methodik der strukturierten Literaturrecherche

Das vorliegende Unterkapitel gibt einen Überblick über die verwendete Literaturrecherche-Methodik, welche auf den Ansätzen von Webster und Watson (2002) sowie Vom Brocke et al. (2009) basiert. Dazu werden, dem Aufruf nach mehr Transparenz von Vom Brocke et al. (2009) folgend, zunächst der Suchstring sowie die Ein- und Ausschlusskriterien vorgestellt, bevor auf den Suchprozess mit seinen Datenquellen eingegangen wird.

Zur Identifikation der relevanten Suchbegriffe wurde zunächst eine Pilotrecherche auf Basis der in bekannten Artikeln zur Bewertung von Daten vorkommenden Stichwörter (engl. *Keywords*) durchgeführt (z.B. Carrascal et al. 2013; Hann et al. 2007; Huberman et al. 2005; Tsai et al. 2011). Die darin verwendeten Stichwörter dienten als Ausgangspunkt für den initialen Suchstring, der iterativ weiterentwickelt wurde. Da der Suchstring entscheidend zur Identifikation der relevanten Literatur ist, wurden möglichst präzise Ausdrücke der Begriffe

gewählt, die das Thema ausreichend detailliert beschreiben (Vom Brocke et al. 2009). In Anbetracht der Vielfalt der Suchbegriffe, die den Term „Wert personenbezogener Daten“ beschreiben können, wurde dieser Ausdruck in seine Hauptkomponenten zerteilt und jeweils nach Synonymen sowie verwandten Ausdrücken gesucht. Letztlich bestand der finale Suchstring aus vier Teilen. Der erste Teil umfasst Synonyme für "Wert", da dies der Hauptansatz der Studie ist. Dazu wurden eine Reihe von Suchbegriffen verwendet, die von "Ökonomie", " Bewertung" und "Wert" bis hin zu Begriffen reichen, die Preisansätze beschreiben. Natürlich wurde auch der Begriff "Bereitschaft" in den Suchstring miteinbezogen, da dies die Hauptkomponente für die Zahlungs- und Verkaufsbereitschaft ist. Der zweite Teil besteht aus verschiedenen Ausdrücken für "personenbezogen", während der dritte Teil die Synonyme "Information" und "Daten" beinhaltet. Der letzte Teil des finalen Suchstrings begrenzt das zu untersuchende Thema auf Studien mit einem Zusammenhang zu „online“, da die Pilotrecherche ergeben hat, dass das Thema erst mit dem Aufkommen von E-Commerce und sozialen Netzwerken Gegenstand wissenschaftlicher Studien geworden ist. Die Suchanfrage wurde in englischer Sprache durchgeführt, weswegen sich insgesamt der folgende Suchstring ergibt:

(("economics" OR "worth" OR valu* OR willingness-to* OR "freemium" OR "pricing") AND ("privacy" OR "personal" OR "private") AND ("data" OR "information") AND ("online"))

Um sicherzustellen, dass nur geeignete und relevante Publikationen in die Analyse einbezogen werden und dass die Auswahl der Literatur immer nach dem gleichen Schema verläuft, wurden Ein- und Ausschlusskriterien festgelegt (Webster und Watson 2002). Die Einschlusskriterien wurden wie folgt definiert:

1. Der Wert von Daten beziehungsweise von personenbezogenen Daten steht im Mittelpunkt der Untersuchung.
2. Die einbezogenen Studien sollten empirisch und auf individueller Nutzerebene durchgeführt worden sein.
3. In den Studien wird die Bereitschaft der Individuen zum Verkauf ihrer personenbezogenen Daten und/oder ihre Bereitschaft zum Schutz für ihre Daten zu zahlen, untersucht.

Dem gegenüber stehen die Kriterien, die für den Ausschluss von Studien definiert wurden:

1. Es werden keine Studien einbezogen, die sich auf das Thema Privatsphäre und personenbezogene Daten im Allgemeinen fokussieren, ohne den monetären Wert der Daten zu untersuchen.
2. Studien, die sich ausschließlich auf das Testen von Messmethoden zur Bewertung von Privatsphäre konzentrieren, werden ebenso ausgeschlossen.
3. Aufgrund der Konzentration auf den Online-Kontext, wird ebenfalls Forschung, die vor 2000 veröffentlicht wurde, vernachlässigt.

In der nächsten Phase wurden für die Recherche geeignete, wissenschaftliche Datenbanken ausgewählt, die potenziell relevante Publikationen enthalten konnten (Webster und Watson 2002). Insgesamt wurde die strukturierte Literatursuche in den folgenden Datenbanken durchgeführt: *ACM Digital Library*, *AIS Electronic Library*, *EBSCOhost Business Source Premier*, *ScienceDirect*, *SpringerLink* und *WebOfScience*. Die Form des Suchstrings hat dabei aufgrund verschiedener design-technischer Anforderungen zwischen den Datenbanken leicht variiert. Der oben vorgestellte Suchstring wurde in der Form für die *EBSCOhost*-Datenbank verwendet.

Aus Gründen der Vollständigkeit wurden die Publikationen der Datenbanken, ohne weitere Einschränkungen in Bezug auf bestimmte Journale oder Konferenzen, durch Anwendung der Suchanfrage selektiert. Darüber hinaus wurde eine manuelle Suche in den acht führenden Wirtschaftsinformatik-Journalen des sogenannten *Senior Scholars Basket of Journals (European Journal of Information Systems, Information Systems Journal, Information Systems Research, Journal of AIS, Journal of Information Technology, Journal of MIS, Journal of Strategic Information Systems* und *MIS Quarterly)* sowie in der *IEEE*-Publikationsliste durchgeführt, um sicherzustellen, dass keine wichtigen Forschungsbeiträge im Wirtschaftsinformatik-Bereich vernachlässigt wurden. Schließlich konnten so 1169 Publikationen (ohne Duplikate) in den benannten Datenbanken identifiziert werden, die zur besseren Handhabung in eine *Citavi*-Datenbank hochgeladen wurden. Im nächsten Schritt wurden die Titel und Abstracts dieser Publikationen anhand der bereits vorgestellten Auswahlkriterien gescannt, wodurch der Stichprobenumfang auf 114 reduziert wurde. Durch die darauffolgende Analyse der Volltexte, konnten schließlich 17 relevante Studien selektiert werden. Wie von Webster und Watson (2002) vorgeschlagen, wurde von dieser Studienmenge ausgehend, eine Vorwärts- und Rückwärtssuche ausgeführt. Der Prozess der Rückwärtssuche bezieht sich dabei auf die Analyse von Publikationen, die wiederum in den

bereits ausgewählten Veröffentlichungen zitiert wurden. Dem gegenüber zielt die Vorwärtssuche darauf ab, Publikationen zu identifizieren, welche die bereits als relevant erkannten Veröffentlichungen zitieren (Webster und Watson 2002). Diese Suche konnte mit den entsprechenden Funktionen in Google Scholar durchgeführt werden. Auch die durch die Vorwärts- und Rückwärtssuche gefundenen Publikationen wurden mit dem zuvor beschriebenen Verfahren des Titel- und Abstract-Screenings sowie nachfolgender Volltextanalysen weiter untersucht. Letztendlich konnten so 37 Veröffentlichungen, die zwischen 2002 und 2017 publiziert wurden, als das relevante Literaturset identifiziert werden. Dieses bildet die Grundlage für weitere Analysen, die im Folgenden detaillierter vorgestellt werden. Abbildung 3 fasst den Suchprozess mit seinen einzelnen Phasen und der daraus resultierenden Anzahl an Studien nochmals zusammen.

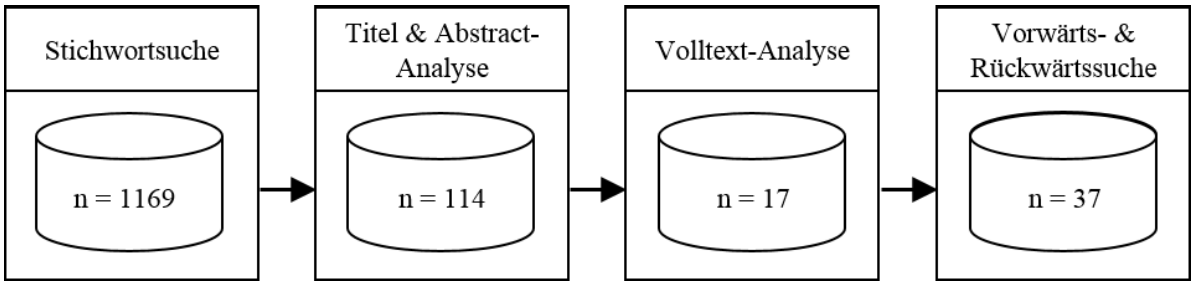


Abbildung 3: Zusammenfassung des Suchprozesses und der Anzahl der Studien am Ende jeder Phase

4.3 Wert von Daten und seine Einflussfaktoren

Nach der Identifikation der relevanten Literatur wurden die selektierten Publikationen ihren Forschungsansätzen entsprechend kodiert und die Ergebnisse in einer Tabelle zusammengefasst. Diese ist dem Anhang 5 dieser Arbeit beigefügt. Zur weitergehenden Analyse der Ergebnisse der Literaturrecherche, wurden, wie von Baumeister und Leary (1997) vorgeschlagen, die Forschungsansätze der identifizierten Studien in einem integrativen theoretischen Framework zusammengefasst (Baumeister und Leary 1997; Webster und Watson 2002). Dieses ist in Abbildung 4 dargestellt.

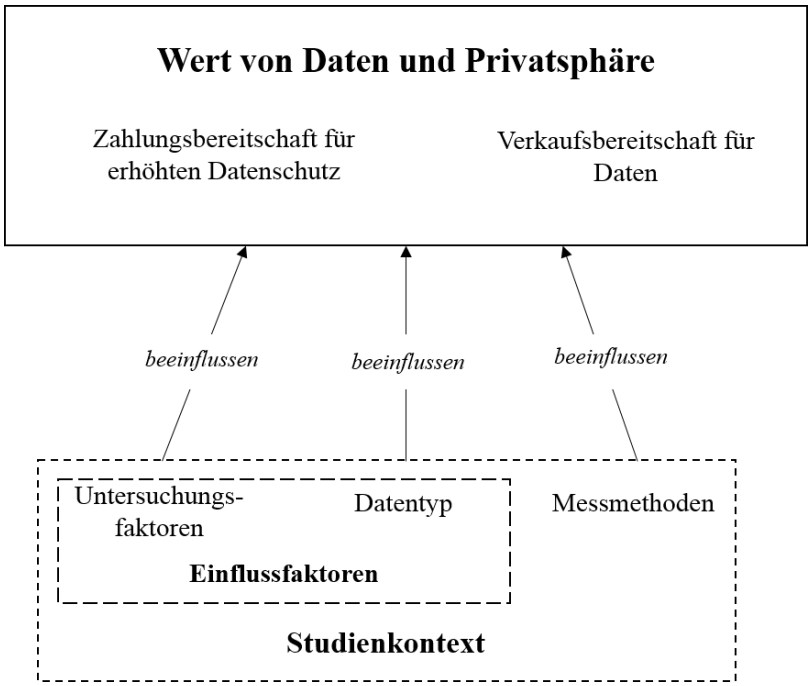


Abbildung 4: Integratives, theoretisches Framework zur Erhebung des Wertes von Daten

In Übereinstimmung mit der bisherigen Privatsphäre-Literatur (z.B. Brandimarte und Acquisti 2012) wurde der Kontext der Studien als sehr relevant für die Bewertung der Privatsphäre der Nutzer identifiziert. Schließlich wurde auch schon im Kapitel 2.2 auf die verschiedenen Kontextfacetten eingegangen und die Wichtigkeit von Kontext für die Spezifizierung und Konzeptualisierung von Privatsphäre betont. In den Studien zur Untersuchung des Wertes von Daten, zeigte sich, dass die Kontexte, in denen frühere Studien durchgeführt wurden, sehr heterogen sind. So untersuchten Acquisti et al. (2009) zum Beispiel die Bereitschaft von Einkaufszentren-Besuchern, Informationen über ihre Einkäufe preiszugeben, indem diese zwischen Geschenkkarten mit unterschiedlichen Geldwerten wählen konnten. Weiterhin erhoben Carrascal et al. (2013) beispielsweise Browserverlaufsdaten von Internetnutzern, die diese dann im Rahmen einer Auktion verkaufen konnten, während in der Auktion von Jentzsch (2014) die Teilnehmer ihre Quizresultate verkaufen konnten, die im Verkaufsfall vor den anderen Auktionsteilnehmern preisgegeben wurden. Diese Beispiele veranschaulichen, wie unterschiedlich die Forschungszusammenhänge in früheren Studien sind.

Durch die strukturierte Literaturrecherche konnten sieben verschiedene Kategorien von Faktoren identifiziert werden, die in Form ihrer Ausprägungen die Wertermittlung beeinflussen können. Dazu zählen beispielsweise die Art der Informationen, aber auch weitere Untersuchungsfaktoren wie Verzerrungen oder auch personenbezogene Faktoren. Weiterhin konnte auch die Messmethode, die von Auktionen, Labor- und Feldexperimenten bis hin zu offenen oder geschlossenen Fragen in Umfragen reichen (z.B. Acquisti et al. 2009;

Barak et al. 2013; Benndorf und Normann 2014; Brush et al. 2010), als relevanter Faktor identifiziert werden. Wie Benndorf und Normann (2014) zeigen, hat die Messmethode einen nicht trivialen Einfluss auf den Wert, den Nutzer ihren personenbezogenen Daten zuweisen. In ihrer Studie verwendeten sie zwei verschiedene Messmethoden, um eine Bewertung von sozialen Netzwerk-Informationen zu ermitteln, die zu Ergebnissen führten, die bis zu 10 Euro variierten. Im Folgenden werden die Einflussfaktoren, die aus den Untersuchungsfaktoren und dem Datentyp gebildet werden, sowie die Messmethoden detaillierter vorgestellt.

4.3.1 Einflussfaktoren

Zunächst einmal konnte der **Datentyp**, also die Art von Information, die in den Studien verkauft oder geschützt werden soll, als ein Faktor identifiziert werden, der relevant für die Bewertung von Daten ist. Mit Ausnahme von Rose (2005) ermittelten alle Publikationen den Wert, den Individuen ihrer Privatsphäre zuweisen, indem Anfragen zur Bewertung bestimmter Arten von Informationen durchgeführt wurden. Die Arten der von den Studienteilnehmern bewerteten Daten reichte von Profilinformationen sozialer Netzwerke (zehn Veröffentlichungen) über Informationen über das Browserverhalten auf Webseiten (sieben Veröffentlichungen), Kaufinformationen (sieben Veröffentlichungen), Standortdaten (acht Veröffentlichungen), Smartphone-Daten (fünf Veröffentlichungen), Resultaten von Intelligenztests oder Quizzen (zwei Veröffentlichungen), Alters- und Gewichtsinformationen (zwei Veröffentlichungen) bis zu allgemeinen beziehungsweise soziodemographischen Daten (vier Veröffentlichungen). Die Studien, die soziale Netzwerkinformationen untersucht haben, wurden in der Regel anhand von Facebook durchgeführt, wobei zwischen allen auf Facebook gespeicherten Informationen (Bauer et al. 2012; Spiekermann et al. 2012), der Facebook-Wand oder Profilinformationen (Benndorf und Normann 2014) unterschieden wurde. Weiterhin testeten Studien auch welchen Wert Individuen Informationen über ihr Browserverhalten beimessen, indem beispielsweise die Zahlungsbereitschaft für eine Privatsphäre-freundliche Suchmaschine untersucht wurde (Bughin 2011).

Im Folgenden werden die Untersuchungsfaktoren vorgestellte, die neben dem Datentyp einen Einfluss auf den Wert, den Individuen ihren Daten zuweisen, haben können. Zur besseren Verständlichkeit sind diese in Kategorien unterteilt worden. Abbildung 5 gibt einen Überblick über diese Einflussfaktoren, die auch den Studienkontext bestimmen.

Einflussfaktoren

Datentyp

- Allgemeine Daten
- Alter & Gewicht
- Smartphone-Daten
- Browserdaten
- Standortdaten
- Soziale Netzwerkdaten
- Testresultate (*IQ Scores*)
- Kaufinformationen

Untersuchungsfaktoren

- **Personenbezogen:** Persönlichkeitsmerkmale, Demographische Begebenheiten
- **Wertbezogen:** Monetäre Vergütung, Wertbewusstsein, Zukünftiger Nutzen (z.B. Zeiteinsparung)
- **Privatsphäre:** Privatsphäre-Bedenken, Sensitivität der Daten, Verwendungszweck, Identifizierung, Datenschutzsymbole, Datenschutzerklärung, Art und Dauer der Datenspeicherung, Sekundäre Datennutzung, Fehlerbegrenzung, Unsachgemäßer Zugriff, Daten erhaltene Instanz
- **Verzerrungen:** *Endowment* Effekt, *Order* Effekt
- **Sozial:** Soziale Norm
- **Individuell:** Nutzungsintensität, „Psychologie des Eigentums“, Wahrgenommene Kontrolle, Wahrgenommene Attraktivität

Abbildung 5: Übersicht über die in der Literatur identifizierten Einflussfaktoren auf den Wert von Daten

Neben des Einflusses von verschiedenen Datentypen, wurden die Wertvorstellungen von Privatsphäre auch als sehr sensibel gegenüber nicht-normativen Einflüssen identifiziert (Acquisti et al. 2009). So testeten einige Studien, die auf Verhaltensökonomie aufbauen, inwiefern bestimmte **Verzerrungen** den Wert beeinflussen den, Individuen ihren Daten zuweisen (z.B. Acquisti et al. 2009; Grossklags und Acquisti 2007; Kamleitner et al. 2016). Acquisti et al. (2009) konnten so beispielsweise zeigen, dass auch im Kontext des Wertes von Daten der sogenannte o*rder effect* gilt, wonach die Reihenfolge der einkommenden Angebote für die Daten einen Einfluss auf die Wertvorstellung der Individuen hat. Weiterhin konnte in anderen Studien auch das Wirken des Besitztumseffekts (engl. *endowment effect*) nachgewiesen werden (z.B. Acquisti et al. 2009; Kamleitner et al. 2016) nachdem Individuen ein Gut höher wertschätzen und daher mehr Geld verlangen, wenn sie es aufgeben müssen als

etwas, das sie erst neu erwerben (Thaler 1980). Den Grund für diesen Effekt sieht der Autor in der Wahrnehmung eines Verlustgefühles: *"Furthermore, a certain degree of inertia is introduced into the consumer choice process since goods that are included in the individual's endowment will be more highly valued than those not held in the endowment, ceteris paribus. This follows because removing a good from the endowment creates a loss while adding the same good (to an endowment without it) generates a gain."* (Thaler 1980, S. 44). Im Rahmen der Studien zur Ermittlung des Wertes von Daten äußert sich der hier beschriebene Effekt durch eine tendenziell niedrigere Bereitschaft für den Schutz von Daten zu zahlen im Vergleich zur Bereitschaft diese zu verkaufen (Grossklags und Acquisti 2007). Auf diesen Sachverhalt wird im weiteren Verlauf dieser Arbeit noch genauer eingegangen.

Neben dem Datentyp und den Verhaltensverzerrungen, wurden noch **personenbezogene** Faktoren identifiziert, die einen direkten Einfluss auf die Verkaufs- und Zahlungsbereitschaft der Individuen haben. So untersuchten Staiano et al. (2014) und Christin et al. (2013) beispielsweise den Einfluss von Persönlichkeitsmerkmalen auf die Bereitschaft der Individuen ihre Daten zu verkaufen. Im Rahmen dessen wurde unter anderem untersucht, ob die *Big Five*-Persönlichkeitsmerkmale Extrovertiertheit, Neurotizismus, Aufgeschlossenheit, Gewissenhaftigkeit und Verträglichkeit (Barrick und Mount 1991; Costa und McCrae 2008) einen Einfluss auf die Wertermittlung haben, wobei sich allerdings nur bei der Verträglichkeit signifikante Zusammenhänge zeigten (Staiano et al. 2014). Darüber hinaus kontrollierten einige Studien den Einfluss von demographischen Begebenheiten auf den Wert von Daten. So konnten Cvrcek et al. (2006) in ihrer Auktionsstudie beispielsweise zeigen, dass die Gebote der teilnehmenden Frauen im Vergleich zu denen der männlichen Bieter höher waren. Interessanterweise fanden die meisten anderen Studien jedoch keine signifikanten Unterschiede der Wertangaben hinsichtlich des Alters, Geschlechtes und Einkommens der Befragten (z.B. Carrascal et al. 2013; Egelman et al. 2013; Steinfeld 2015).

Eine weitere Kategorie der Einflussfaktoren bilden die **Privatsphäre**-relevanten Determinanten. Schließlich sind nach Grossklags und Acquisti (2007) Privatsphäre-Präferenzen die bedeutendsten Vorläufer der Verkaufs- und Zahlungsbereitschaft von Individuen. Viele der in das Literatursample eingeflossenen Studien zeigten, dass allgemeine Privatsphäre-Bedenken der Probanden den Wert von Daten deutlich beeinflussen (Brush et al. 2010; Christin et al. 2013; Preibusch 2015; Staiano et al. 2014; Tsai et al. 2011). Dies verdeutlicht auch die Studie von Steinfeld (2015). Der Autor konnte in seiner Stichprobe drei verschiedene Nutzertypen, die *abstainers*, *traders* und *deceivers*, identifizieren und es zeigte

sich, dass die *abstainers* das Angebot, ihr Facebook-Profil gegen Geld zugänglich zu machen, überwiegend wegen hoher Privatsphäre-Bedenken ablehnten. Egelman et al. (2013) klassifizierten die Teilnehmer der Studie wiederum nach Westin‘s Metrik in *Privacy Fundamentalists*, *Privacy Unconcerned* und *Privacy Pragmatists* (Westin und Louis 1991; Westin und Maurici 1998), fanden aber keinen signifikanten Zusammenhang zwischen dem *Westin Privacy Index* und den Auswahlentscheidungen der Teilnehmer hinsichtlich verschiedener Smartphone-Applikationen mit variierenden Datenschutzeinstellungen. Interessanterweise verwendeten auch Nguyen et al. (2016) diese Metrik und beobachteten in ihrer Studie große Unterschiede zwischen diesen Gruppen.

Neben den allgemeinen Privatsphäre-Bedenken untersuchten die Studien verschiedene weitere Vorläufer der Privatsphäre, indem sie gezielte Rahmenbedingungen des Studiensettings anpassten oder Manipulationen vornahmen. Hann et al. (2002) untersuchten so beispielsweise den Einfluss von drei der vier Unterkategorien der Privatsphäre-Bedenken-Dimensionen von Smith et al. (1996) und zwar Fehlerbegrenzung, sekundäre Datennutzung und unsachgemäßer Zugriff. Die sekundäre Datennutzung erwies sich dabei als der einflussreichste Faktor auf die Bewertung der Daten, was auch von Potoglou et al. (2013) und Preibusch (2013) bestätigt wurde. Darüber hinaus führten auch Identifikationen der Studienteilnehmer zu erhöhten Wertvorstellungen (Barak et al. 2013; Carrascal et al. 2013; Preibusch 2015; Regner und Riener 2017), während Verschleierungsverfahren (engl. *obfuscation*) sie verringern konnten (Brush et al. 2010). Darüber hinaus lieferten Egelman et al. (2009) den Nachweis, dass beim Kauf eines Privatsphäre-sensiblen Produkts Individuen eher bereit sind, für einen höheren Datenschutz zu bezahlen. Weiterhin stellten Danezis et al. (2005) und Cvrcek et al. (2006) erhebliche Unterschiede zwischen der Bereitschaft von Individuen, ihre Daten für eine akademische versus kommerzielle Nutzung zu veräußern, fest. In den Studien verdoppelten sich die verlangten Beträge für Daten, wenn diese für kommerzielle statt akademische Zwecke verwendet wurden. Die Studie von Brush et al. (2010) konnte diesbezüglich allerdings keine Unterschiede in ihrer Datenstichprobe finden. In der analysierten Literatur wurden darüber hinaus noch weitere Privatsphäre-relevante Einflussfaktoren identifiziert, die der Abbildung 5 entnommen werden können.

Weiterhin konnten noch andere Kategorien wie die **wertbezogenen** sowie **sozialen** Determinanten und ihre Ausprägungen als relevante Einflussfaktoren identifiziert werden. Spiekermann et al. (2012) zeigten beispielsweise, dass das Wertbewusstsein der Teilnehmer den Wert sozialer Netzwerkinformationen bestimmt. Die Autoren definieren Wertbewusstsein

dabei als die Erkenntniserlangung darüber, etwas Wertvolles zu besitzen, was beispielsweise durch die Kenntnis, dass es einen Markt für das Objekt gibt, ausgelöst werden kann (Spiekermann et al. 2012). Weiterhin konnte gezeigt werden, dass die Höhe der monetären Vergütung einen Einfluss auf die Verkaufsbereitschaft der Befragten hatte (Steinfeld 2015). Das wird auch durch die bereits erwähnte Gruppeneinteilung von Steinfeld (2015) deutlich. Die Gruppe der *trader* war bereit, selbst für eine geringere Menge an angebotenem Geld Zugang zu ihren Facebook-Accounts bereitzustellen, während einige *abstrainers* angaben, dies prinzipiell abzulehnen, es aber für höhere Geldbeträge nochmals in Betracht ziehen würden. Andere Studien erbrachten den Nachweis, dass Individuen ebenfalls eher bereit sind ihre Daten preiszugeben, um im Gegenzug zukünftige Annehmlichkeiten, wie beispielsweise Zeiteinsparungen, zu erhalten (Hann et al. 2007; Hann et al. 2002). Schließlich konnte von Racherla et al. (2011) gezeigt werden, dass auch soziale Normen die Zahlungsbereitschaft für Datenschutz beeinflussen.

Abschließend konnten noch **individuelle** Untersuchungsfaktoren wie die Nutzungsintensität des bereitgestellten Services (Bauer et al. 2012), das Gefühl der Kontrolle (Schreiner und Hess 2015) oder die wahrgenommene Attraktivität von Eigenschaften (Huberman et al. 2005) als einflussreich identifiziert werden. So fanden Huberman et al. (2005) beispielsweise heraus, dass Alters- und Gewichtsinformationen, die als vom Standard abweichend wahrgenommen werden, höher bewertet wurden als „normale“ Angaben. Schließlich konnte noch der Faktor „Psychologie des Eigentums“, also die besitzergreifenden Empfindungen der Individuen hinsichtlich ihrer Daten, als einflussreich auf die Wertermittlung identifiziert werden (Spiekermann et al. 2012).

4.3.2 Messmethoden

Im folgenden Unterkapitel wird ein Überblick über die verschiedenen Methoden gegeben, die in bisherigen Studien zur Messung des monetären Wertes, den Nutzern ihren personenbezogenen Daten zuweisen, genutzt wurden. Die Kategorisierung basiert auf dem Framework für die Zahlungsbereitschafts-Messmethoden von Breidert et al. (2006), das zunächst eine Einteilung in die beiden Hauptkategorien der Experimente und Umfragen vorsieht, die dann weiter in ihre jeweiligen Ausprägungen klassifiziert werden (siehe Abbildung 6). Ein Überblick über diese Methoden mit einer jeweiligen kurzen Beschreibung folgt in den nächsten Abschnitten.

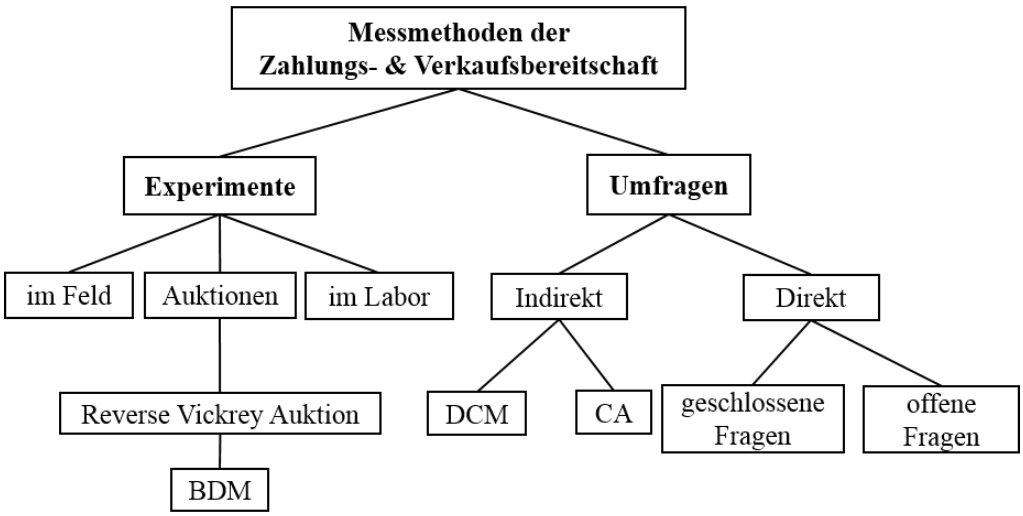


Abbildung 6: Überblick über die Messmethoden der Zahlungs- und Verkaufsbereitschaft für Daten

In der bisherigen Forschung wurden sowohl direkte als auch indirekte Umfragen häufig zur Messung der monetären Bewertung von personenbezogenen Daten verwendet. Besonders direkte Umfragen mit Online-Fragebögen wurden oft entweder mit einfachen offenen Fragen, bei denen die Befragten frei ihre Wertvorstellung in Form eines Schwellenwertes äußern sollten (Racherla et al. 2011), oder mit geschlossenen Fragen, bei der alternative Werte zur Verfügung gestellt wurden, die dann nur akzeptiert oder abgelehnt werden mussten (Barak et al. 2013), verwendet (Grossklags und Acquisti 2007). Eine spezielle Form dieser direkten Umfragen ist die *Contingent Valuation Method* (CVM), die für die Bewertung von Waren oder Dienstleistungen, die noch keinen festen Marktpreis haben, geeignet ist (Spiekermann et al. 2012). Auf Grundlage eines fiktiven Szenarios werden die Teilnehmer entweder aufgefordert, einen bestimmten Wert anzugeben (Spiekermann et al. 2012) oder sie treffen eine diskrete Wahl in Form einfacher Ja/Nein-Antworten für bestimmte Preise (Rose 2005). So wurden die neuseeländischen Studienteilnehmer in der Studie von Rose (2005) beispielweise gefragt, ob sie bereit wären verschiedene Steuererhöhungsbeiträge für strengere Datenschutzgesetze zu zahlen, um so unautorisierte Datenweitergabe oder zweckfremde Datennutzung unterbinden zu können.

Da die meisten direkten Umfragen hypothetischer Natur sind, werden indirekte Umfragen wie Conjoint-Analysen (CA) und die *Discrete Choice Method* (DCM) eingesetzt, um diese Problematik zu reduzieren. Die Conjoint-Analyse basiert auf dem Prinzip, dass der Untersuchungsgegenstand durch mehrere verschiedene Merkmale mit jeweiligen Ausprägungen dargestellt wird (Green und Srinivasan 1978; Pu und Grossklags 2015). Daraus können verschiedene Produktversionen erstellt werden (Pu und Grossklags 2015), zu denen die Befragten durch Auswahl ihrer präferierten Zusammenstellungen Hinweise auf die

relativen Wichtigkeiten der Merkmale ermöglichen (Krasnova et al. 2009). So haben Hann et al. (2002) beispielsweise eine Conjoint-Analyse durchgeführt, um den Trade-off zwischen den Vor- und Nachteilen der Bereitstellung personenbezogener Daten auf Webseiten zu untersuchen. Basierend auf den schon vorgestellten Privatsphäre-Bedenken-Dimensionen von Smith et al. (1996) wurden exemplarische Webseiten als Kombination verschiedener Ausprägungen von unsachgemäßem Zugriff, Fehlerbegrenzung sowie sekundärer Datennutzung, ergänzt durch monetäre Werte und Häufigkeiten des Webseiten-Besuches, dargestellt. Auf die Conjoint-Analyse als Messmethode wird im 6. Kapitel dieser Arbeit noch genauer eingegangen. Ähnlich wie bei der Conjoint-Analyse betrachtet DCM ein Produkt oder einen Service als eine Kombination verschiedener Attribute, wobei dabei im Vergleich zur CA unterschiedliche Schätzmodelle zu Grunde gelegt werden (Breidert et al. 2006). Die Teilnehmer werden gebeten, eine von zwei oder mehreren hypothetischen Alternativen auszuwählen, um den unabhängigen Einfluss der Produktattribute sowie die Bewertung der verschiedenen Attribute zu messen (Krasnova et al. 2014; Potoglou et al. 2013). Ein Typ der DCM ist die *binary choice method*, die von Nguyen et al. (2016) verwendet wurde.

Im Gegensatz zu diesen überwiegend hypothetischen Methoden führten andere Studien zur Ermittlung des Wertes von Daten Feld- oder Laborexperimente mit echtem Realitätsbezug durch, indem sie die Zahlungs- oder Verkaufsbereitschaft als tatsächliches Verhalten entweder lokal in einem Laborumfeld oder einfach von einem zu dem Studiendesign passenden Standort aus gemessen haben (z.B. Acquisti et al. 2009; Beresford et al. 2012; Preibusch et al. 2013). In dem Labor-Experiment von Preibusch (2013) beispielsweise wurde untersucht, wie viel den Teilnehmern ihre Privatsphäre bei der Nutzung einer Suchmaschine wert ist, indem getestet wurde, wie viel Geld sie für verschiedene Privatsphäre-schützende Features, engl. *privacy enhancing technologies* (PETs), zahlen würden.

Allen bisher genannten Methoden ist gemeinsam, dass sie unabhängig von Zeit und Teilnehmerzahl durchgeführt werden können, während bei Auktionen in der Regel mehrere Teilnehmer parallel bieten müssen. In allen acht Publikationen, die eine Auktion durchführen, wurden reverse Vickrey-Auktionen (VA), auch reverse Zweitpreisauktionen (engl. *reverse second price auction*) genannt, angewendet (z.B. Egelman et al. 2009). Die typischen Merkmale dieser Art von Auktionen sind, dass sie mit versiegelten Geboten durchgeführt werden und dass der Bieter mit dem höchsten Gebot gewinnt, aber nur den Preis des zweithöchsten Gebotes zahlen muss (Breidert et al. 2006). Im Falle von Messungen der Verkaufsbereitschaft zeichnet sich diese Art der Auktion dadurch aus, dass der Niedrigstbieter

den Zuschlag erhält und die Möglichkeit bekommt seine personenbezogenen Daten zu verkaufen, aber er erhält den Geldbetrag, der dem zweitniedrigsten Gebot entspricht (Carrascal et al. 2013) oder bei n Geboten das niedrigste Angebot, das nicht ausgewählt wurde (Danezis et al. 2005). Eine spezielle Art von Vickrey-Auktionen, der *Becker-DeGroot-Marshak-Mechanismus* (BDM) (Becker et al. 1964), wird ebenfalls häufig zur Messung der wahren Wertermittlung von Daten eingesetzt und bringt, wie reverse VA, die Teilnehmer dazu, ihre wahre Wertvorstellung zu äußern, da zu hohe oder zu niedrige Gebote nicht erfolgreich sind. Die BDM kann beispielsweise auf den Zahlungsbereitschafts-Kontext angewendet werden, indem den Teilnehmern die Möglichkeit gegeben wird, einen Preis anzugeben, zu dem sie bereit sind, eine bestimmte Ware oder Dienstleistung, zum Beispiel eine datenschutzfreundliche Premium-Version eines sozialen Netzwerkes, zu erwerben (Schreiner und Hess 2015). Wenn dieser Preis niedriger oder gleich einem durch die Experimentatoren zufällig ermittelten Preis ist, kommt der Kauf zum Preis der Zufallsziehung zustande (Schreiner und Hess 2015).

Neben diesen Unterschieden der Messmethoden variierten die durchgeführten Studien auch in den gestalterischen Rahmenbedingungen der Aufgabe, die die Teilnehmer erfüllen mussten. Von allen in die Literaturrecherche eingeflossenen Studien nutzen 20 hypothetische Settings, in denen sich die Teilnehmer bewusst waren, dass sie die Aufgabe ohne reale Auswirkungen für die eigene Person erfüllen können, da sie beispielsweise aufgefordert wurden, sich eine bestimmte Situation vorzustellen (Roeber et al. 2015) oder zwischen verschiedenen hypothetischen Alternativen wählen mussten (Nguyen et al. 2016). Hypothetische Studien reduzieren also die Effekte auf die Studienteilnehmer, da es für sie keine Auswirkungen hat, wenn sie Werte angeben, die nicht ihre wahre Wertvorstellung widerspiegeln (Krasnova et al. 2009; Singleton und Harper 2002). Im Gegensatz dazu gibt es auch einige Studien, die reale Konsequenzen für die Teilnehmer mit sich brachten, beispielweise da sie ihre Daten wirklich verkauften (z.B. Benndorf und Normann 2014; Brush et al. 2010) oder reale Einkäufe tätigen mussten (z.B. Egelman et al. 2009; Tsai et al. 2011). Aber auch in diesen Fällen war den Teilnehmern häufig bewusst, dass sie an einem Experiment teilnehmen, zumal viele Studien in Kontexten durchgeführt wurden, die den Teilnehmern künstlich und unrealistisch erscheinen mussten (z.B. Huberman et al. 2005; Jentzsch 2014).

4.3.3 Studienergebnisse zum Wert von Daten[5]

In dem folgenden Unterkapitel werden einige Studienergebnisse exemplarisch vorgestellt und analysiert. Von den insgesamt 37 in diese Literaturrecherche eingeflossenen Studien, untersuchten mit 21 Publikationen die Mehrheit der Literatur die Zahlungsbereitschaft der Individuen für einen erhöhten Privatsphäre-Schutz. Basierend auf dem schon erwähnten *Endowment*-Effekt, fallen die Werte dieser Studien in der Regel geringer als die der Verkaufsbereitschaft für Daten aus, was auch als *gap between WTA and WTP* bezeichnet wird (Grossklags und Acquisti 2007). Die Neigung von Individuen, mehr Geld für etwas zu verlangen, als sie bereit wären, dafür zu zahlen, ist in der Forschung allgemein bekannt (Horowitz und McConnell 2002) und lässt sich auch auf personenbezogene Daten übertragen (Grossklags und Acquisti 2007).

Einige dieser Studienergebnisse lassen dabei vermuten, dass Individuen ihre personenbezogenen Daten überhaupt nicht wertschätzen. So zeigten die Teilnehmer bezüglich ihrer sozialen Netzwerkdaten beispielsweise eine allgemein niedrige Zahlungsbereitschaft (Krasnova et al. 2009; Schreiner und Hess 2015; Spiekermann und Korunovska 2017). Spiekermann et al. (2012) stellten zum Beispiel fest, dass sich zwar die bereits vorgestellte „Psychologie des Eigentums“ als treibender Faktor für die Zahlungsbereitschaft erwies, dennoch waren bis zu 62% der Studienteilnehmer nicht bereit, auch nur einen trivialen Betrag zu zahlen, um ihre sozialen Netzwerk-Profile vor einer Löschung zu bewahren. Das Ergebnis ändert sich jedoch, wenn den Studienteilnehmern bewusstgemacht wurde, dass ein Dritter an ihren Daten interessiert ist und sie damit unter dem Einfluss des bereits vorgestellten Wertbewusstseins-Faktors stehen (Spiekermann et al. 2012). Der Anteil der Teilnehmer mit einer Zahlungsbereitschaft von 0 Euro sinkt auf 40% und die durchschnittliche Zahlungsbereitschaft steigt um den Faktor 3,4 (Spiekermann et al. 2012). Andere Studien im Kontext sozialer Netzwerke, wie die Conjoint-Analyse von Krasnova et al. (2009) zeigen, dass Nutzer durchschnittlich bereit wären, 14-17 Euro pro Jahr zu zahlen um zu unterbinden, dass demographische Informationen für personalisierte Werbezwecke verwendet werden, während die Studienteilnehmer von Schreiner und Hess‘ BDM nur 63 Cent für eine Facebook-Premiumversion mit Privatsphäre-schützenden Features zahlen würden (Schreiner und Hess 2015). Diese leicht unterschiedlichen Beträge könnten aufgrund entgegenstehender Datenschutzdefinitionen erklärt werden. Schreiner und Hess (2015) beschrieben die Facebook-Alternative als weniger aufdringlich in Bezug auf Werbung. Krasnova et al. (2009)

[5] Einige Absätze dieses Unterkapitels basieren auf Wessels et al. (2019b) und sind somit dem 5. Kapitel dieser Arbeit vorgezogen worden.

gehen darüber hinaus und haben eine Facebook-Alternative entwickelt, die ein höheres Maß an Anpassungsfähigkeit und Datenschutzkontrolle bietet. Eine weitere Studie im Kontext sozialer Netzwerke konzentriert sich auf den Unterschied zwischen den eigenen Profilinformationen und den Profilen anderer (Pu und Grossklags 2016). Die Studie zeigt, dass die Privatsphäre von Freunden weniger wertgeschätzt wird, was ein Indikator dafür ist, dass Individuen "Privatsphären-Egoisten" sind (Pu und Grossklags 2016).

Bezüglich des Datenschutzes im Kontext von Smartphones zeigte sich, dass die befragten Individuen eher abgeneigt sind eine Smartphone-Applikation zu nutzen, die Zugriff auf ihre sozialen Netzwerkdaten hat (Krasnova et al. 2014). Um beispielsweise ein Feature wie den Facebook-Login zu vermeiden, waren die Studienteilnehmer bereit, je nach Anzahl der Berechtigungen des Logins, zwischen 1,79 Euro und 6,24 Euro zu zahlen (Krasnova et al. 2014).

Suchmaschinenbenutzer scheinen hingegen eher zurückhaltend zu sein, wenn es darum geht, ihre eigenen Browserdaten zu schützen. Dies wird durch die Studie von Preibusch (2013) veranschaulicht, in der die Individuen Privatsphäre-schützende Funktionen für Suchmaschinen schätzen, wenn sie kostenlos angeboten werden, aber nur 15% eine geringe Prämie dafür zahlen würden. Wenn jedoch Datenschutzsymbole angezeigt werden, ist der Anteil der Personen, die den Shop mit besseren Datenschutzbedingungen wählen, deutlich höher als ohne (Tsai et al. 2011). Sie würden sogar eine Prämie dafür zahlen (Egelman et al. 2009).

Die Ergebnisse bezüglich der Zahlungsbereitschaft für einen erhöhten Datenschutz fallen also insgesamt relativ niedrig aus, allerdings sind auch deutliche Unterschiede zwischen den einzelnen Studienergebnissen zu erkennen. Diese werden noch größer, wenn die Bereitschaft der Individuen zum Verkauf ihrer personenbezogenen Daten mit einbezogen werden. So variieren die Werte für Standortdaten, die für akademische Zwecke verkauft werden, beispielsweise zwischen 11,42 Euro[6] und 88,71 Euro im Median, selbst für die gleiche Messmethode einer reversen Vickrey-Auktion (Brush et al. 2010; Cvrcek et al. 2006; Danezis et al. 2005), die bereits im Kapitel 4.3.2 vorgestellt wurde. Gründe für die Abweichungen lagen in diesen Fällen unter anderem an den unterschiedlichen Stichproben, sowie an Variationen im Studiendesign (z.B. durch die gegebenen Anreize) und des Kontextes, beispielsweise durch die Integration von verschiedenen Verschleierungsverfahren (Brush et

[6] Zur besseren Vergleichbarkeit der Werte wurden die Ergebnisse in Fremdwährungen auf Basis des Wechselkurses vom November 2018 in Euro umgerechnet.

al. 2010; Cvrcek et al. 2006; Danezis et al. 2005). Dabei zeigte sich, dass die Individuen durchaus Bedenken hinsichtlich der Preisgabe von Daten haben, die es anderen ermöglichen, Rückschlüsse auf ihre tägliche Routine und ihren Aufenthaltsort zu ziehen (Brush et al. 2010). Neben diesen drei Auktions-Studien, führten Barak et al. (2013) eine Umfrage mit geschlossenen Fragen durch, bei der die zur Verfügung stehenden Alternativen nur akzeptiert oder abgelehnt werden mussten. Mit dieser Methode betrug der Medianwert für ein einmaliges Teilen des Standorts wiederum nur 8 Euro (Barak et al. 2013), was die Ergebnisse für den Wert von Standortdaten noch weiter streuen lässt.

Grossklags und Acquisti (2007) stellten weiterhin fest, dass ihre Studienteilnehmer, wenn sie offen danach gefragt wurden, einen Mindestpreis von 31,80 US-Dollar (im Mittelwert) für den Verkauf von Gewichtsinformationen verlangten, während in derselben Studie fast alle Individuen Angebote für sogar 25 Cent oder 1 US-Dollar für die gleiche Art von Daten angenommen haben. Gründe für die Diskrepanz vermuten die Autoren darin, dass sich die Befragten im Gegensatz zur einfachen binären Entscheidung zwischen Annahme und Ablehnen eines Angebotes, unwohler damit zu fühlen scheinen, eine niedrige Verkaufsbereitschaft frei heraus zu nennen (Grossklags und Acquisti 2007). Darüber hinaus werden die Ergebnisse noch stärker gestreut, wenn die Auktionsstudie von Huberman et al. (2005) noch mit einbezogen wird, die eine Mindestverkaufsbereitschaft von 74,06 US-Dollar für Gewichtsinformationen ergeben hat.

Weiterhin zeigen frühere Forschungsstudien, dass Informationen über das Verhalten im Internet im Allgemeinen, seien es die besuchten Shops oder Webseiten, weniger wertgeschätzt werden als Informationen, die nicht nur mit dem Webverhalten des Benutzers, sondern auch mit seiner Offline-Identität (wie Name, Adresse oder Einkommen) verknüpft sind (Carrascal et al. 2013). Der Median der Verkaufsbereitschaft für Daten aus der ersten Kategorie lag bei rund 7 Euro, während die zweite Kategorie mit 25 Euro bewertet wurde (Carrascal et al. 2013).

Zusammengefasst, lassen sich also bestimmte Faustregeln aus dem Vergleich der Studien ableiten, zum Beispiel, dass Standortdaten höher bewertet werden als soziale Netzwerkdaten oder Browserinformationen. Jedoch müssen auch immer die Methoden zur Erhebung des Wertes von Daten sowie die Faktoren, die darüber hinaus noch Einfluss auf die Wertwahrnehmung haben, berücksichtigt werden.

4.4 Diskussion der Ergebnisse

Im Folgenden werden die wichtigsten Erkenntnisse der Studien aus der strukturierten Literaturanalyse diskutiert und mögliche zukünftige Forschungsrichtungen vorgestellt. Durch die Literaturrecherche konnten im Untersuchungszeitraum 2002 bis 2017 37 Studien identifiziert werden, die den monetären Wert, den Individuen ihren Daten zuweisen, quantifizieren. Die Studienkontexte der in das Sample eingeflossenen Literatur unterscheiden sich dabei deutlich voneinander, abhängig von den Messmethoden, den erforschten Datentypen, sowie den spezifischen Untersuchungsfaktoren, die den Wert der Daten zusätzlich beeinflussen können. Diese Faktoren tragen dazu bei, dass die in den Studien resultierenden Werte sehr unterschiedlich sind.

So geht aus einigen Studienergebnissen hervor, dass die befragten Individuen ihre Privatsphäre im Allgemeinen kaum wertschätzen. So hat in manchen Studien sogar die Aussicht auf einen trivialen Cent-Betrag ausgereicht, um Individuen zum Verkauf ihrer personenbezogenen Daten zu bewegen (z.B. Grossklags und Acquisti 2007), während in anderen Studien selbst ein kleiner Geldbetrag zum Schutz der eigenen Daten als zu hoch angesehen wurde (z.B. Bauer et al. 2012; Spiekermann und Korunovska 2017). In anderen Studienkontexten verlangten Teilnehmer für den Verkauf ihrer personenbezogenen Daten hingegen teilweise erstaunlich hochpreisige Werte (z.B. Brush et al. 2010; Huberman et al. 2005).

Die Werte variieren insbesondere da der Untersuchungsgegenstand der personenbezogenen Daten und Privatsphäre so viele verschiedene Ausprägungen in Form verschiedener Arten von Daten, die verkauft oder geschützt werden können, umfassen kann. In den analysierten Studien reichten diese von sozialen Netzwerk-, Lokations- und Smartphone-Daten bis hin zu Alters- und Gewichtsinformationen. Weiterhin konnten in den untersuchten Publikationen sechs weitere Kategorien von spezifischen Untersuchungsfaktoren identifiziert werden. Diese Anzahl an identifizierten Einflussfaktoren spiegelt die Vielfalt der bisherigen Studien wider. Neben dem Datentyp waren vor allem die Privatsphäre-relevanten Einflussfaktoren mit ihren elf Unterkategorien vorherrschend, wobei vor allem die allgemeinen Privatsphäre-Bedenken sowie der Grad der Sensibilität der zu enthüllenden Daten die am häufigsten in den Studien untersuchten Faktoren waren. Dabei haben alle diese Studien ein gemeinsames Ergebnis: Je sensibler die Daten und je identifizierbarer die Personen sind, desto höher ist der Preis, den die Individuen ihren Daten beimessen, da sie dann höhere Risiken wahrnehmen.

Weiterhin tragen auch die zwischen den Studien unterschiedlich präsenten Privatsphäre-Definitionen sowie Bestimmungen darüber, wie und warum Informationen gesammelt werden, zur Varianz der Werte bei. Dabei hat sich gezeigt, je transparenter die Datenpraktiken dargestellt wurden, desto höher war das Risikobewusstsein und damit die Auswirkungen auf die monetäre Bewertung der Daten. Wenn Datenschutzinformationen also leicht zugänglich und plausibel sind, scheinen Individuen sensibler darauf zu reagieren.

Durch die Analyse der bisherigen Forschungsstudien konnte gezeigt werden, dass ebenfalls die Art und Weise wie die Studien durchgeführt wurden und mit welcher Messmethode gearbeitet wurde, einen deutlichen Einfluss auf den Wert von Daten haben können. Die bisher untersuchte Literatur stützt sich dabei auf experimentelle Studiendesigns, die von Online-Umfragen bis hin zu Labor- und Feldexperimenten reichen. Wie schon beschrieben, unterschieden sich die Ergebnisse der Studien mit direkten Umfragen erheblich von Experimenten wie beispielsweise Auktionen. Experimentelle Studien gelten dabei als realistischere Settings, die zu bevorzugen sind, da sie meistens mit echten Konsequenzen und Anreizen für die Teilnehmer einhergehen, was zu einer realistischeren Bewertung der Daten führt (z.B. Acquisti et al. 2009; Grossklags und Acquisti 2007). Auf Untersuchungen hypothetischer Natur sollte hingegen in zukünftigen Studien verzichtet werden, da diese zu Verzerrungen führen können, die sich in überhöhten Verkaufs- und Zahlungsbereitschaftsergebnissen widerspiegeln können und eine der Ursachen für das Privatsphäre-Paradoxon sein können (z.B. Huberman et al. 2005).

Weiterhin unterscheiden sich die Stichprobengröße und die -merkmale zwischen den ausgewählten Studien erheblich, wodurch eine Art "Selektionsverzerrung" entstehen kann. Viele der analysierten Studien wurden dabei hauptsächlich mit Studierenden-Stichproben durchgeführt (z.B. Barak et al. 2013; Cvrcek et al. 2006; Danezis et al. 2005), die sich im Allgemeinen durch verstärkte Studienteilnahmen auszeichnen, da Studierende in der Regel empfindlicher auf finanzielle Belohnungen reagieren und für Forscher leicht erreichbar sind. Dies führt in den betreffenden Studien zu einer verhältnismäßig jungen Stichprobe beispielsweise im Gegensatz zu der Feldstudie von Acquisti et al. (2009). Darüber hinaus variieren die kulturellen Hintergründe der Studienteilnehmer, die von rein deutschen Stichproben (z.B. Bauer et al. 2012; Schreiner und Hess 2015) über europäische (z.B. Cvrcek et al. 2006) bis hin zu US-amerikanischen Stichproben (z.B. Egelman et al. 2009; Tsai et al. 2011) reichen. Weiterhin wurden, wie schon erwähnt, viele Studien im Kontext sozialer Netzwerke durchgeführt. Es kann argumentiert werden, dass soziale Netzwerk-Nutzer

unbesorgter als Nicht-Nutzer sind, da sie ihre Daten kostenlos preisgeben, um im Gegenzug soziale Netzwerkdienste zu nutzen. Zukünftige Forschung sollte also versuchen eine stärkere Repräsentativität für alle Internetnutzer zu schaffen.

Bezüglich der theoretischen Beiträge früherer Studien fällt auf, dass die meisten auf der Privatsphäre-Literatur basieren, wie im 2. Kapitel vorgestellt, und einige Studien das Privatsphäre-Kalkül und den zugrundeliegenden Trade-off zwischen Risiken und Nutzen als konzeptionelles Modell verwenden (z.B. Krasnova et al. 2009; Nguyen et al. 2016). Nur wenige Studien bauen auf Theorien wie der Informationsverarbeitungstheorie (engl. *information-processing theory*) (z.B. Hann et al. 2007; Hann et al. 2002), der Multiattribute-Nutzentheorie (engl. *multi-attribute utility theory*) (z.B. Nguyen et al. 2016), der Verfügungsrechtstheorie (engl. *theory of property rights*) (z.B. Rose 2005) und der Theorie des geplanten Verhaltens (engl. *theory of planned behavior)* (z.B. Schreiner und Hess 2015) auf. Zukünftige Forschung könnte auch Theorien aus anderen Disziplinen adaptieren und erweitern, die sich beispielsweise auf den Entscheidungsprozess und das Bewusstsein der Individuen sowie auf ihr Vertrauen in eigene Urteile konzentrieren. So könnte beispielsweise eine Einbeziehung der Bewertungstheorie (engl. *evaluability theory*) (z.B. Hsee und Zhang 2010) und der *elastic justification* (z.B. Schweitzer und Hsee 2002) sowie allgemeiner Verzerrungen aus der Verhaltensökonomie vielversprechend für Untersuchungen sein. Da die Wirtschaftsinformatik-Forschung interdisziplinärer Natur ist, könnte bei zukünftigen Studien ebenfalls noch stärker hervorgehoben werden, wie Informationstechnologien die Bewertung von Daten beeinflusst, da diese oft bestimmen, wie Informationen über den Datenschutz präsentiert werden. Zusammengefasst könnte zukünftige Forschung einen großen Beitrag leisten, wenn sie die Auswirkungen der wichtigen Einflussfaktoren näher untersucht, um eine allgemeinere Konzeptualisierung zum Wert von Daten zu erreichen. Dazu könnte ebenfalls mehr Forschung zur Untersuchung der moderierenden Effekte auf die Zahlungs- und Verkaufsbereitschaft durchgeführt werden.

Zu guter Letzt, konnte festgestellt werden, dass sich die Mehrheit der Studien, die den Wert von Daten untersucht, auf die Zahlungsbereitschaft konzentrierte. Dabei entstehen, wie schon im Einleitungskapitel dieser Arbeit erläutert, immer mehr Start-ups, die es den Nutzern ermöglichen, ihre personenbezogenen Daten aktiv zu verkaufen. Trotz dieses Trends ist das Wissen über verallgemeinerbare Verkaufsbereitschaft aufgrund der sehr speziellen Kontexte der bisherigen Studien begrenzt. Daher könnte verstärkt Forschungsarbeit im Bereich der Verkaufsbereitschaft von Daten und seinen Einflussfaktoren einen großen Beitrag leisten.

Darüber hinaus könnte zukünftige Forschung die Auswirkungen der Weitergabe von Daten an dritte Parteien näher untersuchen.

Zusammenfassend zeigt die vorliegende strukturierte Literaturrecherche, wie kontextsensitiv Individuen bei der Bewertung ihrer Daten und damit ihrer Privatsphäre sind. Insbesondere die Messmethode und damit das Studiendesign können einen enormen Einfluss auf den ermittelten monetären Wert der Daten aus Nutzerperspektive haben. Aber auch der Datentyp und die Sensitivität der Daten, sowie Untersuchungsfaktoren wie die Privatsphäre-Bedenken der Studienteilnehmer scheinen ein wichtiger Treiber für die Bewertung der Daten zu sein. Je sensibler die Daten und je transparenter die Datenschutzeinschränkungen dargestellt werden, desto höher sind die Privatsphäre-Bedenken der Individuen und damit auch der finanzielle Wert, der den Daten beigemessen wird. Daher hat die bisherige Forschung sich bemüht, viele verschiedene und optimierte Studienkontexte zu untersuchen, die teilweise aber recht künstlich wirken. Diese Studien sind wichtig, um den Wert, den Individuen ihren Daten in einem bestimmten Kontext zuweisen, zu verstehen. Es ist aber schwierig, die Ergebnisse in einen breiteren Kontext zu übertragen, beispielsweise mit komplizierten Datenschutzrichtlinien, einer komplexeren Struktur der involvierten Parteien, sowie indirekten Einflüssen. Hierzu besteht demnach noch weiterer Forschungsbedarf. Daher behandeln die folgenden beiden Studien, die in dem 5. und 6. Kapitel vorgestellt werden, weitere Untersuchungen zum Wert von Daten aus der Nutzerperspektive, um so einige der in dieser Literaturrecherche identifizierten Verbesserungspotenziale für zukünftige Forschung zu adressieren.

5 Eine Feldstudie zur Ermittlung des Wertes personenbezogener Daten durch eine *Name-Your-Own-Price* Auktion[7]

Nachdem im vorausgegangenen Kapitel dieser Arbeit der aktuelle Forschungsstand zur Ermittlung des Wertes von Daten aus Nutzerperspektive erläutert wurde, wird nun eine Studie vorgestellt, die den Wert von personenbezogenen Informationen mit einer neuen, vielversprechenden Methodik misst: der *Name-Your-Own-Price* Auktion mit Option des wiederholten Bietens.

5.1 Motivation und Relevanz

"Digital information is unlike any previous resource; it is extracted, refined, valued, bought and sold in different ways. It changes the rules for markets and it demands new approaches from regulators. Many a battle will be fought over who should own, and benefit from, data."

The Economist (2017a)

Wie bereits in den ersten Kapiteln dieser Arbeit beschrieben, sind personenbezogene Informationen eine immer wichtiger werdende Ressource. Vergleiche von personenbezogenen Daten mit Öl, Gold oder allgemein Rohstoffen sind in den Medien allgegenwärtig (Economist 2017b; Medium 2018) und die Erfolge von datenbasierten Unternehmen wie Google treten traditionellen Geschäftsmodelle den Rang ab (Brynjolfsson et al. 2011). So sind unter den Top 6 der Unternehmen mit dem weltweit größten Marktwert, fünf datenbasierte Unternehmen zu finden (Slotin 2018; Statista 2018a). Aus Perspektive der Unternehmen sind personenbezogene Daten folglich ein wertvolles Gut und sie konkurrieren bereits darum, am besten davon zu profitieren (Bauer et al. 2012).

Im Gegensatz dazu ist der Nutzen, den Individuen aus der Weitergabe personenbezogener Daten ziehen, weniger offensichtlich, da sie in der Regel keine finanzielle Vergütung dafür erhalten. Natürlich profitieren Internetnutzer durch die Verwendung von Tools und Produkten, die auf personenbezogenen Daten basieren, allerdings entwickeln auch immer mehr Individuen, wie bereits in dieser Arbeit ausgeführt, Bedenken hinsichtlich der Offenlegung ihrer personenbezogenen Daten, welche mit dem Gefühl, ungerecht behandelt zu

[7] Dieses Kapitel basiert auf Wessels et al. (2019b).

werden, einhergehen (Acquisti et al. 2016; Culnan und Armstrong 1999; Culnan und Bies 2003). Tatsächlich zeigt eine DDMA-Studie aus den Niederlanden, dass die befragten Individuen den Gegenwert, den sie für ihre Daten erhalten als ungenügend empfinden, denn 89% der Befragten gaben an, dass die Unternehmen die klaren Profiteure der Datenwirtschaft sind (DDMA 2016). Also scheinen sich Individuen zunehmend bewusst zu werden, dass ihre Daten wertvoll sind, zumindest auf einer abstrakten Ebene.

Um jedoch die aktuellen Datenverarbeitungspraktiken und Regulierungsansätze beurteilen zu können, müssten Individuen über diese abstrakte Ebene hinaus den Wert ihrer Daten noch genauer einschätzen können, um so die Kosten potenzieller Privatsphäre-Risiken ihrer Daten-Preisgabe mit den Vorteilen, die durch die Datennutzung entstehen, vergleichen zu können (Carrascal et al. 2013). Allerdings zeigt die Forschung, die sich mit der Vorstellung von Individuen hinsichtlich des Wertes von personenbezogenen Daten beschäftigt, wie im 4. Kapitel bereits dargelegt, dass diese Wertermittlung keineswegs trivial ist, was durch die starken Varianzen in den Forschungsergebnissen, die teilweise sogar widersprüchlich sind, verdeutlicht wird. Denn auch wenn personenbezogene Daten an traditionelle, wertvolle Ressourcen erinnern, unterscheiden sie sich wesentlich von diesen Ressourcen, da sie materiell unendlich sind und sich nicht selbst verbrauchen (Bharosa et al. 2018). Weiterhin können Daten nicht mit „gewöhnlichen“ Gütern, wie beispielsweise Gebrauchsgütern, gleichgesetzt werden, denn schließlich können sie sehr sensitiv sein und den Datenpreisgebenden identifizierbar machen (Spiekermann et al. 2015b). Dies kann es für Individuen schwieriger machen einen Wert für ihre Daten zu eruieren, wodurch sich die erste Untersuchungsfrage ergibt:

Haben Individuen eine klare Wertvorstellung für personenbezogene Daten?

Zur Untersuchung dieser Fragestellung wurden im Rahmen einer Vorstudie 20 Interviews durchgeführt, in denen Individuen eine Ad hoc-Bewertung personenbezogener Daten vorgenommen haben. Dabei hat sich gezeigt, dass es für die befragten Personen durchaus eine Herausforderung darstellt, unvermittelt einen Wert für ihre Daten zu nennen.

In früheren Studien zur Wertermittlung personenbezogener Daten mussten die Teilnehmer jedoch in der Regel ihre Wertvorstellung ähnlich wie in der Vorstudie, direkt und unvermittelt äußern, ohne dass ihnen die Möglichkeit eingeräumt wurde, den genannten Wert nochmals zu überdenken und anzupassen (z.B. Grossklags und Acquisti 2007; Huberman et al. 2005; Jentzsch 2014). Wie durch die Vorstudie bestätigt, kann dies für Individuen jedoch

herausfordernd sein, wenn sie sich bezüglich ihrer eigenen Wertvorstellung unsicher sind, da sie bisher wenig bis keine Erfahrung mit der Monetarisierung von Daten haben.

Vor diesem Hintergrund erfordert Forschung zur Wertermittlung personenbezogener Daten besondere Sorgfalt bei der Wahl des Studiendesigns und der Messmethode. Ein neuer und vielversprechender Ansatz ist die *Name-Your-Own-Price* (NYOP) Auktion. Diese wurde bereits in anderen Kontexten zur Preisgestaltung von "undurchsichtigen" (engl. *opaque*) Gütern angewandt und kann den niedrigsten Preis separat für jeden Einzelnen ermitteln, da keine synchronen Gebote erforderlich sind (Fay 2004; Hinz et al. 2011; Terwiesch et al. 2005). Darüber hinaus können NYOP-Auktionen mit einer wiederholten Biet-Option durchgeführt werden, die Individuen die Möglichkeit gibt, Feedback bezüglich zu hoher Gebote zu erhalten, um dann ein überdachtes Gebot abgeben zu können. Dies kann die Wertermittlung für Individuen erleichtern, indem sie das Feedback als Informationsquelle nutzen (Klemperer 2004; Liu et al. 2016). Auf Basis dessen ergibt sich die zweite Untersuchungsfrage:

Welchen finanziellen Wert weisen Individuen ihren personenbezogenen Daten zu, wenn sie mehrere Werte angeben können, nachdem sie Feedback in einer Name-Your-Own-Price Auktion mit Option des wiederholten Bietens erhalten haben?

Zur Beantwortung dieser Untersuchungsfrage wurde ein Feldexperiment durchgeführt, bei dem die Teilnehmer Selfies von sich in einer NYOP-Auktion mit integrierter Option des wiederholten Bietens verkaufen konnten. Die Ergebnisse der Studie zeigen, dass die meisten Teilnehmer tatsächlich ihre Chancen genutzt haben und mehrmals boten. Insgesamt führten die Gebote zu einem Endverkaufspreis von 5 Euro im Median. Eine weitergehende Analyse der Gebote zeigte zudem verschiedene Bieter-Gruppen innerhalb der Stichprobe, was darauf hindeutet, dass die Wertvorstellung bezüglich personenbezogener Daten sehr individuell ist.

Im weiteren Verlauf dieses Kapitels wird erneut kurz auf den theoretischen Hintergrund zur Wertermittlung personenbezogener Daten und somit der Privatsphäre eingegangen, bevor im darauffolgenden Unterkapitel die Vorstudie zur Untersuchung der ersten Untersuchungsfrage vorgestellt wird. Anschließend wird das Feldexperiment zur Untersuchung der zweiten Untersuchungsfrage mit seiner Methodik und den Ergebnissen vorgestellt. Schließlich folgt die Diskussion der Ergebnisse aus der die Implikationen abgeleitet werden, sowie die Limitationen und zukünftige Forschungsrichtungen aufgezeigt werden.

5.2 Forschung zum Wert von Daten

Im 4. Kapitel dieser Arbeit wurde bereits dargelegt, dass zur Untersuchung des monetären Wertes, den Individuen ihren personenbezogenen Daten zuweisen, Studien entweder die Verkaufsbereitschaft (z.B. Acquisti et al. 2009; Grossklags und Acquisti 2007; Hann et al. 2007) oder die Bereitschaft für den Schutz ihrer personenbezogenen Daten zu zahlen (z.B. Egelman et al. 2013; Krasnova et al. 2009; Tsai et al. 2011), untersuchen. Die Ergebnisse früherer Studien sind allerdings sehr unterschiedlich, wie die strukturierte Literaturrecherche des vorangegangenen Kapitels aufzeigt.

Die im Kapitel 4.3.3 zusammengetragenen Ergebnisse bisheriger Forschung, verdeutlichen die Abhängigkeit der Studien von einer Vielzahl von Faktoren wie dem Datentyp, den Untersuchungsfaktoren oder der Messmethode. Die hohen Diskrepanzen zwischen den resultierenden Werten begrenzen den Beitrag, den dieses Themenfeld eigentlich für Forschung und Praxis darstellen könnte. Es ist jedoch auch ein Indikator dafür, dass Individuen Schwierigkeiten damit haben, einen stabilen und sicheren Geldwert im Zusammenhang mit personenbezogenen Daten zu benennen. Darauf wird im nächsten Kapitel 5.3 noch genauer eingegangen.

5.3 Qualitative Vorstudie

Um die erste Untersuchungsfrage, ob Individuen Schwierigkeiten haben, unvermittelt einen Wert für ihre personenbezogenen Daten zu benennen, beantworten zu können, wurde eine qualitative Vorstudie unter Internetnutzern durchgeführt. Dabei wurden Interviews mit 20 Befragten, zehn Frauen und zehn Männern, durchgeführt, die durchschnittlich 34,05 Jahre (Standardabweichung $\sigma = 11{,}43$) alt waren.

Da die qualitative Studie darauf abzielte die Reaktionen der Befragten hinsichtlich einer Ad hoc-Bewertung ihrer personenbezogenen Daten zu untersuchen, wurde den Studienteilnehmern einfach unvermittelt die Frage: "*Zu welchem Preis würdest du ein Foto von dir selbst verkaufen*?" gestellt. Diese Fragestellung wurde ausgewählt und in der Form ausgedrückt, da sie simpel und einfach zu verstehen ist und nach einem Datum fragt, das einen deutlichen Personenbezug enthält.

Zur Analyse und Kodierung der Interviewdaten wurde ein Ansatz von Miles et al. (1994) genutzt. Basierend auf diesem Ansatz, wurden alle Antworten der Studienteilnehmer hinsichtlich Ähnlichkeiten und Textpassagen untersucht, die kognitive Anstrengungen der Individuen repräsentieren. So wurde in dem Datensatz speziell nach Wörtern gesucht, die

Anzeichen für Schwierigkeiten bei der Benennung des Wertes, wahrgenommenen Druck oder Ahnungslosigkeit der Befragten waren und als Indikator für das Ausmaß der Anstrengung genutzt werden konnte. Es zeigte sich, dass insgesamt 65% der Befragten Füllwörter wie "*ähm*", "*hmm*", "*puh*" oder "*uff*" verwendeten, um ihre Reaktion auf diese Frage auszudrücken. Darüber hinaus brachten neun Befragte ihre Ahnungslosigkeit mit Passagen wie "*Ich habe keine Ahnung*", "*schwierige Frage*", "*sehr schwer zu sagen*" oder "*Ich habe noch nie darüber nachgedacht*" zum Ausdruck. Auffällig war auch, dass viele der Befragten lange Pausen machten und nichts sagten während sie über die Frage nachdachten. Ein Teilnehmer blieb zum Beispiel über 20 Sekunden lang still, mit Ausnahme der kleinen Aussage "*Ich denke nach*" und eine andere Teilnehmerin hielt 14 Sekunden lang inne, bevor sie mit der Antwort begann.

Durch Analyse des Datensatzes konnten außerdem drei verschiedene Gruppen der Interviewten identifiziert werden. Die **erste Gruppe** bestehend aus 13 Befragten gab, in den meisten Fällen nach einer langen Überlegungszeit, schließlich einen Betrag für ein Foto von sich an. Dabei spezifizierten die Teilnehmer die Werte beispielsweise mit Aussagen wie: "*Vielleicht sage ich einfach..."* oder "*Dann sage ich mal pauschal...*" sowie "*.... würde ich jetzt aus dem Bauch heraus sagen*". Die genannten Geldwerte reichten von 50 Cent bis zu 10.000 Euro. Einige Befragte gaben auch keinen konkreten Wert an, sondern Bereiche wie beispielsweise "*ein paar hundert Euro*". Die **zweite Gruppe**, bestehend aus vier Befragten, konnte keinen Wert angeben. Ihre Antworten waren zum Beispiel *"Keine Ahnung, also, ist "keine Ahnung" eine gültige Antwort?"* oder *"Ich kann dir ehrlich gesagt nicht sagen, wie viele Euro mir das wert wäre."* Auch die drei Befragten der **dritten Gruppe** nannten keine Werte, da sie es kategorisch ablehnten ein individuelles Foto zu verkaufen, egal zu welchem Preis.

Zusammengefasst zeigt die Vorstudie in Bezug auf die erste Untersuchungsfrage, dass Individuen kognitiv durchaus herausgefordert sind, wenn sie unvermittelt aufgefordert werden, einen finanziellen Wert für ihre personenbezogenen Daten anzugeben. Nach einer Reflexionsphase konnte die Mehrheit jedoch einen Wert angeben, der unter den Befragten starke Varianzen aufzeigt.

5.4 Feldstudie

Die qualitative Vorstudie hat also gezeigt, dass Individuen tatsächlich Schwierigkeiten haben können, ad hoc einen monetären Wert für ihre personenbezogenen Daten anzugeben, wenn sie

unvermittelt dazu befragt werden. Im weiteren Verlauf dieser Studie, werden diese potenziellen kognitiven Schwierigkeiten bei der Ermittlung eines monetären Wertes für personenbezogene Daten adressiert, indem eine neue, vielversprechende Messmethode angewendet wird, welche die Wertermittlung für Individuen erleichtern kann: eine *Name-Your-Own-Price* Auktion mit Option des wiederholten Bietens. Diese Auktionsart bietet den Vorteil, dass Individuen Feedback erhalten können, wenn ihr Gebot zu hoch ist und diese Ablehnung als Informationsquelle nutzen können (Hann und Terwiesch 2003; Liu et al. 2016), um schließlich ein überdachtes Angebot abgeben zu können. Um die NYOP-Auktion in einem realistischen Szenario anwenden zu können, wurde eine Feldstudie durchgeführt, bei der die Teilnehmer Selfies von sich verkaufen konnten.

5.4.1 Methode der Feldstudie

Im folgenden Unterkapitel wird die Methode der Feldstudie anhand des experimentellen Designs, einer detaillierten Beschreibung der Funktionsweise der NYOP-Auktion, sowie der Studiendurchführung vorgestellt.

Experimentelles Design

Dem Aufruf von Dinev et al. (2015) nach realistischeren Studienszenarien folgend, die auch ein tatsächliches Verhalten der Teilnehmer auslösen können, wurde bei dem experimentellen Design der Studie darauf geachtet, dass die Teilnehmer die Offenlegung ihrer personenbezogenen Informationen als eine natürliche und verständliche Aufgabe wahrnehmen, die zu tatsächlichen Verkäufen führen kann. Daher erschien es auch angebracht das Umfeld der Universität für die Studiendurchführung beizubehalten, da dieses ein natürliches Szenario für eine Forschungsstudie darstellen kann. Demnach waren auch Studierende die Zielgruppe. Es wurde eine fiktive Kampagne entwickelt, nach der der Lehrstuhl die "Gesichter unserer Universität" sucht, um die Institution bei interessierten Schülern und Studienanfängern bewerben zu können. Das angebliche Ziel dieser Kampagne war es daher, Selfies von Studierenden zu sammeln, um damit eine Fotocollage zu erstellen, mit der die Universität mit dem Slogan "von Studierenden für Studierende" authentisch und sympathisch werben könnte.

Die Entscheidung sich auf Selfies als personenbezogene Informationen zu konzentrieren fiel, da Selfies immer die Gesichter von Personen darstellen, wodurch ein Bild im Vergleich zu normalen Fotos direkt in eine personenbezogene Information verwandelt wird. Darüber hinaus sind Selfies derzeit modern und allgegenwärtig, wodurch von einer Vertrautheit der

befragten Studierenden mit Selfies ausgegangen werden kann, was wiederum das Risiko von Missverständnissen in der Studie reduziert (Statista 2018b).

Um die Kampagne adäquat vorstellen zu können, wurde eine Webseite mit einer detaillierten Beschreibung des vorgestellten Marketingzwecks sowie der Realisierung der NYOP-Auktion implementiert, mit der die Studierenden angeblich ihre Selfies an das Fachgebiet verkaufen konnten. Der Ablauf einer NYOP-Auktion wird im Folgenden erläutert.

***Name-Your-Own-Price* (NYOP) Auktion mit Option des wiederholten Bietens**

Die *Name-Your-Own-Price* Auktionsart basiert auf einem „Feilsch"-Prozess, da bei dieser weder ein Durchschnitts- noch ein Marktpreis veröffentlicht wird, sondern vielmehr beruht NYOP auf dem Prinzip, dass sowohl der Verkäufer als auch der Käufer gemeinsam an der Preisfindung beteiligt sind (Chernev 2003; Hann et al. 2006; Spann et al. 2005; Terwiesch et al. 2005). Traditionell werden NYOP-Auktionen von den Produktverkäufern initiiert, um die Zahlungsbereitschaft der Käufer zu untersuchen, ohne den niedrigsten Preis offenlegen zu müssen (z.B. Amaldoss und Jain 2008; Chernev 2003; Hinz et al. 2011). Ebenso wie andere Auktionsarten, wie die reverse Zweitpreisauktion (z.B. Danezis et al. 2005; Egelman et al. 2013; Huberman et al. 2005), sind NYOP-Auktionen auch für die Untersuchung der Zahlungs- und Verkaufsbereitschaft von Individuen gleichermaßen anwendbar. Der Käufer legt dabei den Schwellenwert, also den Wert, den er maximal für das Gut bereit ist zu zahlen, fest, ohne jedoch Auskunft über diesen Schwellenwert zu geben (Hann et al. 2006). Potenzielle Verkäufer können nun Gebote abgeben und wenn diese den Schwellenwert treffen oder unterschreiten, erfolgt jeweils der Kauf in Höhe des vom Verkäufer angebotenen Wertes (Fay und Zeithammer 2016; Spann und Tellis 2006). Liegt das Gebot jedoch über dem Limit, wird es abgelehnt, aber bei der NYOP-Variante mit wiederholter Biet-Option hat der Verkäufer die Möglichkeit, sein Gebot zu wiederholen (Terwiesch et al. 2005).

Die NYOP-Auktionsart ist dabei sehr gut für die Messung des Wertes von Daten aus Nutzerperspektive geeignet, wie die nachfolgend aufgelisteten Punkte demonstrieren:

1. Die NYOP-Auktionsart wurde in anderen Kontexten auch schon für die Preisfindung von Waren angewandt, bei denen Unsicherheiten bezüglich der Produkteigenschaften bestehen und so der Preis intransparent ist (Terwiesch et al. 2005).
2. NYOP wird verwendet, um den niedrigsten Preis des Bieters zu ermitteln und spiegelt somit die tatsächliche Verkaufsbereitschaft der Individuen wider, sodass es gut auf reale Situationen übertragen werden kann (Terwiesch et al. 2005).

3. Im Gegensatz zu einer "ein Preis für alle"-Strategie, identifiziert NYOP zudem den individuellen Verkaufspreis der Bieter (Hinz et al. 2011).

4. Im Vergleich zur bereits beschriebenen reversen Zweitpreisauktion, die häufig in Studien zur Bewertung personenbezogener Daten durch Individuen angewandt wurde (z.B. Carrascal et al. 2013; Huberman et al. 2005; Jentzsch 2014), bekommt bei einer NYOP-Auktion nicht nur der am niedrigsten bietende Teilnehmer den Zuschlag (Spann und Tellis 2006). So hat nicht nur ein Teilnehmer die Möglichkeit seine personenbezogenen Daten zu verkaufen, sondern alle, die entsprechend bieten. Schließlich ist es bei NYOP nicht erforderlich, die Gebote gleichzeitig zu erhalten, da asynchron ankommende Gebote sofort angenommen oder abgelehnt werden können, da der Schwellenwert vorher gesetzt wird (Fay 2004).

5. Weiterhin kann der Initiator der Auktion je nach Designanpassung mehrere Gebote in chronologischer Reihenfolge zulassen, bis der Schwellenwert unterschritten wird (Option des wiederholten Bietens) (Spann et al. 2004). Auf diese Weise erhalten Individuen Rückmeldung, wenn ihre Gebote zu hoch sind, was wiederum als wertvolle Informationsquelle im Rahmen des Feilsch-Prozesses dienen kann (Hann und Terwiesch 2003; Liu et al. 2016). Dies macht die Methode für die Wertermittlung von Daten besonders geeignet, da sie das vage Bewusstsein der Individuen für die Bewertung personenbezogener Daten schärfen kann. Tatsächlich hat die frühere Forschung gezeigt, dass die freie Nennung eines Preises ohne Referenzinformationen mit kognitivem Aufwand verbunden ist und Personen daher Alternativen bevorzugen, bei denen sie einen Preis auswählen oder Informationen über die Bewertung erhalten können, beispielsweise durch vorgegebene Referenzpreisspannen (Chernev 2003). Dies würde jedoch mit einer Beeinträchtigung der Genauigkeit der Bewertung (Chernev 2003) und einer Verzerrung in Richtung der extern bereitgestellten Referenzinformationen (Johnson und Cui 2013) einhergehen. Im Gegensatz dazu stellt das Feedback einer NYOP-Auktion mit wiederholter Biet-Option den Individuen eine subtilere Information bereit, mit der die Wertermittlung erleichtert wird, allerdings ohne die Person zu sehr zu verankern, da schließlich kein Startwert angegeben wird, der dann anzupassen ist (Tversky und Kahneman 1974).

Aufgrund der Designentscheidung zu einer Auktion mit wiederholter Biet-Option musste der Schwellenwert auf einen niedrigen Wert festgelegt werden, da ein höherer Wert das Risiko mit sich gebracht hätte, Informationen über eine geringe Verkaufsbereitschaft zu verlieren.

Wenn der Schwellenwert beispielsweise 5 Euro betragen hätte und eine Person aber bereit wäre, Selfies für 3 Euro zu verkaufen, aber zuerst ein 5 Euro-Angebot versucht hätte, wäre der Verkauf mit 5 Euro abgeschlossen worden und die Information über die tatsächliche Verkaufsbereitschaft von 3 Euro wäre verloren gegangen. Daher wurde der Schwellenwert auf 1 Euro festgesetzt.

Weiterhin wurde die Anzahl der möglichen Gebotsabgaben auf drei begrenzt. Die Entscheidung zu dieser Designanpassung fiel, da frühere Studien zur Gestaltung von NYOP-Auktionen auf der Annahme beruhen, dass die Auktionsteilnehmer erwartete Aufwände, engl. *frictional costs,* in ihre Gebotsauswahl mit einbeziehen (Spann et al. 2004). Unter *frictional costs* werden Aufwände, wie die mentale Anstrengung für die Navigation durch die Webseite, die Eingabe der ausgewählten Gebote sowie die Wartezeit bis zum Zuschlag oder der Ablehnung des Gebotes verstanden (Hann und Terwiesch 2003; Spann et al. 2004). Um zu verhindern, dass diese Aufwände eine zu große Bedeutung erlangen, wurde die Anzahl der Angebote auf drei begrenzt. Dies bringt auch den Vorteil einer besseren Vergleichbarkeit der Ergebnisse aller Teilnehmer mit sich.

Abbildung 7 fasst den Mechanismus der in der Studie verwendeten NYOP-Auktion graphisch zusammen.

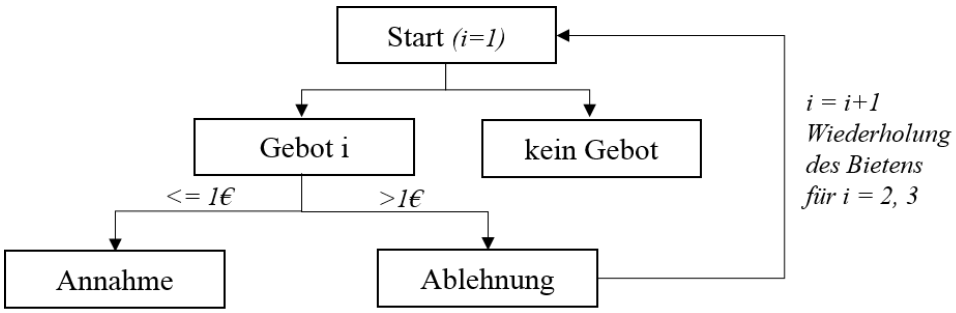


Abbildung 7: NYOP-Mechanismus der Feldstudie, angepasst von Spann et al. (2004)

Studiendurchführung

Die Beschreibung der fiktiven Kampagne sowie die eigentliche NYOP-Auktion, in der die Teilnehmer Selfies von sich verkaufen und dabei selbst Preisvorschläge machen konnten, wurde in einer Webseite implementiert. Zusätzlich zum NYOP-Mechanismus hatten die Teilnehmer auch die Möglichkeit, ihre Selfies für den gleichen Zweck zu spenden, selbst wenn sie bereits ein Gebot abgegeben haben. Um das Risiko zu verhindern, dass potenzielle Verkäufer nur, weil sie möglicherweise zum Zeitpunkt der Umfrage kein passendes Selfie zur

Hand haben, nicht bieten, wurde die Möglichkeit eingeräumt, das Selfie auch später mit einem eigens für diesen Zweck erstellten Link hochzuladen. Es wurde jedoch klar kommuniziert, dass die Vergütung erst erfolgt, wenn das Selfie tatsächlich hochgeladen wurde.

Um die Webseite unter den Studierenden der Universität zu verteilen, wurde die NYOP Auktion in eine Cover-Online-Umfrage integriert, sodass die Teilnehmer zunächst nicht wussten, was die eigentliche Absicht der Studie war. Um möglichst viele Studierende für die Umfrage gewinnen zu können, wurde für die Cover-Studie das Thema Werbung gewählt, da diese Thematik allgegenwärtig und zeitlos ist und damit das Interesse der Studierenden wecken konnte. Um den Studierenden einen zusätzlichen Anreiz zur Teilnahme an der Umfrage zu geben, erhielten sie für die Teilnahme an der Cover-Umfrage 3 Euro in bar.

Die Cover-Studie bestand aus den folgenden Abschnitten: Nach einer Einführungsseite mit allen DSGVO-relevanten Informationen wurden Alters- und Geschlechterdemographische Daten erhoben. Anschließend wurden den Teilnehmern verschiedene Skalen präsentiert, die deren Wahrnehmung und Haltung gegenüber Werbung untersuchen. Nach Abschluss der Cover-Studie wurden die Teilnehmer dann schließlich auf die "Wir suchen die Gesichter unserer Universität"-Kampagne aufmerksam gemacht und kommuniziert, dass die Teilnehmer die Chance haben, zusätzliches Geld zu gewinnen. Durch Anklicken des „Weiter“-Buttons wurden alle Teilnehmer der Cover-Studie auf die NYOP-Webseite weitergeleitet, wo sie eine detaillierte Beschreibung der Kampagne sowie der Funktionsweise der Auktion angezeigt bekamen und, wie oben beschrieben, ihre Gebote eingeben oder eine Spende durchführen konnten. Studierende, die kein Interesse an der Teilnahme hatten, konnten mit einem Klick auf einen „kein Interesse“-Button direkt zur ersten Umfrage zurückkehren und wurden dort über die Fiktion der Kampagne und den wahren Zweck der Studie informiert.

Um die Studie unter den Studierenden zu bewerben, wurden Flyer auf dem Campus verteilt sowie Posts auf der Facebook-Seite des Lehrstuhls gesetzt. Von insgesamt 186 Antworten mussten 15 aufgrund schlechter Datenqualität, wie unvollständige Daten oder ungültige Einträge, ausgeschlossen werden, was zu einem vollständigen Datensatz von 171 führte. Die finale Stichprobe bestand aus 44 Frauen (26%), 125 Männern (73%) und zwei nicht spezifizierten Geschlechtern (1%). Die recht hohe Männerquote repräsentiert die Geschlechterverteilung der technologieorientierten Universität, an der die Studie durchgeführt wurde. Da der Fokus auf Studierende als Zielgruppe gelegt wurde, war die Altersverteilung erwartungsgemäß stärker im jüngeren Segment vertreten. Mit einem Anteil von 75% war die

Mehrheit der Teilnehmer zwischen 18 und 25 Jahren alt. Darüber hinaus waren 22% der Teilnehmer zwischen 26 und 35 Jahren sowie 2% zwischen 36 und 45 Jahren alt. Nur 1% war älter als 46 Jahre.

Um die Daten zu analysieren und die Verteilung der Gebote visuell anschaulich zu präsentieren, wurden Ansätzen früherer Studien zur Bewertung personenbezogener Daten, die reverse Zweitpreisauktionen angewandt haben, gefolgt (Carrascal et al. 2013; Danezis et al. 2005; Staiano et al. 2014). Zusätzlich wurden Wilcoxon Vorzeichen-Rang-Tests sowie hierarchische Clusteranalysen durchgeführt.

5.4.2 Ergebnisse der Feldstudie

In den folgenden Abschnitten werden die Ergebnisse der Feldstudie vorgestellt. Dabei werden zunächst die Erkenntnisse über die Verkaufsbereitschaft der Teilnehmer für die beworbene Kampagne Selfies zu verkaufen präsentiert, bevor auf die Spendenbereitschaft der Befragten eingegangen wird.

Verkaufsbereitschaft von Selfies

Insgesamt haben 54 Teilnehmer der Studie Gebote abgegeben, was einem Anteil von 32% des Gesamtsamples entspricht. Das Sample war durchschnittlich 23,76 Jahre alt (σ = 3,77) und bestand aus 20% Frauen, 78% Männern und 2% nicht spezifizierten Geschlechtern. Während 40 dieser Teilnehmer die Möglichkeit des Mehrfachbietens voll ausschöpften und drei Gebote abgaben, trugen sieben Personen nur zwei Angebote ein, während weitere sieben nur einen Wert angaben. Unter der Annahme, dass das letzte Angebot einer NYOP-Auktionsgebotsreihe die tatsächliche Verkaufsbereitschaft eines Teilnehmers darstellt, ist das finale Angebot von größtem Interesse um den Wert von Selfies zu untersuchen. Es kann also angenommen werden, dass diejenigen, die zwei Werte angegeben haben, ihre wahre Verkaufsbereitschaft bereits innerhalb des zweiten Gebotes erreicht haben, also ihres finalen Gebotes. Analog dazu scheinen diejenigen, die letztlich nur einen Wert eingetragen haben, eine so klare Bewertung im Kopf zu haben, dass sie ihren realistischsten Wert in nur einem Gebot ausdrücken können. Daher wurden alle diese Gebote dem finalen, dritten Gebot zugeordnet. Der Mittelwert dieser finalen Gebote beträgt 29,24 Euro, wobei die Gebote zwischen 997 Euro und 1 Cent liegen. Der Median dieser finalen Gebote beträgt 5 Euro. Da sich somit ein recht großer Unterschied zwischen Mittelwert und Median ergibt und zudem die Standardabweichung von 135,24 ebenfalls recht hoch ist, lässt dies vermuten, dass es einige sehr hohe Bewertungen gibt, die den Mittelwert verschieben. Darauf wird im weiteren Verlauf dieser Analyse noch

detaillierter eingegangen. Insgesamt wurde der Schwellenwert von 1 Euro 14-mal erreicht oder unterschritten, was zu erfolgreichen "Verkäufen" von Selfies führte. Tabelle 4 gibt einen Überblick über die Statistiken der finalen Gebote zusammen mit den ersten und zweiten Geboten.

Tabelle 4: Statistiken der Start-, Zweit- und Finalen Gebote

	Erstes / Start-Gebot	**Zweites Gebot**	**Drittes / Finale Gebot**
Mittelwert (Standardabweichung)	93,28 Euro (221,91)	50,95 Euro (154,93)	29,24 Euro (135,24)
Median	25 Euro	10 Euro	5 Euro
N	40	47	54
[Max; Min]	[999,99 Euro; 2 Euro]	[998 Euro; 1,10 Euro]	[997 Euro; 0,01 Euro]

Bei Betrachtung der ersten und zweiten Gebote fällt auf, dass die Teilnehmer die Werte jedes Gebots sukzessiv verringert haben. Um die Unterschiede zwischen den drei Geboten zu analysieren, wurden paarweise Wilcoxon-Vorzeichen-Rang-Tests (engl. *Wilcoxon signed-rank tests*) durchgeführt, da die Daten nicht normal verteilt sind. Dieser Test entspricht einem Einstichproben-t-Test, wobei die Mediane von je zwei Stichproben miteinander verglichen werden und der Vergleich dabei auf Rängen statt auf den tatsächlichen Unterschieden durchgeführt wird (Imam et al. 2014; Zimmerman und Zumbo 1993). Der Test wurde jeweils zum Vergleich der ersten Gebote mit den zweiten und letzten Geboten genutzt, sowie um die zweiten Gebote ebenfalls mit den letzten Geboten zu vergleichen. Da jeweils Unterschiede zwischen zwei Geboten untersucht wurden, mussten die sieben Teilnehmer, die nur ein Gebot angegeben haben, von dem Test ausgeschlossen werden. Die Studienteilnehmer, die zwei Gebote abgegeben haben, werden durch den Vergleich der zweiten und letzten Gebote analysiert. Die in Tabelle 5 zusammengefassten Teststatistiken zeigen, dass sich alle Gebote signifikant voneinander unterscheiden und eine große Effektstärke (r) basierend auf den Cohen-Indizes (Cohen 1992; Rosenthal 1994) aufweisen. Nach den in Tabelle 4 genannten Statistiken, beträgt der Median der ersten Gebote 25 Euro, während der Median der zweiten Gebote bei 10 Euro liegt, was einer Senkung um 40% zwischen den beiden Werten entspricht. Der Rückgang vom zweiten bis zum finalen Gebot auf 5 Euro ist mit 50% noch höher.

Tabelle 5: Statistiken der Wilcoxon-Vorzeichen-Rang Tests

	z-Wert	**p-Wert**	**N**	**Effektstärke r**
Erstes Gebot – Zweites Gebot	-5,514	,000	40	,87
Zweites Gebot – Finales Gebot	-5,912	,000	47	,86
Erstes Gebot – Finales Gebot	-5,513	,000	40	,87

Weiterhin wurde auch die Verteilung der einzelnen Gebotsreihen untersucht. Unter einer Gebotsreihe ist die Zusammenstellung des ersten, zweiten und finalen Gebotes eines Bieters gemeint. Da einige dieser Gebotsreihen deutlich höher waren als andere, wurden hierarchische Clusteranalysen mit *Median-Clustering*, *Single Linkage* und der *Ward* Methode durchgeführt, um so zu testen, ob es unterschiedliche Gruppen von Bietern gibt (Kaufman und Rousseeuw 2009; Yim und Ramdeen 2015). Da Clusteranalysen nur mit vollständigen Datensätzen arbeiten können, wurden für diese Analysen die Gebotsreihen, bei denen Werte fehlten, imputiert. In den Fällen, in denen nur ein Gebot angegeben wurde, wurden die zwei fehlenden Werte mit diesem einen Wert ausgefüllt. Die anderen Fälle, in denen zwei Gebote von den Studienteilnehmern genannt wurden, wurden mit dem zweiten Gebot ergänzt. Dies ist wiederum mit der Annahme konsistent, dass die Teilnehmer ihre wahre Wertvorstellung in ihrem finalen Gebot zum Ausdruck brachten, welches für sieben Teilnehmer eben der einzige, angegebene Wert war.

Überraschenderweise ergaben sich durch die Analysen keine klare Clusterbildung. Die sehr hohen Werte waren so stark verstreut, dass es zu Clustern mit sehr wenigen (zwischen ein und drei) Werten gekommen wäre, was zu vermeiden ist. Abbildung 8 zeigt die Verteilung der Gebotsreihen mit Hilfe eines Streudiagramms.

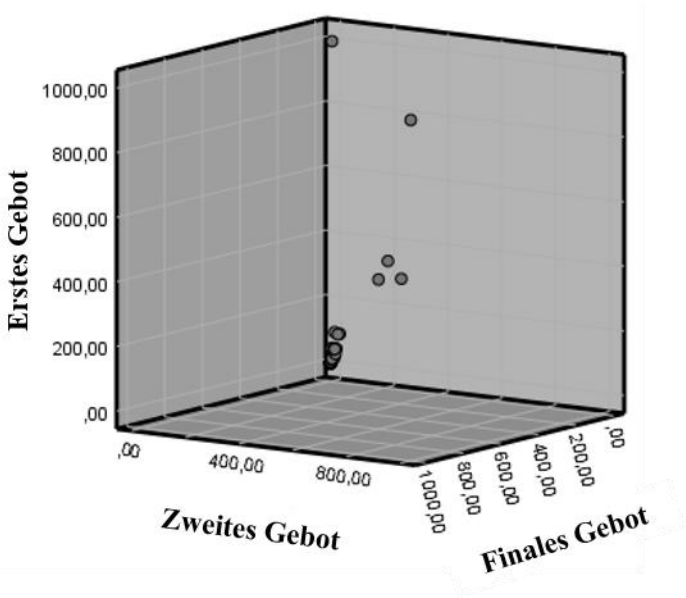


Abbildung 8: Streudiagramm aller Gebotsreihen

Um die starke Verstreuung der Gebotsreihen mit sehr hohen Werten zu reduzieren, wurden in einem zweiten Schritt neun Gebotsreihen mit sehr hohen Werten, die durch die *Single*

Linkage Clusteranalyse sowie einer z-basierten Ausreißer-Analyse identifiziert wurden, von weiteren Analysen ausgeschlossen. Diese Bieter sollten jedoch nicht als Ausreißer im traditionellen Sinne angesehen werden, da es sich hierbei um keine Messfehler handelt, sondern sie spiegeln die sehr hohe Wertvorstellung einiger der Befragten für personenbezogene Daten wider. Diese könnten daher als eine Gruppe von **„Privatsphäre-Schützern“** gesehen werden. Diese Bieter waren im Durchschnitt 25,44 Jahre alt (σ = 4,79) mit 77,78% männlichen Teilnehmern und 11,11% jeweils weiblichen Teilnehmerinnen sowie Teilnehmenden mit nicht näher bezeichneten Geschlechtern.

Eine Wiederholung der Clusteranalysen konnte nun drei verschiedene Cluster identifizieren. Abbildung 9 zeigt das Streudiagramm dieser Gebotsreihen sowie deren Zuordnung zu den drei Clustern.

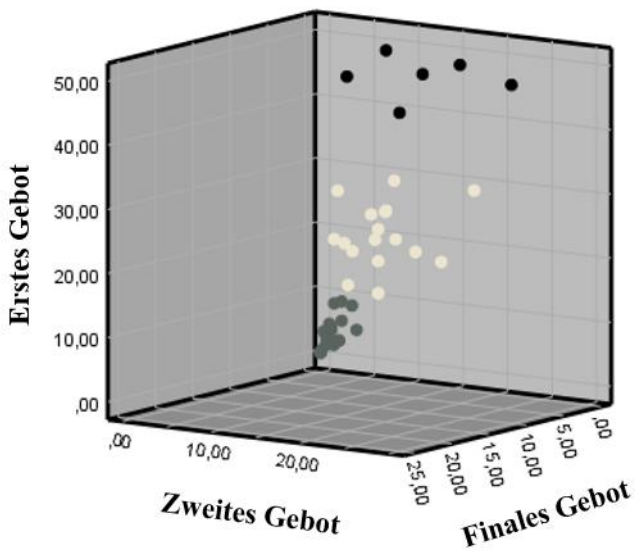


Abbildung 9: Streudiagramm der adaptierten Gebotsreihen und deren Cluster

Das erste Cluster, in der Abbildung 9 schwarz eingefärbt, zeichnet sich dadurch aus, dass alle Bieter mit 50 Euro als Erstgebot begannen. Das zweite Gebot liegt bei 20 Euro im Median und das letzte bei etwa 10 Euro, wie in Tabelle 6 dargestellt. Dieses Cluster wird daher als **„große Schritte“ Bieter** bezeichnet, da die absoluten Schritte zwischen den Geboten mit 30 Euro und 20 Euro Differenz zum nächsten Gebot größer als die der anderen Gruppen sind. Die Bieter in diesem Cluster waren im Durchschnitt 21,17 Jahre alt (σ = 1,34) und 83,33% der Gruppenzugehörigen waren männlich und 16,67% weiblich.

Während die Bieter des weißen Clusters ein ähnliches finales Gebot wie die „große-Schritte“ Bieter abgaben, betrug ihr Startgebot allerdings nur 25 Euro im Median und daher waren ihre

absoluten Schritte zwischen den Geboten im Vergleich zum vorherigen Cluster mit Wertdifferenzen von 10 Euro und 5 Euro deutlich kleiner. Daher werden sie im Folgenden als **moderate Bieter** bezeichnet. Das Durchschnittsalter dieser Bieter betrug 23,71 Jahre (σ = 3,59) und die Gruppe bestand aus 82,35% männlichen Bietern und 17,65% Bieterinnen.

Schließlich boten die Teilnehmer, die dem grauen Cluster zugeordnet sind, für alle drei Gebote vergleichsweise niedrig. Der Median des finalen Gebots in diesem **Niedrigbieter**-Cluster liegt im Median gerade bei dem Schwellenwert von 1 Euro. In dieser Gruppe waren die Bieter im Durchschnitt 23,82 Jahre alt (σ = 3,46) und das Cluster bestand aus 72,73% Männern und 27,27% Frauen.

Zur Untersuchung ob es statistische Unterschiede hinsichtlich Alter und Geschlecht der Teilnehmer zwischen den drei Gruppen sowie den Privatsphäre-Schützern gibt, wurde ein ANOVA-Test durchgeführt. Es konnten allerdings keine signifikanten Unterschiede gefunden werden.

Tabelle 6: Statistiken der hierarchischen Clusteranalyse (*Ward*-Methode) in Euro

Cluster (n)		Erstes Gebot	Zweites Gebot	Finales Gebot
Schwarz (n=6) **"große Schritte" Bieter**	**Mittelwert**	50	20,83	11,20
	Median	50	20	10
Weiß (n=17) **Moderate Bieter**	**Mittelwert**	24,16	15,41	10,01
	Median	25	15	10
Grau (n=22) **Niedrigbieter**	**Mittelwert**	4,36	2,91	1,84
	Median	4,25	2	1

Bereitschaft zur Spende von Selfies

Wie bereits im Kapitel zur Studiendurchführung beschrieben, hatten die Teilnehmer zusätzlich noch die Möglichkeit, ihre Selfies für den angegebenen Zweck zu spenden. Insgesamt entschieden sich 13 Teilnehmer für diese Option. Von diesen waren 38% weiblich, 62% männlich. Das Durchschnittsalter lag bei 24,7 Jahren (σ = 3,07). Drei dieser Spender boten Werte, bevor sie sich zum Spenden entschieden: Eine Person bot 15 Euro, bevor sie sich entschied zu spenden, eine andere Person versuchte zuerst ein 3 Euro-Gebot, und die dritte Person bot 3 Euro und sogar 1 Euro, so dass das Gebot angenommen worden wäre, wenn das Selfie nicht letztlich gespendet worden wäre. Im Folgenden werden alle Ergebnisse diskutiert und die Implikationen sowie Limitationen der Studie aufgezeigt.

5.5 Diskussion der Ergebnisse

Das Ziel dieser Studie war es, den Wert von personenbezogenen Daten aus Nutzerperspektive mit einer vielversprechenden, neuen Messmethode zu untersuchen: einer *Name-Your-Own-Price* Auktion mit wiederholter Biet-Option und Feedbackschleifen. Die folgenden Abschnitte fassen die Implikationen der Studie nochmals zusammen und beschreiben auch die Limitationen der Studie, wobei zudem weiterer Forschungsbedarf aufgezeigt wird.

5.5.1 Implikationen für die Forschung und Praxis

Die Studie ergänzt die bestehende Forschung auf verschiedenen Ebenen. Der **Hauptbeitrag für die Theorie** ist dabei die Untersuchung des Wertes, den Individuen ihren personenbezogenen Informationen zuweisen, auf eine realistische und leicht verständliche Art durchzuführen. In diesem Sinne, wurde der Ansatz einer NYOP-Auktion mit wiederholter Biet-Option genutzt, der den niedrigsten, individuellen Preis ermitteln kann (Hinz et al. 2011; Terwiesch et al. 2005). Durch die Möglichkeit, nach Erhalt von Feedback erneut bieten zu können, fühlen sich Individuen bei der Abgabe ihrer Bewertung wohler, da sie den Feilsch-Prozess als Informationsquelle nutzen können (Liu et al. 2016) und ihre Bewertung bei jedem Gebot überdenken können. Sie sind jedoch nicht zu sehr durch preisgegebene Informationen verankert, da kein Referenzpreis als Ausgangspunkt für das Bieten angegeben wird (Tversky und Kahneman 1974). Im Gegensatz zu anderen Auktionen können Verkäufer in NYOP-Auktionen mit wiederholter Biet-Option strategisch mit einem höheren, intern generierten Wert beginnen und sich dann sequentiell ihrer eigenen, niedrigsten Wertvorstellung auf Grundlage des Feedbacks annähern (Hann und Terwiesch 2003), wodurch die tatsächliche Verkaufsbereitschaft der Individuen offenbart wird.

Die Methode passt daher gut zu der vagen Vorstellung der Individuen, wie viel ihre personenbezogenen Daten wert sind und erleichtert den Prozess der individuellen Wertermittlung. Dies ist wichtig, zumal die qualitative Vorstudie zeigen konnte, dass Personen durchaus Schwierigkeiten haben, ihren Wert für personenbezogene Daten unvermittelt anzugeben. Obwohl die meisten Befragten am Ende einen Wert nannten, drückten sie ihre kognitiven Herausforderungen bezüglich der Aufgabe, bei der sie keine Möglichkeit hatten Feedback zu erhalten, deutlich aus.

Die weiteren durchgeführten Analysen zeigen zusätzliche Implikationen auf. So fällt auf, dass bis auf sieben Teilnehmer, die nur einen Wert angaben, die meisten Bieter die Chance genutzt haben, zweimal oder dreimal zu bieten. Die drei Gebote unterschieden sich auch deutlich

voneinander und sanken vom ersten bis zum zweiten Gebot um 40% und vom zweiten zum finalen Gebot um weitere 50%. Eine detailliertere Analyse der Verteilung der Gebotsreihen zeigt einige verstreute, sehr hohe Gebotsreihen, die als Gruppe der Privatsphäre-Schützer bezeichnet werden können, sowie drei weitere Cluster von Bietern mit ähnlichen Bewertungen. So konnten auch einige sehr niedrige Gebote von 1 Euro im Median innerhalb des Clusters der Niedrigbieter gesehen werden. Diese machen 41% der Gebotsreihen aus. Weitere zwei Cluster, die moderaten Bieter (31% der Bieter) und die "große Schritte" Bieter (11%), kamen beide zu einem finalen Gebot von 10 Euro im Median, unterschieden sich aber durch ihre Gebotsstrategien: Während die Gebotsreihe im "große Schritte" Bieter-Cluster mit einem höheren Gebot von 50 Euro beginnt, sind die Gebotsreihen im moderaten Cluster gemäßigter und beginnen nur mit 25 Euro im Median.

Weiterhin zeigen die Ergebnisse, dass 39% der Teilnehmer bereit waren, ein Selfie zu verkaufen oder zu spenden. Die 13 Spenden demonstrieren, dass diese Teilnehmer an den guten Zweck der Kampagne zu glauben scheinen und eine finanzielle Entschädigung nicht erforderlich ist. Es kann davon ausgegangen werden, dass die drei Personen, die zuerst Gebote abgegeben und sich dann für eine Spende entschieden haben, empfanden, dass der Schwellenwert es nicht wert ist und die Kampagne dann lieber durch eine Spende unterstützen wollten.

Darüber hinaus zeigt die Studie, dass die Teilnehmer ihre Selfies für 5 Euro im Median verkaufen würden. Dieser monetäre Wert scheint angemessen zu sein, da aktuelle Fotoverkaufsplattformen ihren Nutzern etwa 5 Euro für ein Bild anbieten. Candidly Images und Foap beispielsweise sind Marktplätze, auf denen normale Hobbyfotografen ihre Fotos an Interessenten verkaufen können (Candidlyimages 2018; Foap 2018). Die Fotos werden auf diesen Plattformen für 10 US-Dollar verkauft, wobei der Verkäufer 5 US-Dollar Vergütung erhält, was 4,38 Euro basierend auf dem Wechselkurs im Dezember 2018 entspricht. Es zeigt sich also, dass es tatsächlich ein Preis ist, bei dem Nachfrage und Angebot zustande kommen.

Es kann also konkludiert werden, dass die Verkaufsbereitschaft der Teilnehmer in dieser Feldstudie realistisch, aber aufgrund der verstreuten, hohen Werte und der drei verschiedenen Cluster gleichzeitig sehr individuell ist. Dies zeigt, dass die Wertermittlung personenbezogener Daten in Bezug auf die Privatsphäre sehr sensibel, kontextspezifisch und individuell ist, wodurch sie unter Personen kaum generalisierbar ist.

Über die theoretischen Implikationen hinaus liefert die Studie auch **praktische Beiträge**. Schließlich ist die Untersuchung des Wertes, den Individuen ihren personenbezogenen Daten

zuweisen, nicht erst seit dem Vorschlag der Bundeskanzlerin Angela Merkel, zur Besteuerung des Verkaufes personenbezogener Daten ein wichtiges Thema (DW 2018). Bereits 2014 wies Jentzsch darauf hin, dass in dieser Zeit eine wahrheitsgetreue Bewertung personenbezogener Daten wichtig ist, da immer mehr Online-Plattformen den Verkauf personenbezogener Daten an Unternehmen ermöglichen (Jentzsch 2014). Tatsächlich entstehen, wie bereits in dieser Arbeit erwähnt, immer mehr Plattformen auf denen Nutzer ihre personenbezogenen Daten aktiv an interessierte Unternehmen verkaufen können (Brustein 2012; Haberer und Schnurr 2018). In diesem Sinne trägt die Studie zur Praxis bei, indem sie einen Mechanismus bereitstellt, der die Messung der individuellen, niedrigsten Wertvorstellung personenbezogener Daten von Individuen fördert und damit Anbietern von Datenverkaufsplattformen helfen kann, ihre Preise zu bewerten sowie die Geschäftsmöglichkeiten einzuschätzen. Auf diese Plattformen wird in dem nächsten Kapitel noch genauer eingegangen.

Eine zweite, praktische Implikation dieser Studie ergibt sich aus der Tatsache, dass Internetnutzer, wenn sie soziale Netzwerke wie Facebook oder Instagram verwenden, zustimmen, dass das Unternehmen die Lizenz zur Nutzung aller hochgeladenen Bilder erhält (Facebook 2018; Instagram 2018). So nutzen Individuen einen scheinbar kostenlosen Service, bezahlen aber mit ihren personenbezogenen Daten, in diesem Falle, mit ihren Fotos und ihrem Nutzerverhalten. In diesem Sinne könnte argumentiert werden, dass soziale Netzwerk-Nutzer ihre Fotos nicht wertschätzen, da sie diese kostenlos zur Verfügung stellen. Die Ergebnisse dieser Studie belegen jedoch, dass für Individuen ihre Fotos tatsächlich einen Wert über den kostenlosen Service hinaus haben.

5.5.2 Limitationen und weiterer Forschungsbedarf

Im Folgenden werden die Limitationen der Studie behandelt sowie Möglichkeiten für zukünftige Forschung aufgezeigt. Die erste Limitation betrifft die Stichprobe der Studie: Aufgrund der Geschlechterverteilung der technologieorientierten Universität an der die Studie durchgeführt wurde, bestand das Sample aus mehr männlichen als weiblichen Teilnehmern. Zukünftige Forschung könnte die Studie also mit einem ausbalancierteren Sample wiederholen, zumal in den Daten eine Tendenz zu erkennen war, dass Frauen eher spendenwillig waren, wobei diese Tendenz mit diesem Sample nicht signifikant war.

Zweitens, sind, wie durch die Zusammenfassung bestehender Forschung in Kapitel 4 gezeigt, Studien zur Bewertung personenbezogener Daten sehr kontextsensitiv. Das bedeutet, dass die

Bereitschaft zum Verkauf personenbezogener Daten und der tatsächlich geforderte Wert stark von den Umständen abhängen, unter denen die Studie durchgeführt wurde. In der vorliegenden Studie wurde versucht diese Umstände in vielerlei Hinsicht zu optimieren: So wurde in leicht verständlicher Weise angegeben wer, welche Daten, für welchen Zweck kauft und es waren keine komplexen Partnerstrukturen involviert, sondern die Universität war die einzige Käuferpartei, was bereits in anderen Wert-von-Daten-Studien erfolgreich umgesetzt wurde (z.B. Barak et al. 2013; Cvrcek et al. 2006; Danezis et al. 2005). Zudem ist es ein realistisches und Anreiz-gebendes Experiment, welches zu keinen hypothetischen Verzerrungen geführt hat. Nichtsdestotrotz könnte es interessant sein, eine NYOP-Auktion mit wiederholter Biet-Option noch in anderen Kontexten durchzuführen, um die Übertragbarkeit der Ergebnisse zu verbessern.

Die dritte Limitation ergibt sich daraus, dass die Studie mit einer deutschen Stichprobe durchgeführt wurde und dadurch die Verallgemeinerbarkeit der Studienergebnisse für andere Kulturen eingeschränkt ist. Allerdings zeigen die Studienergebnisse auch, dass bereits die deutschen Teilnehmer, die sich im internationalen Vergleich besonders viele Gedanken um ihre Privatsphäre machen (Krasnova et al. 2012), überfordert sind, wenn sie aufgefordert werden, ihre individuelle Verkaufsbereitschaft für personenbezogene Daten zu nennen. Daher sollten die Ergebnisse für andere Kulturen, in denen die Menschen weniger datenschutzbewusst sind und daher über eine geringere Expertise auf dem Gebiet der Bewertung personenbezogener Daten in Bezug auf Privatsphäre verfügen, ebenfalls gelten.

6 Eine Untersuchung von Einflussfaktoren auf die Bereitschaft personenbezogene Informationen auf Datenverkaufsplattformen zu verkaufen[8]

Wie die beiden vorausgegangenen Kapitel, untersucht auch die im Folgenden vorgestellte Studie die Bereitschaft von Internetnutzern personenbezogene Informationen über sich zu verkaufen. Nachdem im 5. Kapitel bereits eine neue Methode zur Messung des Wertes angewendet wurde, wird nun mit Datenverkaufsplattformen ein vielversprechender, bislang nicht für den Wert von Daten erforschter Kontext untersucht. Dabei werden insbesondere die Faktoren analysiert, welche die Wertvorstellung der Individuen zum Verkauf auf solchen Plattformen beeinflussen können. Auf praktischer Ebene wird damit einhergehend auch untersucht, ob Datenverkaufsplattformen von Nutzern adoptiert werden würden, die dann wiederum als alternatives Geschäftsmodell neben Datenmarktplätzen als neue Datenpraktik angesehen werden könnten.[9]

6.1 Motivation und Relevanz

"In 2012, advertising revenue in the United States was around $30 billion. That same year, I made exactly $0 from my own data. But what if I tracked everything myself? Could I at least make a couple bucks back?"

Frederico Zannier (2013)

Mit diesen Worten motivierte Federico Zannier im Jahr 2013 seine Kickstarter-Kampagne, bei der er verschiedenste Arten von Informationen über sein Online-Leben sammelte und für 2 US-Dollar pro Tag zum Verkauf anbot. Dabei bewarb er sein Crowdfunding-Projekt mit Ausführungen wie: *"I've data mined myself. I've violated my own privacy. Now I am selling it all. But how much is it worth?"* (Zannier 2013). Nach eigener Aussage war es sein erklärtes Ziel, mit dem Crowdfunding-Geld eine Browsererweiterung und eine App zu entwickeln, um es so auch anderen Internetnutzern ermöglichen zu können, ihre Daten an Interessierte zu verkaufen. Am Ende konnte sein Crowdfunding-Ziel von 500 US-Dollar mit Einnahmen von über 2700 US-Dollar weit übertroffen werden.

[8] Dieses Kapitel basiert auf Wessels et al. (2019a)

[9] Die Untersuchung von Datenverkaufsplattformen als Ansatz für alternative Datenpraktiken wird in dieser Arbeit nicht aus juristischer Perspektive vorgenommen.

Dabei ist Federico Zannier nicht der Einzige, der die gängigen Praktiken im Umgang mit personenbezogenen Daten überdenkt. Wie in dieser Arbeit bereits dargelegt, haben verschiedene Initiativen begonnen nach alternativen Ansätzen für das Geschäft mit Daten zu suchen, um die Dateneigentümer an dem Wert, den ihre Daten schaffen können, teilhaben zu lassen. Insbesondere die Idee des aktiven, von Individuen selbst initiierten Datenverkaufs hat in den letzten Jahren für Aufmerksamkeit gesorgt. So entstanden immer mehr Unternehmen mit ähnlichen Geschäftsmodellen rund um die Grundidee, Plattformen bereitzustellen, auf denen Individuen selbstbestimmt und gegen eine monetäre Vergütung ihre Daten an Interessierte weitergeben können (Brustein 2012).

Dies ist ein interessanter Ansatz für alternative Geschäftsmodelle, der auch vor dem Hintergrund der Erforschung des Wertes, den Individuen ihren personenbezogenen Daten zuweisen, vielversprechend ist und daher näherer Untersuchung bedarf. Schließlich sind Datenverkaufsplattformen nur für den Zweck des Verkaufes personenbezogener Nutzerdaten entwickelt worden und stellen damit genau den Forschungskontext dar, der den bereits vorgestellten Studien zur Ermittlung des Wertes von Daten durch Analyse ihrer Verkaufsbereitschaft zugrunde liegt. Daher können sie als eine natürliche Forschungsumgebung dienen, um die Verkaufsbereitschaft von Individuen und ihre Einflussfaktoren zu untersuchen.

In der bisherigen Forschung wurde dieser Kontext allerdings noch nicht zur Untersuchung des Wertes von Daten angewandt. Vielmehr stützen sich frühere Studien, wie bereits im 4. Kapitel erläutert, oft auf recht künstlich generierte, experimentelle Settings oder speziell für die Studien entwickelte Forschungskontexte, wie beispielsweise die Auktion zur Versteigerung von Logiktest-Resultaten von Jentzsch (2014) oder die Untersuchung von Bauer et al. (2012) zur Messung des Geldwertes, den die Teilnehmer zahlen würden, um ihre Daten vor der Löschung von Facebook zu bewahren, demonstrieren. Diese unterschiedlichen Kontexte tragen, wie in den vorangegangenen Kapiteln dieser Arbeit bereits erläutert, zu einer großen Varianz der Ergebnisse bei. So liefern bisherige Studien zur Untersuchung des monetären Wertes personenbezogener Daten zwar wertvolle Erkenntnisse, jedoch sind diese spezifisch für den jeweiligen Untersuchungskontext und daher ist es schwierig die Ergebnisse von einem Kontext auf einen anderen zu übertragen. Dies macht es notwendig, vielversprechende Kontexte, wie den der Datenverkaufsplattformen, in separaten Studien zu analysieren.

Vor diesem Hintergrund zielt diese Studie darauf ab, die Bereitschaft von Individuen, eigene personenbezogene Informationen auf Datenverkaufsplattformen zu veräußern, zu untersuchen. Dabei soll besonders auf die Faktoren eingegangen werden, die diese Verkaufsbereitschaft beeinflussen. Schließlich konnten im 4. Kapitel dieser Arbeit bereits eine Reihe von Einflussfaktoren als Treiber für den Wert personenbezogener Daten identifiziert werden. Während die Verkaufsbereitschaft Rückschlüsse bezüglich des monetären Wertes, den Individuen Daten zuweisen, ermöglicht, sind Einflussfaktoren von theoretischem Wert, da sie die Indikatoren repräsentieren, die zu einem Anstieg oder einer Senkung der Verkaufsbereitschaft führen können (z.B. Danezis et al. 2005; Jentzsch 2014). Die Einflussfaktoren, die in früheren Forschungsstudien untersucht wurden, wurden dabei hauptsächlich deduktiv abgeleitet (z.B. Hann et al. 2007; Huberman et al. 2005; Jentzsch 2014) weswegen unklar ist, ob diese bisher untersuchten Einflussfaktoren wirklich die alleinigen und relevanten Treiber des Wertes personenbezogener Daten aus Nutzerperspektive sind. Vor dem Hintergrund, dass in der bestehenden Literatur Erkenntnisse über die Einflussfaktoren der Verkaufsbereitschaft von Nutzern auf Datenverkaufsplattformen fehlen, lautet die erste Untersuchungsfrage dieser Studie:

Welche Faktoren beeinflussen Individuen in ihrer Bereitschaft personenbezogene Informationen auf Datenverkaufsplattformen zu verkaufen?

Zur Beantwortung dieser Untersuchungsfrage wurde zunächst eine induktive Studie unter 49 Internetnutzern durchgeführt, um die aus Nutzerperspektive bedeutendsten Einflussfaktoren der Verkaufsbereitschaft auf Datenverkaufsplattformen zu untersuchen. Während diese qualitative Studie wertvoll zur Identifikation von den relevanten Einflussfaktoren ist, kann diese noch keine Erkenntnisse darüber liefern, ob Individuen manchen der Faktoren eine höhere Wichtigkeit beilegen als anderen. Die relativen Wichtigkeiten der einzelnen Einflussfaktoren sind allerdings für ein besseres Verständnis notwendig, um die individuelle Verkaufsbereitschaft bestimmen zu können. Darüber hinaus ist dies auch aus Praxissicht von besonderem Interesse, um herauszufinden was die individuelle Verkaufsbereitschaft antreibt. Daher lautet die zweite Untersuchungsfrage:

Welche relativen Wichtigkeiten ordnen Individuen einer Auswahl von Einflussfaktoren auf ihre Bereitschaft, Daten auf Datenverkaufsplattformen zu verkaufen, zu?

Diese Frage soll mithilfe einer zweiten Studie, einer Conjoint-Analyse unter 250 Internetnutzern, untersucht werden. Auf die Auswahl der Einflussfaktoren sowie die Gründe zur Eingrenzung wird im späteren Verlauf dieses Kapitels noch genauer eingegangen. Zur

weitergehenden Analyse der von den Teilnehmern der Studie geäußerten Präferenzen bezüglich der Einflussfaktoren dahingehend, ob alle ähnliche relative Wichtigkeiten empfinden oder ob es zwischen den Teilnehmern Unterschiede gibt, wird eine ergänzende Untersuchung der Conjoint-Analyse-Ergebnisse vorgenommen. Dazu soll auf Grundlage der CA-Ergebnisse eine *Latent Class Analyse* durchgeführt werden, um so die dritte Untersuchungsfrage beantworten zu können:

Gibt es unter den Teilnehmern Gruppen mit ähnlichen Präferenzmustern?

Diese Studie untersucht also in einem zweistufigen Prozess zunächst qualitativ die Einflussfaktoren auf die Bereitschaft von Individuen, Informationen auf Datenverkaufsplattformen zu veräußern, sowie mit einer Conjoint-Analyse die relativen Wichtigkeiten einer Auswahl dieser Faktoren. Weiterhin wird auf Grundlage der Resultate der Conjoint-Analyse eine Segmentierungsanalyse vorgenommen, um Gruppen mit ähnlichen Präferenzmustern zu identifizieren. Die theoretischen Implikationen für die Forschung sind dabei dreigeteilt: Erstens, wird ein verständlicher Überblick über die Einflussfaktoren auf die Verkaufsbereitschaft von Individuen auf Datenverkaufsplattformen gegeben und dabei aufgezeigt, wie vielschichtig diese Einflussfaktoren sind. Es konnten dabei drei Faktoren identifiziert werden, die bislang durch die deduktive Forschung noch nicht thematisiert wurden. Zweitens, wurde die relative Wichtigkeit von einer Auswahl an Einflussfaktoren untersucht, wobei die Kompensationshöhe, der Datentyp und die Herkunft des Plattformbetreibers die Wichtigsten waren. Die Segmentierungsanalyse konnte allerdings auch zeigen, dass es sehr wohl unterschiedliche Gewichtungen der Wichtigkeiten zwischen den vier identifizierten Gruppen gibt. Weiterhin konnten drei andere Faktoren als Knock-out-Kriterien identifiziert werden, die von potenziellen Kunden einer Datenverkaufsplattform kompromisslos gefordert wurden: keine Weitergabe an Dritte, das Recht auf Löschung und die Einmaligkeit des Geschäftes.

Diese theoretischen Erkenntnisse helfen darüber hinaus auch Anbietern von Datenverkaufsplattformen. Diese können aufgrund der Ergebnisse dieser Studie ihr Webseiten-Design anpassen und die Wünsche ihrer potenziellen Nutzer besser adressieren, um so letztlich ihren Erfolg zu erhöhen. So könnten Kunden auch stärker in den Datenverarbeitungsprozess involviert werden, indem sie eine aktivere Rolle einnehmen und somit bei der Kommerzialisierung von Daten mitprofitieren könnten.

Im weiteren Verlauf dieses Kapitels wird zunächst kurz auf die theoretischen Grundlagen zu der relevanten Privatsphäre-Forschung eingegangen und im Folgenden verschiedene

Datenverkaufsplattformen detaillierter vorgestellt. Danach wird nochmals kurz ein Überblick über den zweistufigen Prozess gegeben, bevor die Untersuchungsschritte eins und zwei dann jeweils mit ihren Methoden und Ergebnissen vorgestellt werden. Schließlich folgt eine Diskussion der Ergebnisse mit den Limitationen und weiteren Forschungsbedarfen.

6.2 Grundlagen zur Wert-von-Daten-Forschung und zu Datenverkaufsplattformen

6.2.1 Forschung zum Wert von Daten

Wie bereits in den beiden vorausgehenden Kapiteln beschrieben, hat die Forschung zur Ökonomie von Privatsphäre schon vor über einer Dekade begonnen die Zahlungsbereitschaft für Datenschutz sowie die Verkaufsbereitschaft von personenbezogenen Informationen zu untersuchen, um den Wert, den Individuen ihrer Privatsphäre zuweisen, messen zu können. Wie sich zeigte, variieren die Ergebnisse dieser recht heterogenen Studien dabei deutlich und werden von verschiedenen Faktoren, die den Kontext der Studien bilden, beeinflusst. Die verschiedenartigen Ergebnisse dieser Untersuchungen deuten darauf hin, dass es dabei nicht möglich ist, die Resultate einfach von einem Kontext auf einen anderen zu übertragen.

Wie bereits in dieser Arbeit dargelegt, haben sich die bestehenden Studien jedoch in der Regel auf deduktive Ansätze gestützt, um die mutmaßlichen Einflussfaktoren auf den Wert von personenbezogenen Daten zu bestimmen (z.B. Hann et al. 2007; Hann et al. 2002). Dabei ist allerdings nicht klar, ob es sich um diejenigen Faktoren mit den größten Auswirkungen aus Sicht der Individuen handelt. Weiterhin haben diese früheren Studien jeweils nur eine begrenzte Anzahl von Einflussfaktoren ausgewählt, die in ihre Untersuchungen einbezogen wurden. Beispiele hierfür sind die Konzentration auf die Identifizierung (Jentzsch 2014) oder auf den Verwendungszweck und den Grad der Sensitivität (Danezis et al. 2005). Problematisch an diesem Ansatz ist, dass nicht bekannt ist, ob diese untersuchten Determinanten alle Einflussfaktoren vollständig umfassen, die aus Sicht der Nutzer von Bedeutung sind und welche unkontrollierten Auswirkungen weggelassene Faktoren auf die Ergebnisse hätten haben können. Um dies abfangen zu können, werden in dieser Studie die Einflussfaktoren mit Hilfe einer qualitativen Studie induktiv erhoben und zudem der neuartige Kontext der Datenverkaufsplattformen gewählt, der zur Untersuchung der Zahlungsbereitschaft für Daten prädestiniert ist. Im folgenden Unterkapitel werden einige Grundlagen zu diesen Datenverkaufsplattformen gegeben.

6.2.2 Datenverkaufsplattformen

Wie bereits beschrieben, sind Datenverkaufsplattformen so konzipiert, dass Individuen eine Umgebung bereitgestellt wird, auf der sie ihre Daten auf möglichst natürliche Weise verkaufen können. Damit bieten sie einen interessanten und reinen Forschungskontext für Untersuchungen der Verkaufsbereitschaft von Daten, der frei von Störfaktoren ist, welche den Wert, den Individuen ihren personenbezogenen Informationen beimessen, verzerren könnten.

Datenverkaufsplattformen teilen dabei die Grundidee, dass Internetnutzer ihre personenbezogenen Daten im Austausch gegen monetäre Vorteile wie Rabatte oder Geldwerte weitergeben können. Der Pionier unter den Plattformen ist das amerikanische Unternehmen Datacoup. Der Anbieter ermöglicht es Benutzern, ihre bestehenden Konten sozialer Netzwerke, Bankkonten oder sogar Fitness Tracker in seine Webseite einzubinden und die zugehörigen Daten wöchentlich direkt an die Plattform zu verkaufen (Datacoup 2018). Nach eigenen Angaben plant Datacoup das Konzept so auszubauen, dass Individuen ihre Daten zukünftig direkt an Unternehmen veräußern können, sobald es einen größeren Nutzer- und Firmenstamm gibt (Datacoup 2018). Auch der deutsche Anbieter Data Fairplay plant einen Marktplatz zu etablieren, auf dem interessierte Unternehmen relevante Datensätze beispielsweise für personalisierte Werbung anfragen und Preisangebote unterbreiten können (DataFairplay 2018). Ihr Konzept sieht vor, dass Data Fairplay dabei als Intermediär auftritt und die Angebote der Unternehmen an geeignete Nutzer weiterleitet, die diese annehmen oder ablehnen können. Die Plattform befindet sich in einem frühen Stadium, in der sie um die Unterstützung von interessierten Personen und Partnerunternehmen wirbt. Darüber hinaus gibt es einige neuere Plattformen wie Datawallet und Datum.org, die auf *Smart Contracts* und *Blockchain*-Technologie setzen, um den Zugriff auf die Daten ihrer Nutzer zu ermöglichen. Die nachfolgende Tabelle 7 fasst diese und weitere derzeit bekannte Datenverkaufsplattformen und ihre Funktionsweisen zusammen.

Tabelle 7: Überblick über aktuell bekannte Datenverkaufsplattformen

Unternehmen (Gründungsjahr)	Beschreibung des Geschäftsmodell-Ansatzes
Digi.me (2009)	Benutzer von digi.me können Konten verschiedener Dienste (z.B. soziale Netzwerke, Banken, Fitness) miteinander verbinden und digi.me sammelt alle Informationen von diesen Konten in einer Bibliothek, die es den Benutzern ermöglicht, ihre Informationen einzusehen und zu teilen (digi.me 2018). Wenn die Benutzer ihre Zustimmung geben, können andere Apps, Dienste und Unternehmen auf Teile dieser Benutzerbibliotheken zugreifen (digi.me 2018).
Infoscout (2011)	Infoscout gibt es in zwei verschiedenen Varianten: Receipt Hog und Shoparoo. Beide basieren auf dem Prinzip, dass die Nutzer ihre Einkaufsbelege und Quittungen mit den Apps scannen können, und für diese, abhängig von dem Händler des Beleges, Vorteile erhalten (FastCompany 2016). Im Fall von Receipt Hog werden die Datenpreisgebenden mit virtuellen Münzen und der Teilnahme an weiteren Gewinnspielen kompensiert (ReceiptHog 2018). Sobald eine bestimmte Anzahl an Münzen gesammelt ist, können diese gegen PayPal-Guthaben, Amazon-Geschenkkarten oder Zeitschriftenabonnements eingelöst werden (ReceiptHog 2018). Die Quittungsdaten sowie optionale Umfrageergebnisse werden nach Angaben des Unternehmens anonymisiert in Marktforschungsberichten zusammengefasst und verkauft (ReceiptHog 2018). Im Fall von Shooparoo werden die hochgeladenen Quittungen in Spendensammlungen umgewandelt, beispielsweise für Schulen (Shoparoo 2018).
Datacoup (2012)	Datacoup verbindet verschiedene Konten und die dahinterliegenden Daten um ein Profil zu bilden, das derzeit von Datacoup direkt gekauft wird (Datacoup 2018). Die Plattform zeigt wöchentlich den zusammengefassten Preis für das Teilnehmerprofil an (Datacoup 2018). Kaufende Unternehmen haben Zugriff auf einen Pool von aggregierten, anonymen Datacoup-Benutzerdaten (Datacoup 2018).
Meeco.me (2012)	Das australische Start-Up ist eine Art Marktplatz für Daten (meeco.me 2018). Individuen können darüber ihre personenbezogenen Daten verschlüsselt speichern und den Zugriff verwalten, indem sie kontrollieren, an wen die Daten weitergegeben werden, um auf diese Weise Wert generieren zu können (meeco.me 2018).

Data Fairplay (2014)	Mit Data Fairplay soll ein Marktplatz geschaffen werden, auf dem Individuen ein Profil über sich pflegen können, beispielsweise mit Lieblingsmarken, Interessen, Kleidungsgrößen und Arbeitszeiten (DataFairplay 2018). Interessierte Unternehmen können passende Datensets anfragen und wenn Individuen das Angebot der Unternehmen annehmen, findet die Weitergabe der Daten statt (DataFairplay 2018).
Datawallet (2014)	Datawallet ist ein digitales Wallet für Online-Daten (Datawallet 2018). Es ermöglicht seinen Nutzern Daten von Plattformen wie Facebook, Amazon, Uber und Spotify gebündelt an einem Ort zu verwalten (Datawallet 2018). Die Nutzer können dabei bestimmen, wer Zugriff auf die Daten erhält, erfahren, was die Daten aussagen und werden für die Weitergabe der Daten bezahlt (Datawallet 2018).
Datum.org (2016)	Die Nutzer übermitteln ihre personenbezogenen Daten an eine *Blockchain*, auf welcher die Daten sicher und dezentral abgespeichert werden (Haenni 2017). Der *DAT-Smart-Token* ermöglicht die Option des Verkaufes und Kaufes von gespeicherten Daten zu den individuellen Bedingungen des Datenbesitzers (Haenni 2017).
Wibson (2017)	Wibson ist ein *Blockchain*-basierter, dezentraler Datenmarktplatz, der es Individuen ermöglicht private Informationen, wie beispielsweise Facebook-Konten und Standortdaten, anonym gegen Wibson-*Token* zu verkaufen (Wibson 2018). Wibson-*Token* sind eine Art von Kryptowährung, die in der *Blockchain* erstellt und verschlüsselt gespeichert werden (Wibson 2018).
Ocean Protocol (2017)	Ocean Protocol ist eine *Token*-basierte Service-Schicht, die es ermöglicht Daten, insbesondere für die Künstliche Intelligenz (KI), frei zu setzen und durch die *Blockchain*-Technologie sicher und transparent zu speichern, auszutauschen und zu verkaufen, wobei der Datenbesitzer jeden Datensatz kontrollieren kann (OceanProtocol 2018). In das Ocean Protocol können mehrere Datenmarktplätze eingebunden werden, die Datenanbieter und Unternehmen verbinden (OceanProtocol 2018).

6.3 Zweistufiges Studiendesign

Um die drei vorgestellten Untersuchungsfragen beantworten zu können, wurden Untersuchungen im Rahmen eines zweistufigen Studiendesigns angewandt. Im **ersten Untersuchungsschritt** wurde eine qualitative Studie durchgeführt, um so zu erforschen, welche Faktoren die Verkaufsbereitschaft von personenbezogenen Daten auf Datenverkaufsplattformen beeinflussen. Dieser induktive Ansatz hat den Vorteil, dass identifiziert werden kann, welche Faktoren für potenzielle Nutzer wirklich wichtig sind, während sich die bestehende Literatur bei der Untersuchung des Wertes von Daten in der Regel auf deduktiv abgeleitete Einflussfaktoren stützt. Mit Hilfe dieses induktiven Ansatzes wird das Risiko, dass relevante Faktoren vernachlässigt werden, die sich jedoch durchaus auf die Bewertung personenbezogener Daten auswirken können, gemindert.

Die induktiv identifizierten Einflussfaktoren dienen als Grundlage für den **zweiten Untersuchungsschritt**, eine auswahlbasierte Conjoint-Analyse (engl. *Choice-based Conjoint Analysis* (*CBCA*)), welche die relativen Wichtigkeiten ausgewählter Einflussfaktoren untersucht, indem die Faktoren als Attribute der Conjoint-Analyse dienen. Darüber hinaus werden mit Hilfe der *Latent Class Analyse* Gruppen mit ähnlichen Präferenzmustern identifiziert. Abbildung 10 fasst diese beiden Untersuchungsschritte graphisch zusammen.

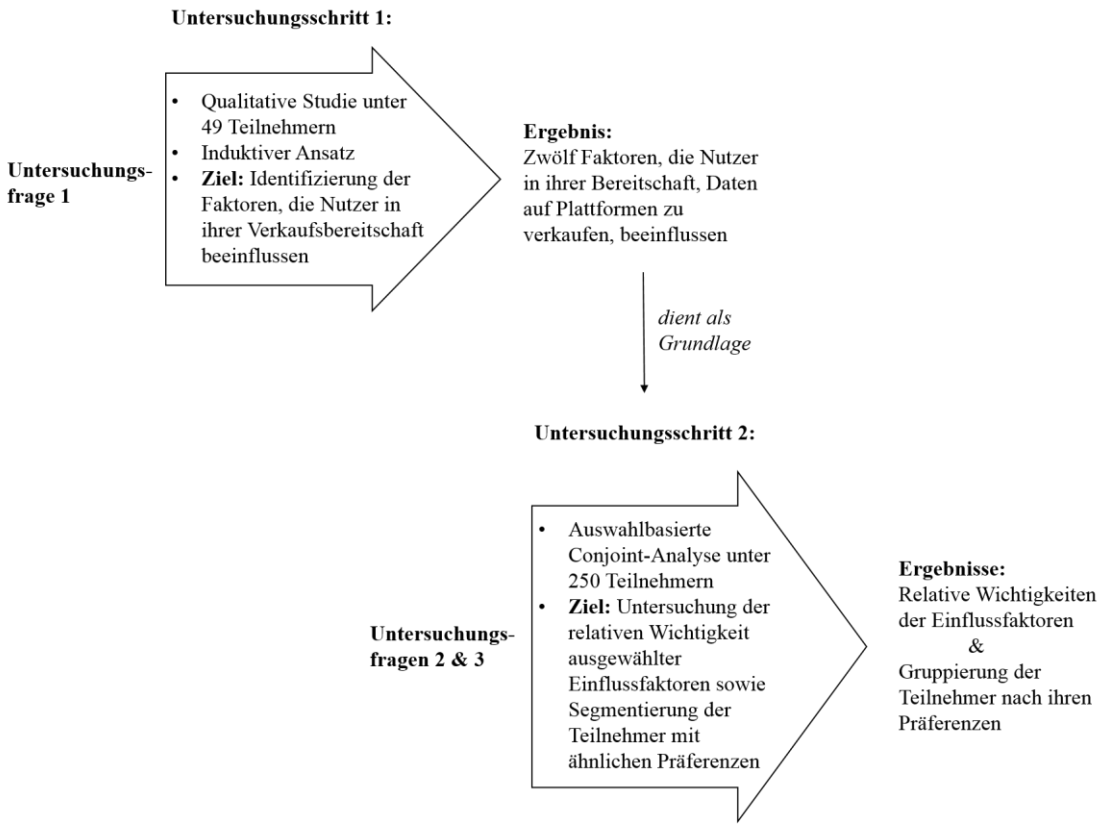


Abbildung 10: Überblick des zweistufigen Studiendesigns

Im weiteren Verlauf dieser Arbeit wird zunächst der erste Untersuchungsschritt mit seiner Methodik und den Ergebnissen vorgestellt bevor im weiteren Verlauf auf die zweite Untersuchungsstudie eingegangen wird.

6.4 Erster Untersuchungsschritt: Qualitative Studie

6.4.1 Methodik

Wie bereits beschrieben, zielt der erste Untersuchungsschritt darauf ab, die Faktoren zu identifizieren, die Individuen in ihrer Bereitschaft personenbezogene Daten zu verkaufen, beeinflussen. Es wurde dabei ein induktiver Ansatz gewählt, da die aus Nutzerperspektive wirklich relevanten Faktoren gefunden werden sollen. Dies macht ein besonders sorgfältiges Vorgehen bei der Definition der Zielpopulation für diesen Untersuchungszweck notwendig: Da Internetnutzer die wahrscheinlichste Nutzergruppe von Datenverkaufsplattformen sind, wurde darauf geachtet, dass das Sample aus Individuen besteht, die hinsichtlich Alter und Geschlecht repräsentativ für Personen sind, die das Internet häufig nutzen (Statista 2014a; Statista 2014b).

Zur Durchführung des ersten Untersuchungsschrittes wurde eine Onlineumfrage mit Mockups und offenen Fragen entwickelt. Die Mockups wurden angefertigt, um den Teilnehmern ein adäquates Wissen über die Funktionsweise von Datenverkaufsplattformen vermitteln zu können, was wichtig ist, da Datenverkaufsplattformen gegebenenfalls noch unbekannt sind und daher eine Erklärung notwendig ist. Weiterhin brachten die Mockups den Vorteil mit sich, dass alle Teilnehmer bei der Beantwortung der Fragen ein einheitliches Bild einer Plattform im Kopf haben. Dies ist wichtig, da die bestehenden Datenverkaufsplattformen, wie im Kapitel 6.2.2 vorgestellt, alle leicht in ihrem Konzept variieren, und so eine Verzerrung durch bestimmte Eigenschaften oder das Marketing der bestehenden Plattformen verhindert werden konnte.

Die Onlineumfrage war dabei wie folgt aufgebaut: Nach einer einleitenden ersten Seite und der Abfrage von demographischen Informationen wie Alter und Geschlecht, wurde den Teilnehmern zunächst eine kurze textbasierte Erklärung zu Datenverkaufsplattformen und dem Verkaufsprozess präsentiert, die anschließend durch die Mockups noch erweitert wurden. Die Mockups zeigten die wichtigsten Inhalte einer exemplarischen Datenverkaufsplattform-Webseite (siehe Anhang 6-8). So wurde auf dem ersten Mockup zunächst die Grundidee von Datenverkaufsplattformen beschrieben: Individuen können hierbei Daten, die sie bereit sind

zu teilen, an Partner-Unternehmen verkaufen, um so stärker am Prozess des Datenhandels teilzuhaben. Das zweite Mockup zeigt exemplarisch, wie ein Datenprofil angelegt werden kann. Der Nutzer kann dabei in verschiedenen Kategorien Datentypen auswählen, die er oder sie verkaufen möchte. Nach Auswahl der Daten wird der Kompensationsbetrag präsentiert. Schließlich zeigt das dritte Mockup den Nutzer-Account mit seinem derzeitigen Kontostand, sowie auf welche Weise der Auszahlungsprozess angestoßen werden kann.

Nach den Mockups wurden den Studienteilnehmern die Hauptfrage der Studie gestellt: *Unter welchen Umständen würdest du deine Daten auf einer solchen Plattform verkaufen?*

Zur Beantwortung dieser offenen Frage konnten die Studienteilnehmer in Freitextfeldern ihre Faktoren benennen und auch eine Beschreibung dieser abgeben. Die Teilnehmer wurden aufgefordert mindestens vier Faktoren zu nennen, wenn sie wollten konnten allerdings bis zu zehn Faktoren benannt werden.

Die Studie wurde mit besonderem Fokus auf die Verständlichkeit und Eignung der Mockups, sowie die Klarheit der Hauptfrage von neun Wirtschaftsinformatik-Forschern getestet. Basierend auf diesem Feedback wurden iterativ kleinere Anpassungen vorgenommen, um die Verständlichkeit sicherzustellen.

Die qualitative Studie wurde mit Hilfe eines Marktforschungsunternehmens durchgeführt und insgesamt nahmen 63 Personen teil. Um unaufmerksame Teilnehmer identifizieren zu können, wurde ein Aufmerksamkeitstest integriert. Hierdurch wurden fünf Teilnehmer, die diesen Test falsch beantworteten, von der weiteren Analyse ausgeschlossen. Von den restlichen 58 Teilnehmern gaben neun an, dass sie es sich unter keinen Umständen vorstellen können ihre Daten auf einer solchen Plattform zu verkaufen. Auch diese wurden aus dem Datensample entfernt, sodass das finale Daten-Set aus den Antworten von 49 Teilnehmern besteht. Insgesamt setzte sich das Sample aus 21 Frauen und 28 Männern zusammen, von denen 35% zwischen 18 und 25 Jahren alt waren, weitere 35% zwischen 26 und 35 Jahren, 10% zwischen 36 und 45 Jahren, wiederum 10% zwischen 46 und 55 Jahren und die restlichen 10% älter als 56 Jahre waren. Hinsichtlich der Erwerbtätigkeitsstruktur waren mit 37% die Mehrheit der Befragten Beschäftigte, gefolgt von 29% Studierenden und 14% Arbeitslosen, 12% waren Selbstständige und 8% haben andere, nicht spezifizierte Tätigkeiten ausgeführt.

Zur Analyse der Daten wurden Kodierungstechniken basierend auf dem bereits in dem 3. Kapitel kennengelernten *Grounded Theory* Ansatz (Charmaz 2014; Glaser und Strauss 1967) gewählt. Ausgehend von dem ersten Kodieren der Daten, dem sogenannten *initial coding*,

wurden den Antworten der Teilnehmer konzeptionelle Labels (*conceptual labels*) zugefügt, um so die Faktoren zu kategorisieren, die von den Befragten beschrieben wurden. Dabei wurde sorgfältig darauf geachtet, alle genannten Faktoren zu identifizieren, welche die Verkaufsbereitschaft personenbezogener Informationen direkt beeinflussen. Allerdings wurden solche Faktoren ausgeschlossen, die lediglich anbieterspezifisch sind und somit für mehrere Arten von Plattformen gelten. Beispiele hierfür sind der Aufwand zur Eingabe der Daten oder die Empfehlung der Plattform durch Freunde oder Kollegen. Solche Faktoren beeinflussen nicht direkt die Verkaufsbereitschaft von Informationen und wurden somit nicht weiter analysiert.

Anschließend wurden die Codes der ersten Kodierung nach ähnlichen Bedeutungen gruppiert und, sofern sinnvoll, unter einem breiteren, konzeptuellen Label zusammengefasst. Die Faktoren wurden dabei von drei Forschern unabhängig voneinander kodiert, jedoch wurden die Kodierungsprinzipien in den verschiedenen Runden untereinander diskutiert und zusammengefasst beziehungsweise angepasst. Schließlich konnten die finalen Faktoren mit jeweils eindeutigen Beschreibungen fixiert werden.

6.4.2 Ergebnisse

Wie bereits angeführt, wurden neun Teilnehmer von der Stichprobe ausgeschlossen, da sie angaben, dass sie unter keinen Umständen bereit wären Daten auf einer solchen Plattform zu verkaufen und daher auch keine Faktoren benennen konnten, die ihre Verkaufsbereitschaft beeinflussen. Eine Teilnehmerin begründete ihre Ablehnung dabei wie folgt: *„Ich wäre nicht bereit meine Daten online zu verkaufen, auch wenn mir bewusst ist, dass aktuell andere Unternehmen Geld mit meinen Daten verdienen und sie ohnehin im Umlauf sind. Es widerspricht meinen Prinzipien, es ist schlimm genug, dass man nicht mehr im Internet unterwegs sein kann, ohne dass jeder Verlauf, jede Information gesammelt und verarbeitet wird.“* Interessanterweise war die Mehrheit der Ablehner weiblich, während nur ein männlicher Teilnehmer sich dagegen aussprach. Weiterhin waren die meisten Ablehner zwischen 36 und 45 Jahren (66%) und damit im "mittleren Lebensalter", während 22% etwas jünger waren (26-35 Jahre) und die restlichen 22% zu der jüngsten Alterskategorie (18-25 Jahren) gehörten.

Insgesamt sind aus der qualitativen Studie zwölf Faktoren hervorgegangen, welche die Bereitschaft der Befragten, personenbezogene Daten auf Datenverkaufsplattformen zu verkaufen, beeinflussen. Diese Faktoren können in acht übergeordnete Kategorien eingeteilt

werden. Tabelle 8 gibt einen Überblick über die Faktoren, ihre Kategorien sowie eine Beschreibung der Faktoren, die innerhalb des qualitativen Schrittes gefunden wurden. Im weiteren Verlauf werden diese noch detaillierter beschrieben.

Tabelle 8: Einflussfaktoren für die Bereitschaft der Benutzer, personenbezogene Daten auf Datenverkaufsplattformen zu verkaufen

Kategorie	Faktor	Beschreibung
Kompensation	Art der Kompensation	Form der Vergütung für die Offenlegung der Daten (monetäre Belohnung oder andere Leistungen wie z.B. Gutscheine, Boni, Zeitersparnis)
	Höhe der Kompensation	Geldbetrag / Nutzen, der für die Offenlegung der Daten bezahlt wird
Kaufende Instanz	Kaufende Instanz (Unternehmen)	Wer kauft und verwendet die Daten?
Daten	Datentyp	Art der Daten und ihre Sensibilität
	Anonymität	Haben die Daten einen Bezug zu meiner Identität? Oder sind sie anonym?
Verwendungs-zweck	Verwendungs-zweck	Zu welchem Zweck werden die Daten verwendet?
Keine Weitergabe an Dritte	Keine Weitergabe an Dritte	Die kaufende Instanz (z.B. Unternehmen) sollte die Daten nicht weiterverkaufen dürfen oder zumindest um Erlaubnis bitten.
Provider der Plattform	Vertrauen in den Plattform-betreiber	Ist der Plattformanbieter ein vertrauenswürdiges Unternehmen? Ist er glaubwürdig? Wird der Provider von einer unabhängigen Instanz überwacht? Ist der Plattformanbieter zuverlässig und seriös? Und wie ist sein Ruf?
	Herkunft und geltendes Recht	Wo ist der Sitz des Unternehmens? Und welcher rechtliche Rahmen gilt?
Zeitrahmen des Geschäftes	Zeitrahmen des Geschäftes	Ist es ein Einzelgeschäft oder erwirbt die Plattform ein langfristiges Recht, aktuelle Informationen über die Person zu erhalten (Dauerauftrag)?
Sicherheit	Sicherheit	Sind die Daten durch eine sichere Infrastruktur (z.B. Verschlüsselung) vor unbefugtem Zugriff geschützt?
	Recht auf Löschung	Ist es möglich, den Prozess zu beenden? Was wäre dann die Folge? Ist es möglich die Daten zu löschen?

Es ist wenig überraschend, dass die Teilnehmer häufig die **Kompensation** als Einflussfaktor auf ihre Bereitschaft, personenbezogene Daten zu verkaufen, nannten. Obwohl die Teilnehmer gefragt wurden, unter welchen Umständen sie bereit wären, Daten auf einer solchen Plattform zu verkaufen, konnten sich einige Befragte neben Geld auch andere

Vergütungsarten vorstellen. So nannten einige Interviewte Gutscheine, Boni, Zeitersparnisse oder sogar Jobangebote als mögliche Vorteile, gegen die sie es sich vorstellen konnten, Daten zu veräußern. In den meisten Fällen forderten die Teilnehmer jedoch eine finanzielle Entschädigung: *„Da ich ohnehin immer schwerer drum herumkomme, meine Daten preiszugeben, warum also nicht dafür bezahlen lassen, da man den Aufwand eh hat (Dateneingabe wird honoriert)“.* Neben den Teilnehmern, die sich zu der Kompensationsform äußerten, nannten die meisten der befragten Internetnutzer auch die **Höhe der Vergütung** als wichtigen Faktor. So gaben sie an, dass die Vergütung „*angemessen*", „*eine hohe Summe*" oder „*nicht nur ein paar Cent*" betragen sollte, schlicht „*es muss sich schon rentieren*“. Zwei Interviewte gaben sogar konkrete Beträge für die Offenlegung ihrer Daten an (500 Euro und 1000 Euro). Weiterhin wurde zum Ausdruck gebracht, dass das Verhältnis zwischen Datenmenge und Vergütungshöhe ebenfalls die Verkaufsbereitschaft beeinflussen würde.

Darüber hinaus äußerten einige Studienteilnehmer, dass es für sie auch relevant sei, **welche Instanz die Daten kauft**: „*Ich wüsste gerne wer denn meine Daten kauft und will sie nicht einfach jedem geben*“. Die Befragten forderten also zumindest Transparenz über die betroffene Instanz: *„man bekommt die Firma konkret vorab genannt (z.B. Versicherungsbranche)“.* Einige Teilnehmer äußerten ausdrücklich den Wunsch, die Auswahl der beteiligten Unternehmen steuern zu können: *„Habe ich Einfluss darauf, welchem Unternehmen meine Daten verkauft werden oder kann ich sogar einzelne ausschließen?“*

Die **Daten** selbst einhergehend mit ihrer Sensibilität spielten für die meisten befragten Internetnutzer ebenfalls eine entscheidende Rolle. Einige Teilnehmer gaben beispielsweise an, dass sie ihre Telefonnummern und/oder Adressdaten nicht verkaufen würden, andere würden zögern Fotos oder Videos zur Verfügung zu stellen. Eine Teilnehmerin sagte: *„Es kommt auf die **Art der Daten** an die ich preisgebe. Für mich gibt es Daten die ich ohne Probleme weitergeben könnte und auch welche die ich nicht unbedingt preisgeben will.“* Dies scheint vom Grad der Sensibilität der Daten abhängig zu sein, so äußert eine Internetnutzerin beispielsweise: *„Wie sensibel sind die zu verkaufenden Daten[?] Angabe[n] über z.B. ausgeübte Sportarten sind weniger sensibel als z.B. aktuelle Medikation[en]“.* Für einige hängt die Sensibilität auch von der Variabilität der Daten ab. Eine Person gab beispielsweise an, dass sie eher bereit sei, E-Mail-Adressen oder sogar Bankkonten zu veräußern, da diese leicht geändert werden können. Ähnlich wie bei der Kaufinstanz forderten die Befragten auch hier die Kontrolle über die Auswahl der Daten: „*Ich kann selbst entscheiden welche Daten ich*

von mir Preis geben möchte". Darüber hinaus erklärten auch einige Befragte, dass die **Anonymität** der Daten Einfluss auf ihre Verkaufsbereitschaft hat: *„Die verkauften Daten müssen anonym verarbeitet werden und nicht mit meiner Person in Verbindung gebracht werden.“*

Weiterhin erklärten viele der Teilnehmer, dass ihre Bereitschaft, personenbezogene Daten zu verkaufen, davon abhänge, **für welchen Zweck** die Daten letztlich **verwendet** werden würden. Einige gaben an, dass sie Daten nur für „*sinnvolle Zwecke*" oder „*gute Gründe*" preisgeben würden, andere nannten konkrete Beispiele wie Spenden und wissenschaftliche Studien. Weiterhin erklärte ein Befragter: *„Es [sollte] nicht zu meinem Nachteil [sein] (Beispiel Behördern, Bonität usw.)"* Ein weiterer, häufig genannter Zweck war die Werbung. Eine befragte Internetnutzerin machte eine positive Assoziation: *„Einer der Gründe von gesammelten Daten ist die Werbung die mich ansprechen soll. Die Werbung wäre auf mich zugeschnitten.“* Im Gegensatz dazu hatte eine andere Teilnehmerin Angst vor unerwünschter Werbung: *„Wenn ich sicher wäre, dass ich nicht jeden Tag 10mal angerufen werde um mir eine günstige Versicherung, Handy, Gewinnspiel oder sonst was anzudrehen, würde ich eher meine Daten preisgeben.“* In einem Fall wurde die Teilnahme sogar als idealistisch angesehen, wie das folgende Zitat zeigt: *„Ich möchte durch meine Daten etwas verändern und das Unternehmen aufbessern“.*

Die Studienteilnehmer erklärten außerdem, dass ihre Daten "nur für interne Zwecke" verwendet werden sollten, was sich in dem Faktor **keine Weitergabe an Dritte** wiederfindet. Dieser kritische Faktor kann durch das folgende Zitat veranschaulicht werden: *„Das datenkaufende Unternehmen sollte sich dazu verpflichten, Nachteile für den Datenverkäufer weitgehend auszuschließen, indem kein direkter Weiterverkauf an Externe erfolgt, die ein Interesse daran haben könnten dem Datenverkäufer einen Nachteil (z.B. finanzieller oder sozialer Natur) entstehen zu lassen.“*

Darüber hinaus wurden der **Standort des Plattformbetreibers und die damit verbundene Rechtslage** als Einflussfaktor für die Verkaufsbereitschaft personenbezogener Daten identifiziert. So forderte beispielsweise ein Teilnehmer: *„Das Unternehmen sollte einen Sitz in der EU haben"*. Ein anderer befragter Internetnutzer äußerte den Wunsch, den rechtlichen Rahmen zu kennen: „*Welcher rechtliche Rahmen ist gegeben? Welches Recht gilt (ggf. bei ausländischer Firma)?“* Dieser Einflussfaktor steht in Zusammenhang mit der **Vertrauenswürdigkeit des Plattformanbieters**, die ebenfalls von den Befragten als relevant wahrgenommen wurde. Einer von ihnen erklärte: *„Das Preisgeben von Daten ist eine heikle*

Angelegenheit und ich muss diesem Anbieter vertrauen können." Um die Vertrauenswürdigkeit zu erhöhen, schlug ein Befragter die Einrichtung von unabhängig kontrollierten Zertifizierungen vor, und ein anderer Studienteilnehmer schlug eine staatliche Kontrolle des Anbieters mit öffentlich zugänglichen Ergebnissen vor. Darüber hinaus können die Zuverlässigkeit und Reputation des Plattformanbieters auch das Vertrauen fördern: *„Wer kauft meine Daten? Ist das Unternehmen vertrauenswürdig? Werden meine Daten bei dem Unternehmen unter allen Umständen geschützt? Wenn sich ein Unternehmen entsprechend seriös präsentiert oder besser noch bewertet werden kann, damit klar ersichtlich ist wer wirklich vertrauenswürdig ist [würde ich die Plattform eher nutzen].“*

Darüber hinaus wurde der **Zeitrahmen des Geschäftes,** genauer gesagt, ob der Verkauf der Daten ein einmaliger Vorgang wäre oder ob die Plattform ein langfristiges Recht auf den Erhalt dieser personenbezogenen Daten erwirbt, erwähnt: *„Die Vergütung sollte variabel und ausreichend sein. Es könnte eine Einmalvergütung für bestimmte Daten geben, jedoch auch eine Vergütung, welche über einen bestimmten Zeitraum ausgezahlt wird und dynamisch ist. Ähnlich der Dynamik in Lebensversicherung zum Ausgleich der Inflation. Sollten Daten im Lauf der Zeit an Bedeutung gewinnen und auch nach Jahren noch relevant sein, sollte der Kunde auch dementsprechend davon profitieren.“* Auch die Frage, ob die Plattformnutzer verpflichtet wären, ihre Daten immer auf dem neuesten Stand zu halten, oder ob sie von Änderungen profitieren können, beschäftigte einige der befragten Teilnehmer: *„Sollte ich heiraten, umziehen, mehr verdienen etc. möchte ich nicht verpflichtet sein, dies anzugeben, sondern erneut davon profitieren, wenn ich Änderung[en] der Daten freiwillig angebe.“*

Ein weiterer wichtiger Faktor ist die **Sicherheit**. Häufig wurden Bedenken hinsichtlich eines angemessenen Sicherheitsniveaus beispielsweise in Bezug auf Verschlüsselung, Speicherung und Serverinfrastruktur sowie generell bezüglich eines angemessenen Schutzes vor Straftaten geäußert: *„Die Sicherheit bei einer solchen Website wäre unfassbar wichtig. Schließlich möchte ich nicht, dass meine Daten zum Beispiel durch Hacker gestohlen werden können.“* Einige Befragte waren auch insbesondere über die Gefahr eines Datenmissbrauchs besorgt. Dies kann durch folgende Aussagen veranschaulicht werden: „*[Ich habe] Angst vor dem Verlust der Identität", „meine Daten sollten nicht missbraucht werden"* oder *„Ich gebe meine Daten nicht preis, zumindest nicht freiwillig. Meine Privatsphäre ist mir zu wichtig."* Um diese Sorgen zu mindern, wurde eine Art Versicherung vorgeschlagen, bei der das Unternehmen dafür verantwortlich ist, im Falle von Vorfällen „*ausreichend*" zu entschädigen. Darüber hinaus stellten einige Teilnehmer der Umfrage die Frage, ob es möglich sei, sich vom

Dienst abzumelden und was die Folgen davon wären, während ein anderer Internetnutzer klar ein **Recht auf Löschung** forderte: „*Auf Wunsch von mir sind die Daten zu löschen*."

Diese identifizierten Einflussfaktoren auf die Verkaufsbereitschaft von Daten dienten als Grundlage für weitere Untersuchungen des zweiten Schritts, die im nächsten Abschnitt beschrieben werden.

6.5 Zweiter Untersuchungsschritt: Auswahlbasierte Conjoint-Analyse

6.5.1 Methodik

Im zweiten Schritt soll nun untersucht werden, welche durchschnittlichen Wichtigkeiten Internetnutzer einer Auswahl der im qualitativen Schritt identifizierten Einflussfaktoren zuweisen. Zur Untersuchung dessen wurde eine auswahlbasierte Conjoint-Analyse, englisch *choice-based conjoint analysis (CBCA),* durchgeführt. Mit dieser Methode können die Präferenzen potenzieller Nutzer analysiert werden, indem die Studienteilnehmer in mehreren Runden zwischen Plattformalternativen, die jeweils in ihren Eigenschaften variieren, ihren Favoriten auswählen (Green et al. 2001; Roßnagel et al. 2014). Da die vorausgegangene, qualitative Studie mehrere Einflussfaktoren für die Daten-Verkaufsbereitschaft von Individuen identifiziert hat, die alle als Eigenschaften oder Merkmale von Datenverkaufsplattformen angesehen werden können, stellt die Conjoint-Analyse eine geeignete Methodik zur Untersuchung der relativen Wichtigkeiten dieser Faktoren dar. Schließlich basiert die Conjoint-Methodik auf der Annahme, dass Individuen, wenn sie sich zwischen Alternativen entscheiden müssen, diese Alternativen als ein Bündel von Merkmalen oder Eigenschaften, so genannter **Attribute**, wahrnehmen, die wiederum unterschiedliche Merkmalsausprägungen, auch **Attributlevel** genannt, annehmen können (Green und Srinivasan 1978; Pu und Grossklags 2015). Mit Hilfe der Conjoint-Analyse können dann die **Teilnutzenwerte** (engl. *partial utilities* oder *part-worths*) der Attributlevel sowie die **durchschnittlichen Wichtigkeiten** der Attribute aus Nutzerperspektive untersucht werden, wodurch Rückschlüsse auf die Zusammensetzung der Nützlichkeiten von Datenverkaufsplattformen gezogen werden können (Johnson 1974; Krasnova et al. 2009). Die Teilnutzenwerte der einzelnen Attributlevel werden dabei so berechnet, dass sie bestmöglich mit den allgemeinen Präferenzen der Befragten übereinstimmen, die sie durch ihre Entscheidungen bei der Auswahl zwischen den Alternativen der Conjoint-Studie angeben (Green und Srinivasan 1978).

Die traditionelle Conjoint-Methodik analysiert Entscheidungen zwischen Alternativen, indem Individuen gleichzeitig dargestellte Alternativen in eine Rangfolge bringen (Green et al. 2001). Dieser Bewertungsansatz kann für die Teilnehmer allerdings kognitiv herausfordernd sein (Braun et al. 2016) und spiegelt auch nur bedingt das tatsächliche Verhalten von Individuen in Entscheidungsprozessen wider (Orme 2009). Daher wurde bei diesem zweiten Untersuchungsschritt eine auswahlbasierte Conjoint-Analyse durchgeführt, die als realistischer und etwas leistungsfähiger als die traditionelle Conjoint-Analyse angesehen wird (Karniouchina et al. 2009). Zudem ist die auswahlbasierte Conjoint-Analyse eine weit verbreitete Form, die auch bereits häufig in der Wirtschaftsinformatikforschung eingesetzt wurde (z.B. Dauda und Lee 2015; Hu et al. 2012; Rollin et al. 2017; Roßnagel et al. 2014). Bei dieser Form der Conjoint-Analyse werden den Teilnehmern jeweils nur wenige Alternativen, die sich in ihren Attributleveln unterscheiden, gleichzeitig angezeigt, aus denen die Befragten dann pro Runde die am meisten bevorzugte Alternative auswählen (Green et al. 2001). Durch die Anwendung des hierarchischen Bayes-Ansatzes (engl. *hierarchical bayes)* ist es möglich, Teilnutzenwerte auf individueller Ebene zu schätzen, aus denen wiederum die relativen Wichtigkeiten der Attribute berechnet werden können (Braun et al. 2016).

Bestimmung der Attribute und Attribut-Level

Wie bereits beschrieben, dienen die zwölf im qualitativen Schritt identifizierten Einflussfaktoren als Grundlage für die Bestimmung der CBCA-Attribute, da diese als Merkmale von Datenverkaufsplattformen angesehen werden können. Aufgrund einiger methodischer Anforderungen müssen jedoch ein paar dieser Faktoren von der Analyse ausgeschlossen werden: Die erste Anforderung an die Attribute in einer Conjoint-Studie ist, dass diese nicht voneinander abhängig sein dürfen (Louviere 1988). Eine Prüfung der im ersten Untersuchungsschritt identifizierten Einflussfaktoren bezüglich dieser Anforderung hat ergeben, dass eine Abhängigkeit zwischen dem Datentyp und der Anonymität bestehen könnte, da verschiedene Arten von Daten in dem Grad, in dem sie zur Identifizierung einer Person verwendet werden können, variieren (Milne et al. 2017). Weiterhin kann die Vertrauenswürdigkeit eines Anbieters sowohl von der Herkunft und den rechtlichen Rahmenbedingungen des Unternehmens als auch von der angebotenen Sicherheit abhängen (z.B. Cheung und Lee 2006; Flavián und Guinalíu 2006; Perusco und Michael 2007). Daher wurden Anonymität und Vertrauenswürdigkeit aus der Liste der Conjoint-Attribute ausgeschlossen, da diese die Faktoren sind, die von den anderen genannten Faktoren abhängig sind. Darüber hinaus wurde noch der Einflussfaktor „keine Weitergabe an Dritte“ von der

Conjoint-Analyse ausgeschlossen, da Untersuchungen im Rahmen der qualitativen Studie darauf hindeuten, dass die Weitergabe an Dritte seitens der Internetnutzer grundsätzlich nicht akzeptiert wird und somit ein Knock-out-Kriterium darstellt. Wie in der Literatur empfohlen (z.B. Hensher 1994), wurde dieser daher für die Conjoint-Analyse fixiert, indem angegeben wurde, dass die Teilnehmer davon ausgehen sollen, dass der Käufer keine personenbezogenen Daten an Dritte weitergibt.

Um die verbleibenden Attribut-Kandidaten weiter zu validieren und geeignete Ausprägungen zu bestimmen, wurden Empfehlungen zu induktiven Ansätzen aus der Conjoint-Analyseliteratur (z.B. Green und Krieger 1991; Krasnova et al. 2009) befolgt und weitere 21 halbstrukturierte Interviews unter Internetnutzern durchgeführt. Auch hierbei wurde zunächst die Idee von Datenverkaufsplattformen mit Hilfe der bereits in dem ersten Untersuchungsschritt verwendeten Mockups vorgestellt. Anschließend wurden die neun verbleibenden Attribute (Art und Höhe der Kompensation, kaufende Instanz, Datentyp, Verwendungszweck, Herkunft und geltendes Recht, Zeitrahmen des Geschäfts, Sicherheit und Recht auf Löschung) vorgestellt und die Befragten gebeten, sich dazu zu äußern und mögliche positive oder negative Ausprägungen dieser Attribute zu nennen.

Basierend auf diesen Interviews wurden zwei weitere Einflussfaktoren von der Conjoint-Analyse ausgeschlossen, da auch diese für die Befragten Knock-out-Kriterien darstellten. So forderten fast alle Befragten das Recht auf Löschung und benannten das einmalige Geschäft als Zeitrahmen. Dies deutet darauf hin, dass wenige Abweichungen in Bezug auf diese Faktoren zu erwarten sind (Hensher 1994), weswegen auch sie für die CBCA fixiert wurden. Die Teilnehmer sollten daher davon ausgehen, dass die Plattform immer die Möglichkeit bietet personenbezogene Daten zu löschen und dass der Verkauf von Daten immer ein einmaliger Vorgang ist.

Darüber hinaus zeigte sich, dass viele der Interviewten es sehr herausfordernd empfanden Ausprägungen für kaufende Unternehmen oder Branchen benennen zu müssen. Da dies ein Indikator dafür ist, dass auch die Teilnehmer der Conjoint-Studie Schwierigkeiten haben könnten, dieses Attribut und seine Level zu bewerten, wurde auch die kaufende Instanz von der Conjoint-Analyse ausgeschlossen. Dies reduzierte das Risiko von verzerrten oder nicht interpretierbaren Ergebnissen.

Für alle anderen Attribute nannten die Interviewten hilfreiche Vorschläge für mögliche Attributlevel. Insgesamt konnten so zwei bis drei Level für jedes Attribut festgelegt werden,

wobei sorgfältig darauf geachtet wurde, dass sich die Level gegenseitig ausschließen und klar formuliert sind (Orme 2002).

Eine Übersicht aller in der Conjoint-Studie verwendeten Attribute und ihrer Attributlevel sind in Tabelle 9 zu finden. Insgesamt sind von den ursprünglichen zwölf Einflussfaktoren des ersten Untersuchungsschrittes also nur die Faktoren für die Conjoint-Analyse ausgewählt worden, die a) weitgehend unabhängig voneinander sind, b) voraussichtlich zu einer Variation der Präferenzen der Teilnehmer führen werden und damit keine Knock-out-Kriterien sind und c) von allen Teilnehmern sinnvoll bewertet werden können.

Tabelle 9: Überblick über die Attribute und ihre Level

Attribut	Anzahl der Attributlevel	Attributlevel
Datentyp	3	Adressdaten (z.B. Name, Straße, Stadt)
		Demographische Daten (z.B. Alter, Geschlecht, Einkommen)
		Persönliche Interessen (z.B. Hobbies, Mode, Nahrung)
Verwendungs-zweck	3	Forschung & Entwicklung
		Werbung
		Anonymisierte Statistiken
Herkunft des Providers und geltendes Recht	3	Westeuropäische Länder (z.B. Frankreich, Deutschland)
		Europäische Union
		Vereinigte Staaten
Sicherheit	3	Passwort
		Passwort & Verschlüsselung
		Passwort, Verschlüsselung & Zertifizierung durch dritte Partei
Art der Kompensation	2	Geld
		Gutscheine für Onlineshops (z.B. Amazon)
Höhe der Kompensation	3	5 Euro
		10 Euro
		20 Euro

Conjoint-Design und Studiendurchführung

Für das Design wurde eine traditionelle *Full-Profile-CBCA* mit drei Plattformvarianten, den sogenannten Konzepten, plus einer "keine Auswahl"-Option (engl. *no choice*) pro Auswahlaufgabe gewählt. Die "keine Auswahl"-Option ist in diesem Zusammenhang von besonderer Bedeutung, da die qualitative Studie bereits gezeigt hat, dass einige Personen generell nicht bereit sind ihre Daten zu verkaufen. Jeder Teilnehmer musste 17 Auswahlaufgaben beantworten, wobei eine Auswahlaufgabe einer Entscheidung zwischen

verschiedenen Konfigurationen entspricht. Diese wurden mit Hilfe der *Sawtooth Software* implementiert und in eine Online-Umfrage mit den gleichen Mockups und Beschreibungen wie im ersten Untersuchungsschritt eingebettet, wobei diesmal zusätzlich noch über die Knock-out-Kriterien informiert wurde. So sollten die Teilnehmer davon ausgehen, dass die Plattform immer die Möglichkeit bietet, personenbezogene Daten zu löschen, es sich stets um ein einmaliges Geschäft handelt und keine Weitergabe der Daten durch die kaufenden Unternehmen an Dritte stattfinden wird. Da die Interviews potenzielle Schwierigkeiten für die Befragten bei der Bewertung verschiedener Arten von kaufenden Unternehmen aufgezeigt haben, wurde zusätzlich angegeben, dass Partnerunternehmen der Plattform die Daten kaufen würden. Schließlich wurden den Teilnehmern die eigentlichen Auswahlaufgaben vorgestellt und sie mussten für jedes Auswahlset die Alternative wählen, die sie verwenden würden, oder, sofern ihnen nichts davon zusprach, die „keine Auswahl“-Option anklicken.

Die Datenerhebung wurde mit demselben Marktforschungsunternehmen durchgeführt, mit dem bereits im ersten Schritt zusammengearbeitet wurde und auch hier wurde eine Alters- und Geschlechterverteilungen zu Grunde gelegt, die für häufige Internetnutzer repräsentativ ist (Statista 2014a; Statista 2014b). Dreiundsiebzig Befragte mussten aufgrund fehlgeschlagener Aufmerksamkeitstests von weiteren Analysen ausgeschlossen werden, so dass insgesamt 250 Teilnehmer das finale Sample der zweiten Studie bildeten, welches aus 133 Männern und 117 Frauen bestand. Von diesen Teilnehmern waren 26% zwischen 18 und 24 Jahre alt, 27% zwischen 25 und 34 Jahre, 20 % zwischen 35 und 44 Jahre, 14% zwischen 45 und 54, und 13 % waren älter als 55 Jahre. Auch bei dieser Studie waren mit einem Anteil von insgesamt 51% die meisten Befragten Beschäftigte, während 20% Studierende waren, 8% Selbständige, 18% gaben "anderes" oder "nicht spezifiziert" an, und 3% waren arbeitslos. Im nächsten Unterkapitel werden die Ergebnisse der Conjoint-Analyse mit den relativen Wichtigkeiten der Attribute und der Teilnutzenwerte der Level vorgestellt.

6.5.2 Ergebnisse

Um die Auswahlentscheidungen der Teilnehmer zu analysieren, wurde die hierarchische Bayes (HB)-Methode zur Schätzung der durchschnittlichen Nützlichkeiten angewandt, welche die Attraktivität der Level sowie die relative Wichtigkeit der sechs Attribute widerspiegeln (Pu und Grossklags 2015). Auf diese Weise können aus den Informationen, welche der angezeigten Plattformalternativen einschließlich der „keine Auswahl“-Option die Befragten während der Umfrage gewählt haben, Einblicke darüber gewonnen werden, wie wichtig den Teilnehmern die Attribute sind. Die Ergebnisse sind in Tabelle 10 dargestellt.

Anlehnend an den Ansatz von Krasnova et al. (2009) wurde darüber hinaus aus den Teilnutzenwerten errechnet, wie sich der Nutzen innerhalb eines Attributes bei einem Wechsel von einem Attributlevel zu einem anderen verändert, was wiederum hilft das Verständnis über die Attraktivität der Level zu verbessern. Diese Ergebnisse sind in der Spalte "Nutzenänderung“ (engl. *utility changes*) in Tabelle 11 zusammengefasst. Zusätzlich wurde ein t-Test auf der Nullhypothese durchgeführt, dass die Teilnutzenwerte gleich sind. Die entsprechenden p-Werte sind ebenfalls in Tabelle 11 dargestellt.

Ein Vergleich der durchschnittlichen Wichtigkeiten der Attribute, also der Faktoren, die Einfluss auf die Verkaufsbereitschaft von Daten haben, zeigt, dass die **Höhe der Kompensation** mit einer relativen Wichtigkeit von 27,36% mit Abstand das einflussreichste Attribut ist. Dieses Ergebnis impliziert, dass Internetnutzer geneigt sind, ihre Daten zu verkaufen, wenn die Entlohnung dafür groß genug ist. Es ist wenig verwunderlich, dass die durchschnittliche Wichtigkeit mit dem Geldbetrag, den die Plattform bietet, wächst, allerdings ist die Nutzenänderung bei einem Wechsel von 5 Euro auf 10 Euro viel größer als der Anstieg bei einem Wechsel von 10 Euro auf 20 Euro, wobei beide Nutzenänderungen signifikant sind, wie die t-Tests zeigen. Die Berechnung der Nützlichkeit pro Euro ergibt, dass die Nützlichkeit zwischen 5 Euro und 10 Euro um 83,38/5= 16,68 Einheiten ansteigt, während sie zwischen 10 Euro und 20 Euro nur um 51,08/10= 5,11 Einheiten wächst, was auf einen sinkenden Grenznutzen hinweist. Diese beiden Werte können auch in der folgenden Analyse zur Berechnung des monetären Wertes der Veränderungen zwischen den Attributlevel verwendet werden (Krasnova et al. 2009; Pu und Grossklags 2015). Da die Kompensation nicht linear steigt, wurden diese monetären Veränderungswerte für die beiden Euro-Äquivalente 16,68 Euro und 5,11 Euro berechnet, welche die Ober- und Untergrenze der monetären Äquivalente ausdrücken. Diese Ergebnisse sind in Tabelle 11 dargestellt.

Mit einer durchschnittlichen Wichtigkeit von 21,88% stellt sich der **Datentyp** in der Analyse als das zweitwichtigste Attribut dar. Ein Vergleich der Teilnutzenwerte zeigt, dass die Teilnehmer klar zwischen verschiedenen Datentypen unterscheiden und dabei Typen bevorzugen, welche die Datenpreisgebenden nicht identifizierbar machen: Während Adressdaten mit einer Nutzenänderung von 74,68 (im Vergleich zu demographischen Daten) die unbeliebteste Datenart darstellt, ist der Unterschied zwischen demographischen Daten und persönlichen Interessen ebenfalls signifikant, hier beträgt die Nutzenänderung aber nur 27,93. Für den monetären Wert der Nutzenänderung bedeutet dies eine Erhöhung zwischen 4,48 Euro (untere Grenze) und 14,61 Euro (obere Grenze).

Auch die **Herkunft** des Anbieters der Datenverkaufsplattform **und das geltende Recht** erwiesen sich mit einer relativen Wichtigkeit von 18,03% als bedeutend. Die höchsten Teilnutzenwerte waren für bestimmte westeuropäische Länder zu verzeichnen, gefolgt von der EU im Allgemeinen, wobei diese Unterschiede aber nicht signifikant waren. Im Gegensatz dazu führte ein Wechsel zu den Vereinigten Staaten von Amerika zu einem deutlichen Rückgang der Nützlichkeit um 83,08. So könnte ein Anstieg der Nützlichkeit bedingt durch die Anhebung der monetären Kompensation von 5 Euro auf 10 Euro, fast vollständig durch eine Abnahme der Nützlichkeit bedingt durch einen Umzug aus der EU in die USA kompensiert werden. Es sollte allerdings an dieser Stelle beachtet werden, dass diese Ergebnisse aufgrund der zugrundeliegenden westeuropäischen Stichprobe verzerrt sein könnten. Zukünftige Forschungsarbeiten könnten die Studienergebnisse mit Hilfe von Stichproben aus verschiedenen Kulturen ergänzen und so validieren.

Der **Verwendungszweck** wurde ebenfalls mit einer merklichen, durchschnittlichen Wichtigkeit von immerhin 13,58% bewertet. Die Teilnutzenwerte zeigen, dass die Teilnehmer Marketingzwecke wie Werbung am stärksten ablehnen und ihre Daten lieber für Forschung und Entwicklung sowie für anonymisierte Statistiken verkaufen würden, wobei letztere die bevorzugte Option sind, wenngleich der t-Test keine signifikanten Unterschiede zwischen Forschung und anonymisierten Statistiken feststellen konnte. Bezüglich des monetären Wertes kann der Wechsel von Werbung als Verwendungszweck hin zu Forschung zwischen 3,35 Euro und 11,27 Euro betragen.

Mit einer durchschnittlichen Wichtigkeit von 10,88% stellt die **Art der Kompensation** das fünftwichtigste Attribut dar. Der Nutzenwertrückgang von 51,68 zeigt eine klare Präferenz für eine geldbasierte Entlohnung gegenüber Gutscheinen mit gleichem Betrag, was sich als Euro –Äquivalent in einem Bereich von -3,10 Euro bis zu -10,11 Euro äußert.

Als das Attribut mit der geringsten durchschnittlichen Wichtigkeit stellte sich der **Sicherheitsfaktor** heraus. Die Ergebnisse zeigen zwar größere Teilnutzenwerte für eine höhere Sicherheitsstufe, aber die Nutzenwert-Änderungen von 20,92 von der sehr einfachen Ebene des simplen Passwortschutzes zur nächsten Ebene des Passwortschutzes mit Verschlüsselung zeigen, dass die Befragten keine hohen Erwartungen an die Sicherheitseinstellungen solcher Plattformen stellen. Der Wechsel auf die nächste Stufe mit einer zusätzlichen Zertifizierung durch einen Dritten führte zu einem noch kleineren Nutzenzuwachs von nur 11,71, die Level sind jedoch signifikant unterschiedlich voneinander, wie der t-Test zeigt.

Zusammengefasst weisen die Ergebnisse darauf hin, dass die am stärksten bevorzugte Datenverkaufsplattform eine möglichst hohe finanzielle Kompensation (in diesem Fall 20 Euro) für den Verkauf von persönlichen Interessen anbieten sollte, die wiederum für anonymisierte Statistiken verwendet werden könnten. Darüber hinaus sollte der Plattformanbieter in einem westeuropäischen Land ansässig sein und ein hohes Sicherheitsniveau, wie Passwortschutz, Verschlüsselung und Zertifizierung durch einen Dritten, bieten.

Tabelle 10: Attribute, Level, Teilnutzenwerte und durchschnittliche Wichtigkeiten

Attribute	Level	Teilnutzenwerte*	Standard-abweichung	Durchschnittliche Wichtigkeiten
Höhe der Kompensation	5 Euro	-72,61	67,02	27,36%
	10 Euro	10,77	20,65	
	20 Euro	61,84	77,43	
Datentyp	Adressdaten	-59,10	66,42	21,88%
	Demographische Daten	15,58	37,44	
	Persönliche Interessen	43,51	49,27	
Herkunft des Providers und geltendes Recht	Westeuropäische Länder	29,70	36,63	18,03%
	Europäische Union	26,69	28,96	
	Vereinigte Staaten	-56,39	60,23	
Verwendungs-zweck	Werbung	-38,89	40,99	13,58%
	Forschung & Entwicklung	18,71	26,89	
	Anonymisierte Statistiken	20,18	30,90	
Art der Kompensation	Geld	25,84	33,06	10,88%
	Gutscheine für Onlineshops	-25,84	33,06	
Sicherheit	Passwort	-17,85	26,59	8,27%
	Passwort & Verschlüsselung	3,07	16,74	
	Passwort, Verschlüsselung & Zertifizierung	14,78	27,39	

* Die Teilnutzenwerte werden mit nullzentrierten Differenzen (engl. *zero-centered differences*) skaliert.

Tabelle 11: Nutzenänderung und monetärer Wert der Änderungen

Attribute	Wechsel zwischen den Leveln	Nutzen-änderung	p-Wert (t-Test auf Gleichheit)	Monetärer Wert der Nutzen-änderung (obere und untere Grenze)
Höhe der Kompensation	5 Euro → 10 Euro	83,38	0,0001	
	10 Euro → 20 Euro	51,08	0,0001	
Datentyp	Adressdaten → Demographische Daten	74,68	0,0001	4,48 Euro – 14,61 Euro
	Demographische Daten → Persönliche Interessen	27,93	0,0001	1,67 Euro – 5,11 Euro
Herkunft des Providers und geltendes Recht	Westeuropäische Länder → Europäische Union	-3,00	0,3098	-0,18 Euro – -0,59 Euro
	Europäische Union → Vereinigte Staaten	-83,08	0,0001	-4,98 Euro – -16,26 Euro
Verwendungs-zweck	Werbung → Forschung und Entwicklung	57,59	0,0001	3,35 Euro – 11,27 Euro
	Forschung & Entwicklung → Anonymisierte Statistiken	1,48	0,5691	0,09 Euro – 0,29 Euro
Art der Kompensation	Geld → Gutscheine	-51,68	0,0001	-3,10 Euro – -10,11 Euro
Sicherheit	Passwort → Passwort & Verschlüsselung	20,92	0,0001	1,25 Euro – 4,09 Euro
	Passwort & Verschlüsselung → Passwort, Verschlüsselung & Zertifizierung	11,71	0,0001	0,70 Euro – 2,29 Euro

In einem weiteren Analyseschritt, wurde eine *Latent Class Analyse* durchgeführt, um so basierend auf den CBCA-Auswahlen der befragten Individuen Gruppen mit ähnlichem Präferenzmuster bestimmen zu können (SawtoothSoftware 2004). *Latent Class* ermöglicht es dabei die durchschnittlichen Wichtigkeiten der Attribute sowie die Teilnutzenwerte der Level für jede Gruppe akkurat und effektiv zu identifizieren (SawtoothSoftware 2004). Basierend auf der Empfehlung, die Gruppenanzahl nach sinkenden Unterschieden zwischen Statistiken wie *Relative Chi Square (RelChiSq)* und *Percent certainty (Pct Cert)* festzumachen, konnten vier Gruppen als optimale Anzahl identifiziert werden, da die nächst größere Gruppenanzahl kleinere Differenzen aufgewiesen hat (Orme 2012). Die vier Gruppen weisen dabei relativ homogene Gruppengrößen von 24,2%, 22,7%, 30,7% sowie 22,4% auf. Die einzelnen

Gruppen lassen sich durch ihre durchschnittlichen Wichtigkeiten charakterisieren, die in Tabelle 12 zusammengefasst werden. Zur weitergehenden Analyse können darüber hinaus die Teilnutzenwerte herangezogen werden, die in Tabelle 13 für jede Gruppe dargestellt sind.

Die erste Gruppe zeichnet sich dadurch aus, dass den Gruppenzugehörigen mit deutlicher Mehrheit von fast 55% der Datentyp das wichtigste Attribut bei der Auswahl-Entscheidung ist, gefolgt von der Höhe der Kompensation, die allerdings mit 24% weniger als die Hälfte der Datentyp-Wichtigkeit ausmacht. Alle anderen Attribute wurden in dieser Gruppe mit einer sehr geringen Wichtigkeit bewertet. Diese Gruppe kann also als **Datentyp-bewusste Individuen** gesehen werden. Ein Blick auf die Teilnutzenwerte bezüglich des Attributs Datentyp innerhalb dieser Gruppe zeigt eine deutliche Ablehnung der Befragten bezüglich Adressdaten, während persönliche Interessen klar präferiert wurden.

Die zweite Gruppe zeichnet sich durch recht gleichverteilte durchschnittliche Wichtigkeiten aus, die alle zwischen 6% (für die Sicherheit) und fast 26% (für die Art der Kompensation) schwanken, weswegen diese auch als **Nutzergruppe mit homogen verteilten Präferenzen** betitelt werden kann. Interessanterweise ist, obwohl die Kompensationsart in dieser Gruppe das wichtigste Attribut darstellt und die Gruppenzugehörigen ganz klar ihre Präferenz zur geldbasierten Vergütung zum Ausdruck bringen, die Höhe der Kompensation nur das viertwichtigste Attributlevel. Im Gegensatz zur ersten Gruppe präferieren die Befragten dieser Gruppe demographische Informationen als Datentyp vor den persönlichen Interessen und die Ablehnung gegen Adressdaten ist wesentlich weniger stark ausgeprägt. Weiterhin ist bei dieser Gruppe bemerkenswert, dass das zweite Sicherheitslevel bestehend aus Passwort und Verschlüsselung am stärksten bevorzugt wurde, wenngleich dieser Teilnutzenwert nur geringfügig höher ist als das dritte Sicherheitslevel.

Auch in der dritten Gruppe sind die durchschnittlichen Wichtigkeiten für die jeweiligen Attribute recht gleichverteilt. In diesem Fall schwanken die Werte zwischen ca. 5% für den Datentyp sowie 36% für die Herkunft des Providers und damit einhergehend das geltende Recht, wobei die Vereinigten Staaten klar abgelehnt werden. Daher werden die Zugehörigen dieser Gruppe als **Standort-bewusste Individuen** bezeichnet. Mit 19% ist der Verwendungszweck das zweitwichtigste Attribut, gefolgt von der Höhe der Kompensation mit 18%. Wie die Teilnehmer der ersten Gruppe auch, präferieren die Befragten den Verwendungszweck der anonymisierten Statistiken, während Werbezwecke klar verneint werden.

Die vierte und letzte Gruppe ist die der **monetär-motivierten Nutzer**. Mit fast 64% ist die Höhe der Kompensation das wichtigste Attribut für die Befragten, die dieser Gruppe zugewiesen wurden, während die anderen vier Attribute jeweils nur durchschnittliche Wichtigkeiten zwischen 10% und 3% erreichten. Am wenigsten wichtig waren den Teilnehmern dieser Gruppe der Datentyp sowie die Sicherheit.

Tabelle 12: Durchschnittliche Wichtigkeiten der vier Gruppen

Attribute	**Gruppe 1** (24.2% des Gesamtsamples)	**Gruppe 2** (22.7% des Gesamtsamples)	**Gruppe 3** (30.7% des Gesamtsamples)	**Gruppe 4** (22.4% des Gesamtsamples)
Höhe der Kompensation	23,66%	17,66%	18,08%	63,50%
Datentyp	54,78%	12,42%	4,61%	3,67%
Herkunft des Providers und geltendes Recht	4,98%	20,29%	36,35%	10,29%
Verwendungszweck	6,67%	17,81%	19,12%	9,50%
Art der Kompensation	6,54%	25,75%	7,39%	9,57%
Sicherheit	3,38%	6,08%	14,45%	3,48%

Tabelle 13: Teilnutzenwerte der vier Gruppen (mit nullzentrierten Differenzen)

Attribute	Level	Gruppe 1	Gruppe 2	Gruppe 3	Gruppe 4
Höhe der Kompensation	5 Euro	-71,62	-62,19	-59,34	-193,81
	10 Euro	1,30	18,39	10,20	6,64
	20 Euro	70,33	43,80	49,14	187,17
Datentyp	Adressdaten	-205,08	-47,66	-6,04	-6,20
	Demographische Daten	81,48	26,83	-10,81	-7,91
	Persönliche Interessen	123,60	20,83	16,85	14,11
Herkunft des Providers und geltendes Recht	Westeuropäische Länder	14,76	31,32	81,94	7,56
	Europäische Union	0,36	45,22	54,22	27,10
	Vereinigte Staaten	-15,12	-76,54	-136,16	-34,65
Verwendungs-zweck	Werbung	-25,00	-66,86	-70,00	-36,57
	Forschung & Entwicklung	10,00	39,95	25,25	20,40
	Anonymisierte Statistiken	15,00	26,92	44,74	16,17
Art der Kompensation	Geld	19,61	77,24	22,16	28,72
	Gutscheine für Onlineshops	-19,61	-77,24	-22,16	-28,72
Sicherheit	Passwort	-10,09	-23,92	-42,80	-8,16
	Passwort & Verschlüsselung	-0,09	12,56	-1,09	-4,53
	Passwort, Verschlüsselung, & Zertifizierung	10,18	11,36	43,89	12,69

6.6 Diskussion der Ergebnisse

Datenverkaufsplattformen bieten ein großes Potenzial um die Verkaufsbereitschaft personenbezogener Daten beziehungsweise aus theoretischer Sicht, ihre Einflussfaktoren in einem natürlichen Kontext zu untersuchen. Daher wurde eine qualitative Online-Umfrage durchgeführt, um diese Faktoren zu identifizieren und so die erste Untersuchungsfrage beantworten zu können. Zusätzlich wurden, zur Beantwortung der zweiten

Untersuchungsfrage, die durchschnittlichen Wichtigkeiten einer Auswahl dieser Einflussfaktoren ermittelt. Weiterhin wurde eine *Latent Class Analyse* zur Identifikation von Gruppen mit ähnlichen Präferenzen durchgeführt. Basierend auf einer zweistufigen Studie und den Daten von insgesamt 299 Teilnehmern konnten zwölf Einflussfaktoren identifiziert werden. Darüber hinaus zeigte sich, dass die Wichtigkeiten zwischen einer ausgewählten Teilmenge der Faktoren variieren und dass Internetnutzer klare Präferenzen für einige der untersuchten Ausprägungen haben, die je nach Individuum unterschiedlich sein können, wie die Segmentierungsanalyse zeigt.

Im Folgenden werden die theoretischen und praktischen Auswirkungen der Studie sowie ihre Limitationen und zukünftige Forschungsvorschläge diskutiert.

6.6.1 Implikationen für Forschung und Praxis

Bezüglich der **theoretischen Implikationen** können drei wesentliche Beiträge der Studie festgehalten werden: Erstens, trägt die Studie zur Literatur über den Wert von personenbezogenen Daten bei, ein Thema das in der Zeit datenbasierter Geschäftsmodelle bei denen Daten wie Waren gehandelt werden, von besonderer Wichtigkeit ist. Während sich, wie im 4. Kapitel dieser Arbeit bereits dargelegt, frühere Wert-von-Daten-Studien oft auf eher künstliche Experimente und sehr spezielle Forschungskontexte konzentriert haben, untersucht diese Studie die Bereitschaft der Internetnutzer personenbezogene Daten im reinen Datenverkaufs-Kontext zu veräußern: auf Plattformen, die ausschließlich für diesen Zweck konzipiert wurden. Diese Plattformen sind ein vielversprechender Kontext, um die Verkaufsbereitschaft von Individuen zu untersuchen. Ein einfaches Übertragen der bereits bestehenden Ergebnisse früherer Forschung auf diesen Kontext ist dabei nicht möglich, wie die sehr heterogenen Ergebnisse vorausgehender Studien in anderen Kontexten zeigen.

Dennoch stimmen einige Ergebnisse mit denen früherer Studien anderer Kontexte überein, wie beispielsweise der Präferenz von Individuen nicht-identifizierbare Daten weiterzugeben (z.B. Benndorf und Normann 2014; Jentzsch 2014) oder der Ablehnung von Marketingzwecken zugunsten von Forschungszwecken (z.B. Cvrcek et al. 2006; Danezis et al. 2005). Allerdings identifiziert diese Studie im Rahmen von Datenverkaufsplattformen auch eine Reihe neuer Faktoren, die bisher nicht als Einflussfaktoren der Verkaufsbereitschaft von personenbezogenen Daten diskutiert wurden: Die Herkunft des Unternehmens, das Sicherheitsniveau und seine Vertrauenswürdigkeit sind Faktoren, die in früheren Studien bisher nicht berücksichtigt wurden. Insgesamt konnten durch die qualitative Studie zwölf

induktiv abgeleitete Einflussfaktoren identifiziert werden, die sich auf die Verkaufsbereitschaft von personenbezogenen Daten auf Datenverkaufsplattformen auswirken. Nach bestem Wissen und Gewissen ist dies die erste Studie, die die Faktoren, welche für Individuen bei der Beurteilung des Wertes, den sie ihren personenbezogenen Daten beimessen, relevant sind, mit einem induktiven Ansatz identifiziert hat. Diese sollten in zukünftigen Studien mitberücksichtigt werden, die darauf abzielen, die Bereitschaft von Individuen zum Verkauf von Daten auf Datenverkaufsplattformen besser zu verstehen.

Die zweite Implikation betrifft die durchschnittlichen Wichtigkeiten, die Individuen einer Auswahl der Faktoren, die in der qualitativen Studie identifiziert wurden, zuordneten. Eine wichtige Erkenntnis ergab sich dabei bereits in der Designphase der Conjoint-Analyse. Auf Grundlage der durchgeführten Interviews konnten drei Knock-out-Kriterien für potenzielle Nutzer von Datenverkaufsplattformen identifiziert werden: keine Weitergabe an Dritte, das Recht auf Löschung und einmalige Geschäfte als Zeitrahmen. Diese Faktoren scheinen wie Inhibitoren zu wirken (Cenfetelli 2004; Cenfetelli und Schwarz 2011) und zu verhindern, dass Internetnutzer tatsächlich bereit sind, ihre Daten zu verkaufen. Daher sollten diese Faktoren in zukünftigen Studien zur Messung der Verkaufsbereitschaft von personenbezogenen Daten besonders sorgfältig behandelt werden. Darüber hinaus zeigte sich, dass die Höhe der Kompensation in diesem Zusammenhang der wichtigste Faktor ist, gefolgt von dem Datentyp, der Herkunft des Providers und dem geltenden Recht, sowie des Verwendungszweckes. Als weniger wichtig stellten sich hingegen die Form der Kompensation sowie die Sicherheit heraus. Zukünftige Studien, welche die Daten-Verkaufsbereitschaft von Individuen im Rahmen von Datenverkaufsplattformen untersuchen, sollten sich dieser Unterschiede in der Wichtigkeit bewusst sein, wenn sie sich auf bestimmte Faktoren konzentrieren.

Drittens konnten unter den Teilnehmern vier verschiedene Gruppen mit ähnlichen Präferenzmustern identifiziert werden: die monetär-motivierten, die Standort-bewussten, die Datentyp-bewussten Individuen sowie die Personen mit homogen verteilten Präferenzen. Es zeigt sich also, dass die durchschnittlichen Wichtigkeiten der Attribute und die Wahrnehmungen der Nützlichkeiten unter den Individuen durchaus unterschiedlich sind. Eine detailliertere Betrachtung des Attributes Höhe der Kompensation zeigt beispielsweise, dass es einer Gruppe von Befragten mit großem Abstand das wichtigste Attribut ist, für die anderen drei Gruppen war es allerdings nur auf dem zweiten oder sogar erst dritten Platz.

Zusätzlich zu den theoretischen Implikationen, hält die Studie auch **praktische Erkenntnisse** für Anbieter und Kunden von Datenverkaufsplattformen sowie kaufenden

Partnerunternehmen bereit. Für die Anbieter von solchen Plattformen bietet diese Studie eine Liste von Einflussfaktoren und Inhibitoren an, die bei der Gestaltung von Datenverkaufsplattformen berücksichtigt werden sollten. Darüber hinaus werden auch die durchschnittlichen Wichtigkeiten für sechs dieser Faktoren errechnet und Erkenntnisse über mögliche Ausprägungsformen bereitgestellt. Basierend auf den Nutzenveränderungen und den Euro-Äquivalenten dieser, liefert die Studie Erkenntnisse über mögliche Preisgestaltungsstrategien für solche Plattformen. Darüber hinaus veranschaulicht die Studie, wie die aus Nutzersicht bevorzugte Datenverkaufsplattform aussehen würde. Unter Berücksichtigung der identifizierten Faktoren können Anbieter die Bereitschaft potenzieller Nutzer, personenbezogene Daten zu verkaufen, besser einschätzen und die Adoption der Plattformen beeinflussen, indem sie diese nach den Wünschen der Nutzer und unter Berücksichtigung individueller Präferenzen ausgestalten. So ist beispielsweise zu beachten, dass die Kompensation angemessen sein sollte und dass Internetnutzer den Verkauf von Adressdaten für Werbezwecke am wenigsten favorisieren. Eine derartige Einbeziehung der Kundenwünsche würde dazu führen, dass die Nutzer solcher Plattformen eine aktivere Rolle im Datenhandelsprozess spielen, was wiederum zu einer erhöhten Fairnesswahrnehmung beitragen kann.

6.6.2 Limitationen und weiterer Forschungsbedarf

In diesem Abschnitt werden die Limitationen der Studie sowie mögliche, zukünftige Forschungsrichtungen aufgezeigt. Die erste Limitation betrifft die Gegebenheit, dass die Geschäftsmodelle von Datenverkaufsplattformen einen innovativen Charakter haben und die zugrundeliegende Prämisse des Handels mit personenbezogenen Daten für die meisten Individuen eine neue Idee darstellen. Daher mussten die Teilnehmer dieser Studie zunächst grundlegende Informationen zu den Plattformen und ihren Funktionalitäten angezeigt bekommen, was durch textbasierte Beschreibungen und Mockups realisiert wurde. Es ist nicht von der Hand zu weisen, dass diese weniger realistisch als echte Webseiten sind. Dennoch sind hypothetische Szenarien eine gängige Praxis in der Forschung (z.B. Malhotra et al. 2004) und aufgrund dieser Mockups konnten Variationen in der Funktionalität, dem Branding und Marketing verschiedener Plattformen ausgeschlossen werden und der Fokus auf Aspekte gelegt werden, die für diese Studie wirklich relevant waren.

Eine zweite Limitation ergibt sich dadurch, dass die Daten in Deutschland erhoben wurden und daher kein Vergleich der Ergebnisse zwischen verschiedenen Ländern vorgenommen werden kann. Datensamples aus anderen Ländern könnten zusätzliche Faktoren identifizieren,

die sich auf die Bereitschaft zum Verkauf personenbezogener Informationen auf Datenverkaufsplattformen auswirken könnten, und auch die relativen Wichtigkeiten zwischen diesen Faktoren können ebenfalls variieren. Folglich könnte zukünftige Forschung diese Studie mit einem interkulturellen Sample wiederholen, was, wie diese Ergebnisse bereits zeigen, von besonderem Interesse wäre, da die Herkunft des Plattformproviders und ihr rechtlicher Rahmen für die deutschen Teilnehmer tatsächlich wichtig waren. Daher wäre es besonders interessant zu sehen, wie ein außereuropäisches Sample die verschiedenen Optionen in Bezug auf die Herkunft der Plattform bewerten würde.

Eine dritte Limitation betrifft die Notwendigkeit, einige der zwölf in der qualitativen Studie identifizierten Einflussfaktoren aufgrund methodischer Anforderungen von der Conjoint-Analyse auszuschließen. Die Ergebnisse dieser Studie helfen bereits, eine Vielzahl der Einflussfaktoren auf die Daten-Verkaufsbereitschaft von Internetnutzern zu verstehen und können als Ausgangspunkt für die weitere Untersuchung zum Wert von Informationen dienen. Zukünftige Untersuchungen könnten diese Ergebnisse als Grundlage nehmen, um weitere Studien auf Datenverkaufsplattformen durchzuführen, da dieser Kontext in der Forschung des Wertes von Daten aufgrund ihres natürlichen Zweckes von besonderer Bedeutung sein sollte.

Im nächsten Kapitel werden die Ergebnisse dieser und der vorangegangenen Studien nochmals zusammengefasst und der übergeordnete, wissenschaftliche und praxisrelevante Beitrag dieser Dissertation sowie weitere Forschungspotenziale aufgezeigt.

7 Zusammenfassung und Ausblick[10]

Diese Arbeit schließt wie sie beginnt, und zwar mit einem Auszug aus der Rede von Miglena Kuneva vor der Europäischen Kommission. Frau Dr. Kuneva resümierte dabei: *"Personal data is the new oil of the internet and the new currency of the digital world. We accept this reality because it is one chosen by users. Internet users have massively opted for free services offered in exchange for acceptance of advertisement. […] Tools must now be developed that balance the interests of business with that of the consumers. This means two things: the respect of users' right to control their public exposure; and the obligation to protect them against abusive and risky practices targeted at them."* (Kuneva 2009).

Mit diesem Zitat beschreibt die damalige EU-Kommissarin treffend die Begebenheiten, die sich durch die stetig wachsende Verwendung und Kommerzialisierung von personenbezogenen Daten in der digitalen Ökonomie ergeben. Diese Umstände bilden den Hintergrund, der diese Arbeit geprägt hat. Schließlich nehmen personenbezogene Daten und Informationen in Wirtschaft und Gesellschaft einen hohen Stellenwert ein. Ihre Verwendung und Analyse bringt für Unternehmen und Nutzer sowohl Vorteile als auch Risiken mit sich (Acquisti et al. 2016), wobei die Risiken für die Nutzer größer zu sein scheinen als für die Unternehmen (Li et al. 2014). Dennoch haben sich die Nutzer vermehrt für datenbasierte Dienste und Angebote der Unternehmen entschieden, wie beispielsweise die Nutzerzahlen von Facebook, Instagram und Twitter belegen (Facebook 2019; Techcrunch 2018; Twitter 2019). Daher ist es notwendig die Privatsphäre der Individuen zu schützen und den unsachgemäßen Gebrauch der Daten zu unterbinden, indem den Nutzern mehr Kontrolle über ihre Daten ermöglicht wird. Acquisti et al. (2016, S. 477) beschreiben Privatsphäre in diesem Zusammenhang als das Finden eines Gleichgewichtes auf einem Kontinuum zwischen dem Öffentlichen, das ein Individuum in einem bestimmten Kontext zu teilen bereit ist, und dem Privaten, das die Person schützen möchte. Vor diesem Hintergrund, so führen die Autoren weiter aus, *"neither does the sharing of certain information with others imply, per se, a loss of privacy, nor is the complete hiding of data necessary for the protection of privacy"* (Acquisti

[10] Dieses Kapitel basiert auf den Studien Gerlach et al. (2019), Wagner et al. (2018), Wessels et al. (2019b) und Wessels et al. (2019a)

et al. 2016, S. 477). Daher ist die Erforschung von Datenpraktiken wichtig, deren Umgang mit Informationen und Privatsphäre von Anbieter- und Anwenderseite akzeptiert werden und sie ihre jeweiligen Interessen vertreten sehen. Folglich bedarf es Ansätzen, die Nutzern mehr Kontrolle über ihre Daten und Privatsphäre geben und es Unternehmen weiterhin ermöglichen, ihr Geschäft zu erfüllen und profitabel zu bleiben.

Die vorliegende Arbeit gliedert sich in die Literatur zur Erforschung solcher Privatsphäre-freundlicher Datenpraktiken ein, indem eine Analyse der Bedeutung von Privatsphäre aus der Unternehmens- und Nutzerperspektive vorgenommen wurde, um so Erkenntnisse über die Anforderungen beider Seiten gleichermaßen gewinnen zu können. Dabei wurde zunächst aus Unternehmensperspektive untersucht, wie Organisationen mit dem Spannungsverhältnis zwischen ihrem Informationsbedarf, der mit Privatsphäre-Einschnitten einhergehen kann, und ihrem Bedarf zur Gewinnung und Bindung von Nutzern, die einen adäquaten Privatsphäre-Schutz fordern, einhergehen. Anschließend untersuchte diese Arbeit den monetären Wert, den Individuen ihren personenbezogenen Informationen und damit ihrer Privatsphäre beimessen und geht in diesem Zuge auch auf einen möglichen alternativen Ansatz für Datenpraktiken ein. Die folgenden Abschnitte fassen die wichtigsten Erkenntnisse der vorliegenden Arbeit nochmals zusammen und gehen dabei detaillierter auf den übergeordneten, wissenschaftlichen und praxisrelevanten Beitrag dieser Dissertation ein. Darauf aufbauend werden im Anschluss potenzielle, zukünftige Forschungsrichtungen vorgestellt.

7.1 Wissenschaftlicher Beitrag der Arbeit

Die vorliegende Arbeit gliedert sich in Untersuchungen der Unternehmens- und Nutzerperspektive auf Privatsphäre und personenbezogene Nutzerdaten auf. Die Studie des 3. Kapitels konnte dabei aus organisationaler Perspektive zeigen, dass der Zielkonflikt zwischen dem Umgang mit Nutzerdaten und der Privatsphäre der Individuen erhebliche Herausforderungen für Unternehmen mit sich bringt, die sich in vier verschiedenen Spannungsfeldern ausdrücken können. Schließlich ist einerseits die Erfüllung des Bedarfes der Unternehmen zur Erfassung und Verwendung von Nutzerinformationen mit einem gewissen Grad an Datenschutzverletzungen verbunden, die wiederum (potenzielle) Kunden abschrecken können. Dagegen kann der Schutz der Privatsphäre der Nutzer durch die Erhebung und Verwendung weniger personenbezogener Daten von Vorteil sein, um Kunden zu gewinnen, vernachlässigt aber den Informationsbedarf der Unternehmen. Durch die im 3. Kapitel dieser Arbeit vorgestellte Analyse und daraus entwickelte *Grounded Theory* zeigte sich, dass Unternehmen versuchen, diese gegensätzlichen Anforderungen auszugleichen, um

wettbewerbsfähig zu bleiben. Sie operieren dabei aber in einem turbulenten Umfeld, in dem interne und externe Belastungen sie in ihrem Gleichgewicht stören können. Vor diesem Hintergrund wurde Ambidextrie als Meta-Theorie eingeführt, die auch in zukünftiger Privatsphäre-Forschung aus Unternehmenssicht berücksichtigt werden sollte. Darüber hinaus konnten drei Kategorien von Taktiken identifiziert werden, die von den Unternehmen angewandt werden, um mit den negativen Auswirkungen ihrer Entscheidungen über die Erhebung und Verwendung von Nutzerdaten umzugehen. Diese helfen auch dabei, das Gleichgewicht nach einer Störung wiederherzustellen oder proaktiv zu sichern.

Die aus der Unternehmensperspektive gewonnenen Erkenntnisse werden durch die Beiträge der Studien aus der Nutzerperspektive erweitert. Dabei untersucht die vorliegende Arbeit in den Kapiteln 4 bis 6 den monetären Wert, den Individuen ihren personenbezogenen Informationen und damit ihrer Privatsphäre zuweisen. Auf diese Weise leistet diese Arbeit einen Beitrag zur Forschung der Ökonomie von Privatsphäre, welche auf die Untersuchung von „*measurable, or at least assessable, privacy components*“ (Acquisti et al. 2016, S. 449) fokussiert ist. Dies ist wichtig, damit Internetnutzer die Vor- und Nachteile, die mit der Nutzung eines Onlinedienstes und der damit einhergehenden Preisgabe ihrer Daten abwägen und so fundierte Entscheidungen für oder gegen die Adoption treffen können (Carrascal et al. 2013). Schließlich argumentierte schon Laudon (1997, S. 2), dass Datenpraktiken, welche die Nutzer nicht am Erfolg der Kommerzialisierung von Daten teilhaben lassen, die Preise für personenbezogene Daten so sinken lassen, dass sie die tatsächlichen sozialen Kosten des Umgangs mit personenbezogenen Daten nicht widerspiegeln. Dies lässt wiederrum auch die Hemmschwelle für Privatsphäre-Verletzungen weiter sinken (Laudon 1997, S. 2), welchen durch ein besseres Verständnis zur Wertvorstellung von Individuen entgegengewirkt werden soll.

Vor diesem Hintergrund fasst die strukturierte Literaturrecherche des 4. Kapitels dieser Arbeit bisherige Forschungserkenntnisse zu dem Wert, den Individuen ihren personenbezogenen Informationen zuweisen, zusammen und gibt einen umfassenden Überblick über die empirischen Studien aus Nutzerperspektive. Insgesamt sind 37 Publikationen in die Literaturrecherche eingeflossen. Die Recherche ist dabei die erste Studie, welche die bisherigen Ansätze und Ergebnisse zur Bewertung des Wertes von Privatsphäre einheitlich mit Hilfe eines integrativen, theoretischen Frameworks konzeptualisiert. Es zeigte sich, dass der Wert von Daten von einer Reihe von Faktoren beeinflusst wird: Neben der Methode, die zur Messung der Wertvorstellung der Individuen herangezogen wird, hat auch der Datentyp

sowie eine Reihe weiterer Untersuchungsfaktoren Einfluss auf den monetären Wert von Privatsphäre, die zusammen den Kontext der Studien bilden. Die bisherigen Studien variieren stark in diesen Faktoren und liefern so für die jeweiligen Kontexte wertvolle Erkenntnisse zum Wert von Daten, wohingegen einheitliche, generalisierbare Ergebnisse schwer zu entwickeln sind.

Basierend auf der Erkenntnis der Literaturrecherche zum Einfluss, den die Messmethode auf die Wertermittlung von Daten haben kann, untersucht die Studie des 5. Kapitels der vorliegenden Arbeit mit Hilfe einer Feldstudie eine neue, vielversprechende Methode zur Messung des Wertes von Daten: eine *Name-Your-Own-Price* Auktion mit Option des wiederholten Bietens. Diese Methode bietet den Vorteil, dass Individuen Rückmeldung zu überhöhten Geboten bekommen und diese Ablehnung als Informationsquelle nutzen können (Liu et al. 2016), um ihre Verkaufsbereitschaft nochmals zu überdenken und angepasste Gebote abzugeben. Den Individuen kann die Wertermittlung so erleichtert werden, ohne sie dabei zu stark zu ankern, da kein Referenzwert genannt wird (Tversky und Kahneman 1974). Vielmehr können sie ihren intern generierten Wert auf Grundlage des subtilen Feedbacks nochmals überdenken und sich dann sequentiell ihrer individuellen, niedrigsten Verkaufsbereitschaft nähern (Hann und Terwiesch 2003; Hinz et al. 2011; Terwiesch et al. 2005). Die Untersuchung wurde mit Hilfe einer Feldstudie durchgeführt, bei der die Studienteilnehmer Selfies zu Werbezwecken an die Universität verkaufen konnten. Insgesamt waren 39% der Teilnehmer bereit, ihr Selfie zu spenden oder zu verkaufen, wobei der Median bei 5 Euro lag und die Mehrzahl der Teilnehmer ihre Chance, mehrfach zu bieten, wahrgenommen hat. Weiterhin konnten verschiedene Cluster der Bieter identifiziert werden, was zeigt, wie individuell die Wertvorstellung von Daten ist.

Dieses Ergebnis konnte die Studie des 6. Kapitels dieser Arbeit bestätigen. Die Studie untersucht den Wert von Daten innerhalb eines bislang unerforschten, natürlichen Forschungskontextes: den Datenverkaufsplattformen. Da diese Plattformen ausschließlich für den Kauf und Verkauf personenbezogener Daten konzipiert sind, eignen sie sich sehr gut, um den reinen monetären Wert zu untersuchen, den Nutzer ihren personenbezogenen Daten beimessen. Zur Untersuchung dessen wurde eine zweistufige Studie durchgeführt. Dabei wurden im ersten, qualitativen Schritt induktiv Einflussfaktoren auf die Bereitschaft, personenbezogene Informationen auf diesen Plattformen zu verkaufen, identifiziert. Insgesamt konnten zwölf Faktoren gefunden werden, die zum Teil die Einflussfaktoren anderer Kontexte bestätigten, teilweise aber auch neu entdeckt wurden. In einem zweiten

Schritt wurde darauf aufbauend untersucht, welche relativen Gewichte die befragten Internetnutzer einer Teilmenge dieser Einflussfaktoren zuordnen und ob es unterschiedliche Präferenzmuster gibt. Drei der Faktoren konnten als Knock-out-Kriterien identifiziert werden, die als Inhibitoren zu wirken scheinen (Cenfetelli 2004; Cenfetelli und Schwarz 2011). Darüber hinaus konnte die Höhe der monetären Vergütung als der wichtigste Faktor identifiziert werden, während die Befragten die Sicherheit als am wenigsten wichtig erachteten. Weiterhin konnten unter den Teilnehmern vier verschiedene Gruppen mit ähnlichen Präferenzmustern identifiziert werden und so gezeigt werden, dass die durchschnittlichen Wichtigkeiten der Faktoren und die Wahrnehmungen der Nützlichkeiten unter den Individuen durchaus unterschiedlich sind.

7.2 Beitrag der Arbeit für die Unternehmenspraxis

Die vorliegende Arbeit trägt zu einem verbesserten Verständnis der Bedeutung von Privatsphäre und personenbezogenen Daten aus Nutzer- und Unternehmensperspektive bei, welches auch auf praktischer Ebene von Relevanz ist. Die im 3. Kapitel entwickelte *Grounded Theory* mit Ambidextrie als meta-theoretischer Grundlage zeigt, dass Unternehmen ein Gleichgewicht zwischen den beiden konkurrierenden Anforderungen ihres Informationsbedarfes und dem Schutz ihrer Nutzerdaten anstreben sollten. Die gewonnenen Erkenntnisse über die Spannungen und Taktiken können Anbietern von Online-Diensten dabei helfen, Entscheidungen über ihre Datenpraktiken zu treffen, um so das Gleichgewicht aufrechterhalten oder nach einer Störung wiederherstellen zu können. So können die mit bestimmten Praktiken verbundenen Nachteile besser diskutiert und berücksichtigt werden.

Die Untersuchungen des Wertes von personenbezogenen Daten und Privatsphäre leisten wiederum einen praktischen Beitrag, indem sie Individuen helfen den Abwägungsprozess zwischen den Vor- und Nachteilen der Offenlegung ihrer Daten fundierter treffen zu können (Carrascal et al. 2013). Weiterhin sind diese Erkenntnisse auch für die Unternehmen hilfreich, die ihre Dienste entsprechend ausgestalten können. Dies hilft, dem übergeordneten Ziel von Privatsphäre-freundlichen Datenpraktiken, die Anbieter und Anwender gleichermaßen akzeptieren, näher zu kommen. Schließlich zeigt die Literaturrecherche des 4. Kapitels dieser Arbeit auf, wie vielschichtig die Faktoren sind, die die Wertvorstellung der Individuen bezüglich ihrer Daten beeinflussen und somit auch welche Auswirkungen diese für den Onlinedienst haben können. Darüber hinaus zeigte die Studie des 5. Kapitels, dass es für Individuen durchaus kognitiv herausfordernd ist, ihren Wert für personenbezogene Daten unvermittelt anzugeben, was aber durch geeignete Methoden, wie die *Name-Your-Own-Price*

Auktion mit wiederholter Biet-Option, erleichtert werden kann. Dies ist auch vor dem Hintergrund von immer neu entstehenden Datenverkaufsplattformen hilfreich (Jentzsch 2014), die so ihre Preise und damit generell ihre Geschäftserfolge validieren können. Schließlich könnten diese Plattformen ein alternativer Ansatz für gängige Datenmarktplätze sein, auf denen Nutzerinformationen ohne die Partizipation der Datenpreisgebenden gehandelt werden (Acquisti et al. 2016; Spiekermann et al. 2015a; Spiekermann et al. 2015b). Darüber hinaus weisen die Ergebnisse der Studie des 6. Kapitels Anbieter solcher Datenverkaufsplattformen auf wichtige Einflussfaktoren und mögliche Ausprägungsformen hin, die bei der Gestaltung der Plattformen berücksichtigt werden sollten, um die Akzeptanz von potenziellen Nutzern zu erhöhen. In diesem Zusammenhang veranschaulicht die Studie auch, wie die aus Sicht der Studienteilnehmer bevorzugte Datenverkaufsplattform aussehen würde und geben weitere Hinweise über mögliche Preisgestaltungsstrategien.

7.3 Zukünftiges Forschungspotenzial

Die vorliegende Arbeit leistet einen Beitrag zur Erforschung des übergeordneten Zieles zur Entwicklung Privatsphäre-freundlicher Datenpraktiken. Allerdings besteht noch weiterer Forschungsbedarf und die durch diese Arbeit gewonnenen Erkenntnisse sollten durch zukünftige Untersuchungen erweitert werden. Dabei ist eine integrierte Sichtweise der Anbieter als auch der Anwender von Onlinediensten notwendig, um zu Ergebnissen zu kommen, die für alle beteiligten Interessensgruppen zufriedenstellend sind. Schließlich sollten Datenverarbeitungspraktiken ein Gleichgewicht zwischen der Preisgabe und dem Schutz personenbezogener Daten anstreben, das den Interessen der verschiedenen Parteien am besten dient (Acquisti et al. 2016, S. 448).

Dabei konnte in dieser Arbeit bereits gezeigt werden, dass viele verschiedene Faktoren einen Einfluss darauf haben, wie viel Nutzern ihre Privatsphäre wert ist. In ähnlicher Weise könnten auch die gängigen Datenpraktiken zwischen Internetnutzern verschieden wahrgenommen werden und von unterschiedlichen Faktoren abhängen. Eine Untersuchung dessen könnte interessante Erkenntnisse liefern.

Weiterhin könnte der Zielkonflikt der Unternehmen noch weiter untersucht werden, beispielsweise dahingehend, welche von den Unternehmen bereits verwendeten Taktiken aus Nutzerperspektive am meisten akzeptiert sind und zu den größten Erfolgen führen. Schließlich resümierte diese Arbeit, dass Unternehmen nicht starr auf eine Strategie beim Umgang mit ihren Nutzerdaten festgelegt sind, sondern durch sich ergebenden Begebenheiten

und internen sowie externen Druck immer neuen Entscheidungen gegenüberstehen und flexibel reagieren müssen.

Zu guter Letzt konnte durch diese Arbeit gezeigt werden, dass der Ansatz der Datenverkaufsplattformen aus Nutzerperspektive unter bestimmten, designtechnischen Ausgestaltungen adoptiert werden würde. Dabei können allerdings noch keine Rückschlüsse zur Unternehmenssichtweise geschlossen werden. Zukünftige Forschung sollte daher untersuchen, ob Unternehmen das Konzept von Datenverkaufsplattformen unter diesen Bedingungen ebenfalls annehmen würden und diese als Ersatz für die gängigen Datenmarktplätze genutzt werden könnten. Schließlich hat die Studie aus dem 3. Kapitel gezeigt, dass Unternehmen sehr wohl unter dem Trade-off zwischen ihrem Informationsbedarf und den Privatsphäre-Bedenken ihrer Nutzer leiden und nach Alternativen suchen.

Literaturverzeichnis

Accenture. 2015. "Guarding and Growing Personal Data Value." Abgerufen am 25.11.2017, von https://www.accenture.com/_acnmedia/PDF-4/Accenture-Guarding-and-Growing-Personal-Data-Value-POV-Low-Res.pdf.

Ackoff, R. L. 1989. "From Data to Wisdom," *Journal of Applied Systems Analysis* (16:1), S. 3-9.

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

Acquisti, A. 2010. "The Economics of Personal Data and the Economics of Privacy," *Heinz College at Research Showcase*, S. 1-50.

Acquisti, A., Brandimarte, L., und Loewenstein, G. 2015. "Privacy and Human Behavior in the Age of Information," *Science* (347:6221), S. 509-514.

Acquisti, A., und Grossklags, J. 2005. "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy* (3:1), S. 26-33.

Acquisti, A., und Grossklags, J. 2007. "What Can Behavioral Economics Teach Us About Privacy," *Digital Privacy: Theory, Technologies and Practices* (18), S. 363-377.

Acquisti, A., John, L. K., und Loewenstein, G. 2009. "What Is Privacy Worth?," in: *Twenty First Workshop on Information Systems and Economics (WISE)*. Phoenix, AZ: S. 1-39.

Acquisti, A., Taylor, C., und Wagman, L. 2016. "The Economics of Privacy," *Journal of Economic Literature* (54:2), S. 442-492.

Acxiom. 2019. "People-Based Marketing." Abgerufen am 09.01.2019, von https://www.acxiom.de/.

Adler, P. S., Goldoftas, B., und Levine, D. I. 1999. "Flexibility Versus Efficiency? A Case Study of Model Changeovers in the Toyota Production System," *Organization Science* (10:1), S. 43-68.

Al-Fedaghi, S. S. 2005. "How to Calculate the Information Privacy," in: *PST*. S. 3-13.

Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Belmont, California: Wadsworth Publishing Company, Inc.

Amaldoss, W., und Jain, S. 2008. "Joint Bidding in the Name-Your-Own-Price Channel: A Strategic Analysis," *Management Science* (54:10), S. 1685-1699.

Andriopoulos, C., und Lewis, M. W. 2009. "Exploitation-Exploration Tensions and Organizational Ambidexterity: Managing Paradoxes of Innovation," *Organization Science* (20:4), S. 696-717.

Anton, A. I., Earp, J. B., He, Q., Stufflebeam, W., Bolchini, D., und Jensen, C. 2004. "Financial Privacy Policies and the Need for Standardization," *IEEE Security & Privacy* (2:2), S. 36-45.

Auh, S., und Menguc, B. 2005. "Balancing Exploration and Exploitation: The Moderating Role of Competitive Intensity," *Journal of Business Research* (58:12), S. 1652-1661.

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), S. 13-28.

Baker, T., und Nelson, R. E. 2005. "Creating Something from Nothing: Resource Construction through Entrepreneurial Bricolage," *Administrative Science Quarterly* (50:3), S. 329-366.

Bansal, G., und Zahedi, F. 2008. "The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation," in: *Proceedings of the Twenty Ninth International Conference on Information Systems (ICIS)*. Paris, France: S. 7.

Barak, O., Cohen, G., Gazit, A., und Toch, E. 2013. "The Price Is Right?: Economic Value of Location Sharing," in: *Proceedings of the 2nd ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication*. Zurich, Switzerland: ACM, S. 891-900.

Barrick, M. R., und Mount, M. K. 1991. "The Big Five Personality Dimensions and Job Performance: A Meta - Analysis," *Personnel Psychology* (44:1), S. 1-26.

Bauer, C., Korunovska, J., und Spiekermann, S. 2012. "On the Value of Information - What Facebook Users Are Willing to Pay," in: *Proceedings of the Twenthies European Conference on Information Systems (ECIS)*. Barcelona, Spain.

Baumeister, R. F., und Leary, M. R. 1997. "Writing Narrative Literature Reviews," *Review of General Psychology* (1:3), S. 311.

BBC. 2014. "Edward Snowden: Leaks That Exposed Us Spy Programme." Abgerufen am 09.01.2019, von https://www.bbc.com/news/world-us-canada-23123964.

Becker, G. M., DeGroot, M. H., und Marschak, J. 1964. "Measuring Utility by a Single - Response Sequential Method," *Behavioral Science* (9:3), S. 226-232.

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), S. 1017-1042.

Benndorf, V., und Normann, H. T. 2014. "The Willingness to Sell Personal Data," in: *Düsseldorf Institute for Competition Economics (DICE) Discussion Paper, No. 143.*, H.T. Normann (ed.). S. 1-17.

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

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

Berthold, S., und Böhme, R. 2010. "Valuating Privacy with Option Pricing Theory," in *Economics of Information Security and Privacy*. Springer, S. 187-209.

Bharosa, N., Luitjens, S., van Wijk, R., und Pardo, T. 2018. "Panel: Removing the Barriers for Personal Data Management," in: *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*. ACM, S. 125.

Birks, D. F., Fernandez, W., Levina, N., und Nasirin, S. 2013. "Grounded Theory Method in Information Systems Research: Its Nature, Diversity and Opportunities," *European Journal of Information Systems* (22:1), S. 1-8.

Bloustein, E. J. 1964. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser," *N.Y.U. Law Review* (39), S. 962.

Brandimarte, L., und Acquisti, A. 2012. "The Economics of Privacy," *The Oxford Handbook of the Digital Economy*, S. 547-571.

Braun, A., Schmeiser, H., und Schreiber, F. 2016. "On Consumer Preferences and the Willingness to Pay for Term Life Insurance," *European Journal of Operational Research* (253:3), S. 761-776.

Breidert, C., Hahsler, M., und Reutterer, T. 2006. "A Review of Methods for Measuring Willingness-to-Pay," *Innovative Marketing* (2:4), S. 8-32.

Brush, A., Krumm, J., und Scott, J. 2010. "Exploring End User Preferences for Location Obfuscation, Location-Based Services, and the Value of Location," in: *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*. Copenhagen, Denmark: S. 95-104.

Brustein, J. 2012. "Start-Ups Seek to Help Users Put a Price on Their Personal Data." *The New York Times* Abgerufen am 03.11.2017, von http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html?_r=1&ref=technology.

Brynjolfsson, E., Hitt, L. M., und Kim, H. H. 2011. "Strength in Numbers: How Does Data-Driven Decisionmaking Affect Firm Performance?," *SSRN*.

Bughin, J. 2011. "Digital User Segmentation and Privacy Concerns," *Journal of Direct, Data and Digital Marketing Practice* (13:2), S. 156-165.

Buxmann, P. 2018. "Der Preis des Kostenlosen: Das Spannungsfeld zwischen dem Wert von Daten und der Privatsphäre von Nutzern," in: *Ifo-Schnelldienst. - München: Institut für Wirtschaftsforschung*. S. 18-21.

Calo, R. 2014. "Digital Market Manipulation," *The George Washington Law Review* (82:4), S. 995-1051.

Campbell, A. J. 1997. "Relationship Marketing in Consumer Markets: A Comparison of Managerial and Consumer Attitudes About Information Privacy," *Journal of Direct Marketing* (11:3), S. 44-57.

Candidlyimages. 2018. "Frequently Asked Questions " Abgerufen am 16.08.2018, von https://www.candidlyimages.com/About/FAQ.

Cao, Q., Gedajlovic, E., und Zhang, H. 2009. "Unpacking Organizational Ambidexterity: Dimensions, Contingencies, and Synergistic Effects," *Organization Science* (20:4), S. 781-796.

Cardinal, L. B., Sitkin, S. B., und Long, C. P. 2004. "Balancing and Rebalancing in the Creation and Evolution of Organizational Control," *Organization Science* (15:4), S. 411-431.

Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., und de Oliveira, R. 2013. "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online," in: *Proceedings of the 22nd International Conference on World Wide Web*. ACM, S. 189-200.

Castells, M. 2010. "The Information Age," *Media Studies: A Reader* (2:7), S. 152.

Cenfetelli, R. T. 2004. "Inhibitors and Enablers as Dual Factor Concepts in Technology Usage," *Journal of the Association for Information Systems* (5:11), S. 472-492.

Cenfetelli, R. T., und Schwarz, A. 2011. "Identifying and Testing the Inhibitors of Technology Usage Intentions," *Information Systems Research* (22:4), S. 808-823.

Chan, Y. E., Culnan, M. J., Greenaway, K., Laden, G., Levin, T., und Smith, H. J. 2005. "Information Privacy: Management, Marketplace, and Legal Challenges," *Communications of the Association for Information Systems* (16:1), S. 270-298.

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

Charmaz, K. 2014. *Constructing Grounded Theory*, (2nd ed.). London, UK: Sage.

Chellappa, R. K., und Shivendu, S. 2010. "Mechanism Design for “Free” but “No Free Disposal” Services: The Economics of Personalization under Privacy Concerns," *Management Science* (56:10), S. 1766-1780.

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), S. 181-202.

Chen, H., Chiang, R. H., und Storey, V. C. 2012. "Business Intelligence and Analytics: From Big Data to Big Impact," *MIS Quarterly* (36:4), S. 1165-1188.

Chernev, A. 2003. "Reverse Pricing and Online Price Elicitation Strategies in Consumer Choice," *Journal of Consumer Psychology* (13:No. 1 & 2), S. 51-62.

Cheung, C. M., und Lee, M. K. 2006. "Understanding Consumer Trust in Internet Shopping: A Multidisciplinary Approach," *Journal of the Association for Information Science and Technology* (57:4), S. 479-492.

Cho, H., Lee, J.-S., und Chung, S. 2010. "Optimistic Bias About Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience," *Computers in Human Behavior* (26:5), S. 987-995.

Choi, B., Wu, Y., Yu, J., und Land, L. 2018. "Love at First Sight: The Interplay between Privacy Dispositions and Privacy Calculus in Online Social Connectivity Management," *Journal of the Association for Information Systems* (19:3), S. 124-151.

Choo, C. W. 1996. "The Knowing Organization: How Organizations Use Information to Construct Meaning, Create Knowledge and Make Decisions," *International Journal of Information Management* (16:5), S. 329-340.

Christin, D., Buchner, C., und Leibecke, N. 2013. "What's the Value of Your Privacy? Exploring Factors That Influence Privacy-Sensitive Contributions to Participatory Sensing Applications," in: *38th Conference on Local Computer Networks Workshops (LCN Workshops)*. Sydney, Australia: IEEE, S. 918-923.

Clarke, R. 1999a. "Internet Privacy Concerns Confirm the Case for Intervention," *Communications of the ACM* (42:2), S. 60-67.

Clarke, R. 1999b. "Introduction to Dataveillance and Information Privacy, and Definitions of Terms," in: *Roger Clarke's Dataveillance and Information Privacy Pages*.

CNBC. 2018. "Facebook Revamps Privacy Settings Ahead of Strict New EU Laws." Abgerufen am 11.02.2019, von https://www.cnbc.com/2018/01/29/facebook-revamps-privacy-settings-ahead-of-strict-new-eu-laws.html.

Cohen, J. 1992. "A Power Primer," *Psychological Bulletin* (112:1), S. 155.

Cohen, J. E. 2001. "Privacy, Ideology, and Technology: A Response to Jeffrey Rosen," *The Georgetown Law Journal* (89), S. 2029-2045.

Cohen, W. M., und Levinthal, D. A. 1990. "Absorptive Capacity: A New Perspective on Learning and Innovation," *Administrative Science Quarterly* (35:1), S. 128-152.

Corbett, J., und Mellouli, S. 2017. "Winning the SDG Battle in Cities: How an Integrated Information Ecosystem Can Contribute to the Achievement of the 2030 Sustainable Development Goals," *Information Systems Journal* (27:4), S. 427-461.

Costa, P. T., und McCrae, R. R. 2008. "The Revised Neo Personality Inventory (Neo-Pi-R)," *The SAGE Handbook of Personality Theory and Assessment* (2:2), S. 179-198.

Culnan, M. J. 1993. "" How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3), S. 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), S. 104-115.

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

Culnan, M. J., und Williams, C. C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches," *MIS Quarterly* (33:4), S. 673-687.

Cummings, L. L. 1981. "State of the Art* Organizational Behavior in the 1980s," *Decision Sciences* (12:3), S. 365-377.

Cvrcek, D., Kumpost, M., Matyas, V., und Danezis, G. 2006. "A Study on the Value of Location Privacy," in: *5th ACM Workshop on Privacy in Electronic Society (WPES)*. Alexandria, Virginia, USA: ACM, S. 109-118.

Danezis, G., Lewis, S., und Anderson, R. J. 2005. "How Much Is Location Privacy Worth?," in: *Workshop on the Economics of Information Security Series (WEIS)*. S. 1-13.

Datacoup. 2018. "Datacoup - How It Works." Abgerufen am 06.12.2018, von http://datacoup.com/docs#how-it-works.

DataFairplay. 2018. "Die Idee, die alles ändert." Abgerufen am 06.12.2018, von https://www.datafairplay.com/die-idee/.

Datawallet. 2018. "Datawallet - Take Control of Your Data." Abgerufen am 22.12.2018, von https://datawallet.com/#.

Dauda, S. Y., und Lee, J. 2015. "Technology Adoption: A Conjoint Analysis of Consumers′ Preference on Future Online Banking Services," *Information Systems* (53), S. 1-15.

Davenport, T. H. 2010. "Business Intelligence and Organizational Decisions," *International Journal of Business Intelligence Research (IJBIR)* (1:1), S. 1-12.

Davies, S. G. 1998. "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity," in *Technology and Privacy: The New Landscape*, P.E. Agre and M. Rotenberg (eds.). Cambridge, Massachusetts & London, England: The MIT Press, S. 143-165.

Dawar, N., und Pillutla, M. M. 2000. "Impact of Product-Harm Crises on Brand Equity: The Moderating Role of Consumer Expectations," *Journal of Marketing Research* (37:2), S. 215-226.

DDMA. 2016. "Ddma Privacy Monitor 2016 - What Consumers Currently Think About Data." Abgerufen am 25.07.2018, von https://ddma.nl/download/53179/.

Detwiler, B. 2015. "Big Data Is a Competitive Advantage Companies Can No Longer Ignore." Abgerufen am 30.12.2018 von http://www.zdnet.com/article/big-data-is-a-competitive-advantage-companies-can-no-longer-ignore/.

Diamantoulakis, P. D., Kapinas, V. M., und Karagiannidis, G. K. 2015. "Big Data Analytics for Dynamic Energy Management in Smart Grids," *Big Data Research* (2:3), S. 94-101.

digi.me. 2018. "Take Control of the Data Powering Your Digital Life." Abgerufen am 06.12.2018, von https://digi.me/.

DigitalTrends. 2016. "Runkeeper Is the Latest Mobile App to Run Afoul of Privacy Advocates." Abgerufen am 11.02.2019, von https://finance.yahoo.com/news/runkeeper-tracking-background-selling-advertisers-204216046.html.

Dinev, T., und Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), S. 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), S. 639-655.

DW. 2018. "Taxes Coming to Big Data in Germany?" Abgerufen am 24.07.2018, von https://www.dw.com/en/taxes-coming-to-big-data-in-germany/a-43972540.

Economist. 2017a. "Fuel of the Future: Data Is Giving Rise to a New Economy." Abgerufen am 12.08.2018, von https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy.

Economist. 2017b. "Regulating the Internet Giants - the World’s Most Valuable Resource Is No Longer Oil, but Data." Abgerufen am 11.08.2018, von https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

Egelman, S., Cranor, L. F., und Hong, J. 2008. "You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings," in: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, S. 1065-1074.

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

Egelman, S., Tsai, J., Cranor, L. F., und Acquisti, A. 2009. "Timing Is Everything?: The Effects of Timing and Placement of Online Privacy Indicators," in: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, S. 319-328.

Einav, L., Jenkins, M., und Levin, J. 2013. "The Impact of Credit Scoring on Consumer Lending," *The RAND Journal of Economics* (44:2), S. 249-274.

Eisenhardt, K. M. 1989. "Making Fast Strategic Decisions in High-Velocity Environments," *Academy of Management Journal* (32:3), S. 543-576.

Eisenhardt, K. M., Furr, N. R., und Bingham, C. B. 2010. "Crossroads—Microfoundations of Performance: Balancing Efficiency and Flexibility in Dynamic Environments," *Organization Science* (21:6), S. 1263-1273.

Eisenhardt, K. M., und Graebner, M. E. 2007. "Theory Building from Cases: Opportunities and Challenges," *The Academy of Management Journal* (50:1), S. 25-32.

Engelbrecht, A., Gerlach, J., und Widjaja, T. 2016. "Understanding the Anatomy of Data-Driven Business Models-Towards an Empirical Taxonomy," in: *Proceedings of the Twenty-Fourth European Conference on Information Systems (ECIS)*. İstanbul, Turkey: S. 1-15.

Etzioni, A. 2005. "The Limits of Privacy," *Contemporary Debates in Applied Ethics. Oxford: Blackwell*, S. 253-262.

EuropeanCommission. 2019. "Building a European Data Economy." Abgerufen am 16.02.2019, von https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.

Evans, P. B., und Wurster, T. S. 1997. *Strategy and the New Economics of Information*. Harvard Business Review New York, NY.

Facebook. 2018. "Terms of Service." Abgerufen am 28.08.2018, von https://www.facebook.com/terms.php.

Facebook. 2019. "Facebook Q4 2018 Results." Abgerufen am 20.02.2019, von https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q4/Q4-2018-Earnings-Presentation.pdf.

Farrell, J. 2012. "Can Privacy Be Just Another Good," *Journal on Telecommunications and High Technology Law* (10), S. 251.

FastCompany. 2016. "This Startup Lets Users “Sell” Their Own Shopping Data." Abgerufen am 06.12.2018, von https://www.fastcompany.com/3056265/this-startup-lets-users-sell-their-own-shopping-data.

Fay, S. 2004. "Partial-Repeat-Bidding in the Name-Your-Own-Price Channel," *Marketing Science* (23:3), S. 407-418.

Fay, S., und Zeithammer, R. 2016. "Bidding for Bidders? How the Format for Soliciting Supplier Participation in NYOP Auctions Impacts Channel Profit," *Management Science* (63:12), S. 4324-4344.

FAZ. 2018. "Merkel will Daten besteuern." Abgerufen am 11.06.2018, von http://www.faz.net/aktuell/wirtschaft/diginomics/radikale-steuerreform-merkel-will-daten-besteuern-15612688.html.

Feldman, M. S., und March, J. G. 1981. "Information in Organizations as Signal and Symbol," *Administrative Science Quarterly* (26:2), S. 171-186.

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

Flavián, C., und Guinalíu, M. 2006. "Consumer Trust, Perceived Security and Privacy Policy: Three Basic Elements of Loyalty to a Web Site," *Industrial Management & Data Systems* (106:5), S. 601-620.

Foap. 2018. "Foap General Terms of Use and Trade Terms." Abgerufen am 16.08.2018, von https://www.foap.com/terms.

Fortune. 2016. "Maker of Popular Running App Admits It Did Track Users Too Much." Abgerufen am 11.02.2019, von http://fortune.com/2016/05/18/runkeeper-privacy-bug/.

Friedman, E. J., und Resnick, P. 2001. "The Social Cost of Cheap Pseudonyms," *Journal of Economics & Management Strategy* (10:2), S. 173-199.

Geminn, C., und Roßnagel, A. 2015. "Privatheit und Privatsphäre aus der Perspektive des Rechts–Ein Überblick," *JuristenZeitung* (70:14), S. 703-708.

Genkina, A., und Camp, L. J. 2005. "Re-Embedding Existing Social Networks into Online Experiences to Aid in Trust Assessment," *SSRN*.

Gerlach, J. P., Eling, N., Wessels, N., und Buxmann, P. 2019. "Flamingos on a Slackline: Companies' Challenges of Balancing the Competing Demands of Handling Customer Information and Privacy," *Information Systems Journal* (29:2), S. 548-575.

Gibson, C. B., und Birkinshaw, J. 2004. "The Antecedents, Consequences, and Mediating Role of Organizational Ambidexterity," *Academy of Management Journal* (47:2), S. 209-226.

Glaser, B. (ed.) 1978. *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory*. Mill Valley, CA: Sociology Press.

Glaser, B., und Strauss, A. 1967. *The Discovery of Grounded Theory*. Hawthorne, NY: Aldine Publishing Company.

Granados, N., und Gupta, A. 2013. "Transparency Strategy: Competing with Information in a Digital World," *MIS Quarterly* (37:2), S. 637-641.

Green, P. E., und Krieger, A. M. 1991. "Segmenting Markets with Conjoint Analysis," *The Journal of Marketing* (55:4), S. 20-31.

Green, P. E., Krieger, A. M., und Wind, Y. 2001. "Thirty Years of Conjoint Analysis: Reflections and Prospects," *Interfaces* (31:3), S. 56-73.

Green, P. E., und Srinivasan, V. 1978. "Conjoint Analysis in Consumer Research: Issues and Outlook," *Journal of Consumer Research* (5:2), S. 103-123.

Greenaway, K. E., Chan, Y. E., und Crossler, R. E. 2015. "Company Information Privacy Orientation: A Conceptual Framework," *Information Systems Journal* (25:6), S. 579-606.

Gregor, S. 2006. "The Nature of Theory in Information Systems," *MIS Quarterly* (30:3), S. 611-642.

Gregory, A. 2011. "Data Governance—Protecting and Unleashing the Value of Your Customer Data Assets," *Journal of Direct, Data and Digital Marketing Practice* (12:3), S. 230-248.

Gregory, R. W., Beck, R., und Keil, M. 2013. "Control Balancing in Information Systems Development Offshoring Projects," *MIS Quarterly* (37:4), S. 1211-1232.

Gregory, R. W., Keil, M., Muntermann, J., und Mähring, M. 2015. "Paradoxes and the Nature of Ambidexterity in It Transformation Programs," *Information Systems Research* (26:1), S. 57-80.

Grossklags, J., und Acquisti, A. 2007. "When 25 Cents Is Too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information," in: *Workshop on the Economics of Information Security Series (WEIS)*. Pittsburgh, PA (USA).

Haberer, B., und Schnurr, D. 2018. "An Economic Analysis of Data Portability and Personal Data Markets," in: *Proceedings of the Thirty Ninth International Conference on Information Systems (ICIS)*. San Francisco, CA, USA.

Haenni, R. 2017. "Datum Network - the Decentralized Data Marketplace," *White Paper V15*.

Hagiu, A., und Jullien, B. 2011. "Why Do Intermediaries Divert Search?," *The RAND Journal of Economics* (42:2), S. 337-362.

Hann, I.-H., Hinz, O., und Spann, M. 2006. "Dynamic Pricing in Name-Your-Own-Price Channels: Bidding Behavior, Seller Profit and Price Acceptance," in: *Workshop on Information Systems and Economics (WISE)*.

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), S. 13-42.

Hann, I.-H., Hui, K.-L., Lee, T., und Png, I. 2002. "Online Information Privacy: Measuring the Cost-Benefit Trade-Off," in: *Proceedings of the Twenty-Third International Conference on Information Systems (ICIS)*. Barcelona, Spain: S. 1-10.

Hann, I.-H., und Terwiesch, C. 2003. "Measuring the Frictional Costs of Online Transactions: The Case of a Name-Your-Own-Price Channel," *Management Science* (49:11), S. 1563-1579.

Hanson, J. D., und Kysar, D. A. 1999. "Taking Behavioralism Seriously: The Problem of Market Manipulation," *NYU Law Review* (74), S. 630.

Hensher, D. A. 1994. "Stated Preference Analysis of Travel Choices: The State of Practice," *Transportation* (21:2), S. 107-133.

Hinz, O., Hann, I.-H., und Spann, M. 2011. "Price Discrimination in E-Commerce? An Examination of Dynamic Pricing in Name-Your-Own Price Markets," *MIS Quarterly* (35:1), S. 81-98.

Hirsch, D. D. 2014. "That's Unfair-or Is It: Big Data, Discrimination and the FTC's Unfairness Authority," *Kentucky Law Journal* (103:3), S. 345-361.

Hoofnagle, C. J., Soltani, A., Good, N., und Wambach, D. J. 2012. "Behavioral Advertising: The Offer You Can't Refuse," *Harvard Law and Policy Review* (6), S. 273-296.

Horowitz, J. K., und McConnell, K. E. 2002. "A Review of WTA/WTP Studies," *Journal of Environmental Economics and Management* (44:3), S. 426-447.

Hsee, C. K., und Zhang, J. 2010. "General Evaluability Theory," *Perspectives on Psychological Science* (5:4), S. 343-355.

Hu, H.-f., Moore, W., und Hu, P. J. 2012. "Incorporating User Perceptions and Product Attributes in Software Product Design and Evaluation," in: *Proceedings of the Thirty Third International Conference on Information Systems (ICIS)*. Orlando, Florida, USA.

Huber, G. P. 1990. "A Theory of the Effects of Advanced Information Technologies on Organizational Design, Intelligence, and Decision Making," *Academy of Management Review* (15:1), S. 47-71.

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

Hui, K.-L., und Png, I. 2006. "Economics of Privacy," in *Handbook of Information Systems and Economics*, T. Hendershott (ed.). Elsevier.

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), S. 19-33.

Imam, A., Mohammed, U., und Moses Abanyam, C. 2014. "On Consistency and Limitation of Paired T-Test, Sign and Wilcoxon Sign Rank Test," *IOSR Journal of Mathematics* (10:1), S. 1-6.

Instagram. 2018. "Terms of Use." Abgerufen am 28.08.2018, von https://help.instagram.com/581066165581870/.

Jentzsch, N. 2014. "Auctioning Privacy-Sensitive Goods," in: *Annual Privacy Forum*, B. Preneel and D. Ikonomou (eds.). Springer International Publishing Switzerland, S. 133-142.

Johnson, J. W., und Cui, A. P. 2013. "To Influence or Not to Influence: External Reference Price Strategies in Pay-What-You-Want Pricing," *Journal of Business Research* (66:2), S. 275-281.

Johnson, R. M. 1974. "Trade-Off Analysis of Consumer Values," *Journal of Marketing Research* (11:2), S. 121-127.

Kamleitner, B., Dickert, S., und Haddadi, H. 2016. "Can Users Price Real-Time Contextual Information," WU Vienna Working Paper.

Karniouchina, E. V., Moore, W. L., van der Rhee, B., und Verma, R. 2009. "Issues in the Use of Ratings-Based Versus Choice-Based Conjoint Analysis in Operations Management Research," *European Journal of Operational Research* (197:1), S. 340-348.

Kaufman, L., und Rousseeuw, P. J. 2009. *Finding Groups in Data: An Introduction to Cluster Analysis*. John Wiley & Sons, Hoboken, New Jersey.

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), S. 607-635.

Keller, K. L. 1993. "Conceptualizing, Measuring, and Managing Customer-Based Brand Equity," *Journal of Marketing* (57:1), S. 1-22.

Kettinger, W. J., und Marchand, D. A. 2011. "Information Management Practices (IMP) from the Senior Manager's Perspective: An Investigation of the IMP Construct and Its Measurement," *Information Systems Journal* (21:5), S. 385-406.

Klemperer, P. 2004. "Auctions: Theory and Practice, Economics Group, Nuffield College, University of Oxford," *Economics Papers*.

Kokolakis, S. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon," *Computers & Security* (64), S. 122-134.

Kordzadeh, N., und Warren, J. 2017. "Communicating Personal Health Information in Virtual Health Communities: An Integration of Privacy Calculus Model and Affective Commitment," *Journal of the Association for Information Systems* (18:1), S. 45.

Krasnova, H., Eling, N., Abramova, O., und Buxmann, P. 2014. "Dangers of 'Facebook Login' for Mobile Apps: Is There a Price Tag for Social Information?," in: *Proceedings of the Thirty Fifth International Conference on Information Systems (ICIS)*. Auckland.

Krasnova, H., Hildebrand, T., und Guenther, O. 2009. "Investigating the Value of Privacy on Online Social Networks: Conjoint Analysis," in: *Proceedings of the Thirtieth International Conference on Information Systems (ICIS)*. Phoenix, Arizona, USA.

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

Krasnova, H., Veltri, N. F., und Günther, O. 2012. "Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture," *Business & Information Systems Engineering* (4:3), S. 127-135.

Kreiner, G. E., Hollensbe, E. C., und Sheep, M. L. 2006. "Where Is the “Me” among the “We”? Identity Work and the Search for Optimal Balance," *Academy of Management Journal* (49:5), S. 1031-1057.

Kuneva, M. 2009. "European Consumer Commissioner Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling Brussels, 31 March 2009." Abgerufen am 20.10.2017, von http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm.

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

Larson, G. S., und Pepper, G. L. 2003. "Strategies for Managing Multiple Organizational Identifications: A Case of Competing Identities," *Management Communication Quarterly* (16:4), S. 528-557.

Laudon, K. 1997. "Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information," *Working Paper Series, Stem #IS-97-4*

Laudon, K. C. 1996. "Markets and Privacy," *Communications of the ACM* (39:9), S. 92-104.

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), S. 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), S. 423-444.

Lehmann, S., und Buxmann, P. 2009. "Pricing Strategies of Software Vendors," *Business & Information Systems Engineering* (1:6), S. 452-462.

Li, C., Li, D. Y., Miklau, G., und Suciu, D. 2014. "A Theory of Pricing Private Data," *ACM Transactions on Database Systems (TODS)* (39:4), S. 34.

Li, H., Sarathy, R., und Xu, H. 2011. "The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors," *Decision Support Systems* (51:3), S. 434-445.

Liu, J., Dai, R., Wei, X. D., und Li, Y. 2016. "Information Revelation and Customer Decision-Making Process of Repeat-Bidding Name-Your-Own-Price Auction," *Decision Support Systems* (90), S. 46-55.

Louviere, J. J. 1988. "Conjoint Analysis Modelling of Stated Preferences: A Review of Theory, Methods, Recent Developments and External Validity," *Journal of Transport Economics and Policy* (22:1), S. 93-119.

Lowry, P. B., Dinev, T., und Willison, R. 2017. "Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda," *European Journal of Information Systems* (26:6), S. 546-563.

Lv, Y., Duan, Y., Kang, W., Li, Z., und Wang, F.-Y. 2015. "Traffic Flow Prediction with Big Data: A Deep Learning Approach," *IEEE Trans. Intelligent Transportation Systems* (16:2), S. 865-873.

MacRumors. 2017. "Apple's Concern with User Privacy Reportedly Stifling Siri Development." Abgerufen am 09.02.2019, von https://www.macrumors.com/2017/06/08/apple-struggling-to-develop-siri-privacy/.

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), S. 336-355.

March, J. G. 1991. "Exploration and Exploitation in Organizational Learning," *Organization Science* (2:1), S. 71-87.

McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D., und Barton, D. 2012. "Big Data: The Management Revolution," *Harvard Business Review* (90:10), S. 60-68.

Medium. 2018. "Data Is the New Gold." Abgerufen am 11.08.2018, von https://medium.com/datareum/data-is-the-new-gold-e6eb1aeeb640.

meeco.me. 2018. "Access, Control and Share Personal Data on Your Terms." Abgerufen am 06.12.2018, von https://meeco.me/people.html.

Mikians, J., Gyarmati, L., Erramilli, V., und Laoutaris, N. 2013. "Crowd-Assisted Search for Price Discrimination in E-Commerce: First Results," in: *Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies*. ACM, S. 1-6.

Milberg, S. J., Burke, S. J., Smith, H. J., und Kallman, E. A. 1995. "Values, Personal Information Privacy, and Regulatory Approaches," *Communications of the ACM* (38:12), S. 65-74.

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

Miles, M. B., Huberman, A. M., Huberman, M. A., und Huberman, M. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*. Sage.

Miller, A. R., und Tucker, C. 2018. "Privacy Protection, Personalized Medicine, and Genetic Testing," *Management Science* (64:10), S. 4648-4668.

Milne, G. R., Pettinico, G., Hajjat, F. M., und Markos, E. 2017. "Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing," *Journal of Consumer Affairs* (51:1), S. 133-161.

Moorman, C. 1995. "Organizational Market Information Processes: Cultural Antecedents and New Product Outcomes," *Journal of Marketing Research* (32:3), S. 318-335.

Mowday, R. T., und Sutton, R. I. 1993. "Organizational Behavior: Linking Individuals and Groups to Organizational Contexts," *Annual Review of Psychology* (44:1), S. 195-229.

Nambiar, R., Bhardwaj, R., Sethi, A., und Vargheese, R. 2013. "A Look at Challenges and Opportunities of Big Data Analytics in Healthcare," in: *Proceedings of the IEEE International Conference on Big Data*. IEEE, S. 17-22.

NewYorkTimes. 2018. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." *The New York Times* Abgerufen am 06.01.2019, von https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Nguyen, K. D., Rosoff, H., und John, R. S. 2016. "The Effects of Attacker Identity and Individual User Characteristics on the Value of Information Privacy," *Computers in Human Behavior* (55:A), S. 372-383.

Nissenbaum, H. 2004. "Privacy as Contextual Integrity," *Washington Law Review* (79), S. 119.

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), S. 100-126.

Nutt, P. C. 1998. "How Decision Makers Evaluate Alternatives and the Influence of Complexity," *Management Science* (44:8), S. 1148-1166.

OceanProtocol. 2018. "Frequently Asked Questions About Ocean Protocol." Abgerufen am 06.12.2018, von https://oceanprotocol.com/faq/.

Oracle. 2018. "Products Menu - There's an Audience for Everything." Abgerufen am 06.01.2018, von https://www.oracle.com/applications/customer-experience/data-cloud/third-party-data.html.

Orange. 2014. "The Future of Digital Trust - a European Study on the Nature of Consumer Trust and Personal Data." Abgerufen am 23.11.2017, von https://www.orange.com/content/download/25973/582245/version/2/file/Report+-+My+Data+Value+-+Orange+Future+of+Digital+Trust+-+FINAL.pdf.

Orlikowski, W. J. 1993. "Case Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development," *MIS Quarterly* (17:3), S. 309-340.

Orme, B. 2002. "Formulating Attributes and Levels in Conjoint Analysis," *Sawtooth Software Research Paper*, S. 1-4.

Orme, B. 2009. "Which Conjoint Method Should I Use," *Sawtooth Software Research Paper Series*, S. 1-6.

Orme, B. 2012. "Latent Class V4.5 Software for Latent Class Estimation for CBC Data."

Ozdemir, Z. D., Jeff Smith, H., und Benamati, J. H. 2017. "Antecedents and Outcomes of Information Privacy Concerns in a Peer Context: An Exploratory Study," *European Journal of Information Systems* (26:6), S. 642-660.

Parks, R., Xu, H., Chu, C.-H., und Lowry, P. B. 2017. "Examining the Intended and Unintended Consequences of Organisational Privacy Safeguards," *European Journal of Information Systems* (26:1), S. 37-65.

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

Pavlou, P. A., Liang, H., und Xue, Y. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* (31:1), S. 105-136.

Perusco, L., und Michael, K. 2007. "Control, Trust, Privacy, and Security: Evaluating Location-Based Services," *IEEE Technology and Society Magazine* (26:1), S. 4-16.

Porter, M. E. 1996. "What Is Strategy," *Havard Business Review* (74:6), S. 61-78.

Porter, M. E., und Millar, V. E. 1985. "How Information Gives You Competitive Advantage," *Harvard Business Review Cambridge, MA* (63:4), S. 149-174.

Posner, R. A. 1977. "The Right of Privacy," *Georgia Law Review* (12:3), S. 393.

Potoglou, D., Patil, S., Gijón, C., Palacios, J., und Feijóo, C. 2013. "The Value of Personal Information Online: Results from Three Stated Preference Discrete Choice Experiments in the Uk," in: *Proceedings of the Twenty-First European Conference for Information Systems (ECIS)*. Utrecht.

Preibusch, S. 2013. "The Value of Privacy in Web Search," in: *The Twelfth Workshop on the Economics of Information Security (WEIS)*.

Preibusch, S. 2015. "The Value of Web Search Privacy," *IEEE Security & Privacy* (13:5), S. 24-32.

Preibusch, S., Kübler, D., und Beresford, A. R. 2013. "Price Versus Privacy: An Experiment into the Competitive Advantage of Collecting Less Personal Information," *Electronic Commerce Research* (13:4), S. 423-455.

Pu, Y., und Grossklags, J. 2015. "Using Conjoint Analysis to Investigate the Value of Interdependent Privacy in Social App Adoption Scenarios," in: *Proceedings of the Thirty Sixth International Conference on Informations 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," in: *Proceedings on Privacy Enhancing Technologies*. S. 61-81.

Racherla, P., Babb, J. S., und Keith, M. J. 2011. "Pay-What-You-Want Pricing for Mobile Applications: The Effect of Privacy Assurances and Social Information," in: *Conference for Information Systems Applied Research Proceedings*. S. 1-13.

Raisch, S., und Birkinshaw, J. 2008. "Organizational Ambidexterity: Antecedents, Outcomes, and Moderators," *Journal of Management* (34:3), S. 375-409.

Raisch, S., Birkinshaw, J., Probst, G., und Tushman, M. L. 2009. "Organizational Ambidexterity: Balancing Exploitation and Exploration for Sustained Performance," *Organization Science* (20:4), S. 685-695.

Ramesh, B., Mohan, K., und Cao, L. 2012. "Ambidexterity in Agile Distributed Development: An Empirical Investigation," *Information Systems Research* (23:2), S. 323-339.

ReceiptHog. 2018. "What Is Receipt Hog?" Abgerufen am 06.12.2018, von https://receipthog.zendesk.com/hc/en-us/articles/227155648-What-is-Receipt-Hog-.

Regner, T., und Riener, G. 2017. "Privacy Is Precious: On the Attempt to Lift Anonymity on the Internet to Increase Revenue," *Journal of Economics & Management Strategy* (26:2), S. 318-336.

Roeber, B., Rehse, O., Knorrek, R., und Thomsen, B. 2015. "Personal Data: How Context Shapes Consumers' Data Sharing with Organizations from Various Sectors," *Electronic Markets* (25:2), S. 95-108.

Rollin, R., Steinmann, S., Schramm-Klein, H., Neus, F., und Nimmermann, F. 2017. "Drivers of Market Success for Mobile Gaming Apps-Results of a Choice-Based Conjoint Experiment," in: *Proceedings of the Thirty Eighth International Conference on Information Systems (ICIS)*. Seoul, South Korea S. 1-20.

Rose, E. 2005. "Data Users Versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information?," in: *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*. IEEE, S. 180c.

Rosenthal, R. 1994. "Parametric Measures of Effect Size," in *The Handbook of Research Synthesis,* H. Cooper and L.V. Hedges (eds.). New York: Russell Sage Foundation., S. 231-244.

Roßnagel, H., Zibuschka, J., Hinz, O., und Muntermann, J. 2014. "Users' Willingness to Pay for Web Identity Management Systems," *European Journal of Information Systems* (23:1), S. 36-50.

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

SawtoothSoftware. 2004. "The CBC Latent Class Technical Paper (Version 3)," *Sawtooth Software Technical Paper Series*.

Schoeman, F. D. 1984. *Philosophical Dimensions of Privacy: An Anthology*. Cambridge University Press.

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

Schwartz, P. M. 2004. "Property, Privacy, and Personal Data," *Harvard Law Review*, S. 2056-2128.

Schweitzer, M. E., und Hsee, C. K. 2002. "Stretching the Truth: Elastic Justification and Motivated Communication of Uncertain Information," *Journal of Risk and Uncertainty* (25:2), S. 185-201.

Seidel, S., und Urquhart, C. 2013. "On Emergence and Forcing in Information Systems Grounded Theory Studies: The Case of Strauss and Corbin," *Journal of Information Technology* (28:3), S. 237-260.

Shapiro, C., Carl, S., und Varian, H. R. 1998. *Information Rules: A Strategic Guide to the Network Economy*. Harvard Business Press.

Shoparoo. 2018. "Shoparoo Hassle-Free Fundraising." Abgerufen am 06.12.2018, von https://www.shoparoo.com/.

Singleton, S. M., und Harper, J. 2002. "With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us," *SSRN*.

Skinner, G., Han, S., und Chang, E. 2006. "An Information Privacy Taxonomy for Collaborative Environments," *Information Management & Computer Security* (14:4), S. 382-394.

Slotin, J. 2018. "What Do We Know About the Value of Data?" Abgerufen am 25.07.2018, von http://www.data4sdgs.org/news/what-do-we-know-about-value-data.

Smith, H. J. 1993. "Privacy Policies and Practices: Inside the Organizational Maze," *Communications of the ACM* (36:12), S. 104-122.

Smith, H. J., Dinev, T., und Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), S. 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), S. 167-196.

Smith, W. K., und Tushman, M. L. 2005. "Managing Strategic Contradictions: A Top Management Model for Managing Innovation Streams," *Organization Science* (16:5), S. 522-536.

Spann, M., Bernhardt, M., Häubl, G., und Skiera, B. 2005. "It’s All in How You Ask: Effects of Price Elicitation Format on Bidding Behavior in Reverse-Pricing Markets," in: *Proceedings of the 26th Annual Conference of the Society for Judgment and Decision Making (SJDM)* Toronto, Canada.

Spann, M., Skiera, B., und Schäfers, B. 2004. "Measuring Individual Frictional Costs and Willingness-to-Pay Via Name-Your-Own-Price Mechanisms," *Journal of Interactive Marketing* (18:4), S. 22-36.

Spann, M., und Tellis, G. J. 2006. "Does the Internet Promote Better Consumer Decisions? The Case of Name-Your-Own-Price Auctions," *Journal of Marketing* (70:1), S. 65-78.

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

Spiekermann, S., Böhme, R., Acquisti, A., und Hui, K.-L. 2015b. "Personal Data Markets," *Electronic Markets* (25:2), S. 91-93.

Spiekermann, S., und Korunovska, J. 2017. "Towards a Value Theory for Personal Data," *Journal of Information Technology* (32:1), S. 62-84.

Spiekermann, S., Korunovska, J., und Bauer, C. 2012. "Psychology of Ownership and Asset Defense: Why People Value Their Personal Information Beyond Privacy," in: *Proceedings of the Thirty Third International Conference on Information Systems (ICIS)*. Orlando, Florida, USA: S. 1-20.

Staiano, J., Oliver, N., Lepri, B., de Oliveira, R., Caraviello, M., und Sebe, N. 2014. "Money Walks: A Human-Centric Study on the Economics of Personal Mobile Data," in: *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, S. 583-594.

Statista. 2014a. "Distribution of Global Internet Users Who Say They Are Online at Least 10 Times a Day as of July 2014, by Gender." Abgerufen am 17.10.2017, von https://www.statista.com/statistics/408674/global-continuously-connected-internet-users-gender/.

Statista. 2014b. "Internet Users by Age Worldwide." Abgerufen am 17.10.2017, von https://www.statista.com/statistics/272365/age-distribution-of-internet-users-worldwide/.

Statista. 2018a. "The 100 Largest Companies in the World by Market Value in 2018 (in Billion U.S. Dollars)." Abgerufen am 25.07.2018, von https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/.

Statista. 2018b. "Share of Adults in the United States Who Are Familiar with the Word Selfie as of August 2018, by Age Group." Abgerufen am 27.08.2018, von https://www.statista.com/statistics/683924/us-adults-familiar-selfie-age/.

Steinfeld, N. 2015. "Trading with Privacy: The Price of Personal Information," *Online Information Review* (39:7), S. 923-938.

Strahilevitz, L. J. 2008. "Privacy Versus Antidiscrimination," *The University of Chicago Law Review* (75:1), S. 363-381.

Strauss, A., und Corbin, J. 1990. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques* London: Sage publications.

Strong, D. M., und Volkoff, O. 2010. "Understanding Organization—Enterprise System Fit: A Path to Theorizing the Information Technology Artifact," *MIS Quarterly* (34:4), S. 731-756.

Tang, Z., Hu, Y., und Smith, M. D. 2008. "Gaining Trust through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor," *Journal of Management Information Systems* (24:4), S. 153-173.

Taylor, C. R. 2004. "Consumer Privacy and the Market for Customer Information," *RAND Journal of Economics*, S. 631-650.

Techcrunch. 2018. "Instagram Hits 1 Billion Monthly Users, up from 800m in September." Abgerufen am 20.02.2019, von https://techcrunch.com/2018/06/20/instagram-1-billion-users/.

Tene, O., und Polonetsky, J. 2012. "Big Data for All: Privacy and User Control in the Age of Analytics," *Northwestern Journal of Technology and Intellectual Property* (11:5), S. xxvii.

Terwiesch, C., Savin, S., und Hann, I.-H. 2005. "Online Haggling at a Name-Your-Own-Price Retailer: Theory and Application," *Management Science* (51:3), S. 339-351.

Thaler, R. 1980. "Toward a Positive Theory of Consumer Choice," *Journal of Economic Behavior & Organization* (1:1), S. 39-60.

TheGuardian. 2018. "Facebook Fined for Data Breaches in Cambridge Analytica Scandal." Abgerufen am 09.02.2019, von https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal.

Thomson, J. J. 1975. "The Right to Privacy," *Philosophy & Public Affairs*, S. 295-314.

Time. 2017. "How Humankind Could Become Totally Useless." Abgerufen am 07.12.2018, von http://time.com/4672373/yuval-noah-harari-homo-deus-interview/.

TowerData. 2019. "Clean, Enhance & Personalize Get the Data You Need to Increase Engagement and Conversions." Abgerufen am 09.01.2019, von https://www.towerdata.com/.

Troncoso, C., Danezis, G., Kosta, E., Balasch, J., und Preneel, B. 2011. "Pripayd: Privacy-Friendly Pay-as-You-Drive Insurance," *IEEE Transactions on Dependable and Secure Computing* (8:5), S. 742-755.

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), S. 254-268.

Tucker, C. E. 2012. "The Economics of Advertising and Privacy," *International Journal of Industrial Organization* (30:3), S. 326-329.

Tversky, A., und Kahneman, D. 1974. "Judgment under Uncertainty: Heuristics and Biases," *Science* (185:4157), S. 1124-1131.

Twitter. 2019. "Selected Company Metrics and Financials." Abgerufen am 20.02.2019, von https://s22.q4cdn.com/826641620/files/doc_financials/2018/q4/Q4-2018-Selected-Company-Financials-and-Metrics.pdf.

Urquhart, C., und Fernandez, W. 2013. "Using Grounded Theory Method in Information Systems: The Researcher as Blank Slate and Other Myths," *Journal of Information Technology* (28:3), S. 224-236.

Urquhart, C., Lehmann, H., und Myers, M. D. 2010. "Putting the 'Theory'back into Grounded Theory: Guidelines for Grounded Theory Studies in Information Systems," *Information Systems Journal* (20:4), S. 357-381.

Varian, H. R. 2002. "Economic Aspects of Personal Privacy," in *Cyber Policy and Economics in an Internet Age*. Springer, S. 127-137.

Venkatesh, V., Thong, J. Y., Chan, F. K., und Hu, P. J. 2016. "Managing Citizens' Uncertainty in E-Government Services: The Mediating and Moderating Roles of Transparency and Trust," *Information Systems Research* (27:1), S. 87-111.

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

Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., und Cleven, A. 2009. "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process," in: *Proceedings of the Seventeenth European Conference on Information Systems*. Verona, Italy: S. 2206-2217.

Wagner, A., Wessels, N., Buxmann, P., und Krasnova, H. 2018. "Putting a Price Tag on Personal Information - a Literature Review.," in: *Proceedings of the Hawaii International Conference on System Sciences (HICSS)*. Waikoloa Village, Hawaii S. 3760-3769.

Wall, J., Lowry, P. B., und Barlow, J. B. 2015. "Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess," *Journal of the Association for Information Systems* (17:1), S. 39–76.

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

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

Weick, K. E. 1995. *Sensemaking in Organizations*. Thousand Oaks, CA: Sage.

Wessels, N., Gerlach, J., und Wagner, A. 2019a. "To Sell or Not to Sell – Antecedents of Individuals' Willingness-to-Sell Personal Information on Data-Selling Platforms," in: *Fortieth International Conference on Information Systems (ICIS)* Munich, Germany.

Wessels, N., Wagner, A., Prakash Sarswat, J., und Buxmann, P. 2019b. "What Is Your Selfie Worth? A Field Study on Individuals' Valuation of Personal Data," in: *Proceedings of the 14th International Conference on Wirtschaftsinformatik*. Siegen, Germany.

Westin, A., und Louis, H. 1991. "Equifax-Harris Consumer Privacy Survey," *Conducted for Equifax Inc*.

Westin, A. F. 1967. *Privacy and Freedom*. New York: ig Publishing.

Westin, A. F., und Maurici, D. 1998. *E-Commerce & Privacy: What Net Users Want*. Privacy & American Business Hackensack, NJ.

Wibson. 2018. "Don't Give Away Your Data for Free. Make a Profit." Abgerufen am 06.12.2018, von https://wibson.org/#app.

Wilson, F. 2018. "Tweet Fred Wilson." Abgerufen am 29.12.2018, von https://twitter.com/getdock/status/996413365567172608.

Wu, M., Miller, R. C., und Garfinkel, S. L. 2006. "Do Security Toolbars Actually Prevent Phishing Attacks?," in: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, S. 601-610.

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

Yim, O., und Ramdeen, K. T. 2015. "Hierarchical Cluster Analysis: Comparison of Three Linkage Measures and Application to Psychological Data," *The Quantitative Methods for Psychology* (11:1), S. 8-21.

Zannier, F. 2013. "A Bite of Me." Abgerufen am 26.03.2018, von https://www.kickstarter.com/projects/1461902402/a-bit-e-of-me?lang=de.

Zheng, Z., und Pavlou, P. A. 2010. "Research Note—toward a Causal Interpretation from Observational Data: A New Bayesian Networks Method for Structural Models with Latent Variables," *Information Systems Research* (21:2), S. 365-391.

Zimmerman, D. W., und Zumbo, B. D. 1993. "Relative Power of the Wilcoxon Test, the Friedman Test, and Repeated-Measures Anova on Ranks," *The Journal of Experimental Education* (62:1), S. 75-86.

Anhang

Anhang 1: Überblick über die Charakteristiken des finalen Samples

Unternehmensgröße	**Service-ID**	**Branche**
Kleine Unternehmen (< 10 Mitarbeiter)	S#01	Nachrichten
	S#02	Share Economy
	S#03	Nachrichten
	S#04	Rettungsservice
	S#05	Gesundheit & Fitness
	S#06	E-Commerce
	S#07	Gesundheit & Fitness
	S#08	Lifestyle
	S#09	Gesundheit & Fitness
Mittlere Unternehmen (10-250 Mitarbeiter)	S#10	E-Commerce
	S#11	Vermittlungsservice
	S#12	E-Commerce
	S#13	E-Commerce
	S#14	Bewertungsservice
	S#15	Vermittlungsservice
	S#16	Spiele
	S#17	Finanzen
	S#18	E-Commerce
Großunternehmen (> 250 Mitarbeiter)	S#19	Spiele
	S#20	Unterhaltung
	S#21	E-Commerce
	S#22	Nachrichten
	S#23	E-Commerce

Anhang 2: Leitfaden für die Interviews

Die folgenden Fragen dienten als grobe Orientierungshilfe für die durchgeführten Interviews, wobei jedes Interview auch in eine etwas andere Richtung einschlagen konnte, da interessante Ideen spontan verfolgt wurden. Darüber hinaus entwickelte sich der Interviewleitfaden im Laufe der Studie weiter, da einige neue Fragen erst zu einem bestimmten Zeitpunkt während des Forschungsprozesses aufgekommen waren (vgl. Glaser 1978).

- Bitte beschreiben Sie kurz die von Ihrem Unternehmen erbrachten Leistungen/Produkte.
- Wie wichtig sind Nutzerdaten für Ihr Unternehmen? Worauf basiert ihr Wert?
- Welche Rolle spielen Nutzerdaten für Ihr Geschäftsmodell/Ihre Geschäftsprozesse?
- Wie entscheiden Sie darüber, welche Nutzerdaten erhoben werden und welche Berechtigungen erteilt werden?
- Welche Nutzerdaten erfassen Sie und welche Rechte erhalten Sie? Warum?
- In welchen Prozessen werden die Nutzerdaten genau benötigt?
- Wie weit und wie informieren Sie die Nutzer über Ihre Datenerhebung und -nutzung?
- Signalisieren Sie in diesem Zusammenhang den Nutzern etwas, was Sie tatsächlich nicht tun?
- Machen Sie sich Sorgen darüber, wie Nutzer Ihre Datenerhebung und -nutzung wahrnehmen könnten?
- Erleben Sie Spannungen in Bezug auf Ihre Datenerhebung und -nutzung? Wenn ja, wie gehen Sie mit diesen Spannungen um?

Anhang 3: Überblick über die identifizierten Spannungen und zusätzliche Zitate

Spannung 1: **Datensammlung gegen Nutzergewinnung**	**Beschreibung**: Ein Unternehmen muss den potenziellen Nutzen der Datensammlung mit dem potenziellen Verlust von Kunden bedingt durch deren verstärkte Privatsphäre-Bedenken abwägen.	Beispiel-Zitat Nr. 1 (S#19, großes Unternehmen, Spieleservice): *"Und da war unser Ergebnis, dass der, quasi der Erkenntnisgewinn, den wir dadurch [durch die Praktik] haben, der war nicht so hoch wie das, was man da verliert."* Beispiel-Zitat Nr. 2 (S#03, kleines Unternehmen, Nachrichten): *"Ja, es wäre zum Beispiel interessant Locations vom Nutzer zu tracken. Das kann man wahrscheinlich… damit kann man extrem interessante Sachen machen. Also zum Beispiel für Marketing, für lokale Werbung. Also auch für Verlage wäre das extrem interessant wo der Nutzer sich aufhält. Und zum Beispiel wo der seine „Homebase" [hat], wo der Nutzer zu Hause ist. Damit sie Homebase News austragen können. Die Nachrichten, die in deren Umgebung passieren, da wo sie wohnen. Da könnte man bestimmt viele Sachen machen. Aber ich meine, das Tracken der Nutzerlocation, das ist wahrscheinlich das Schlimmste, das du machen kannst [in Bezug auf die Privatsphäre der Nutzer]."*
Spannung 2: **Zeitrahmen der Sammlung**	**Beschreibung**: Ein Unternehmen kann entweder heute mehr Nutzerdaten sammeln und eine geringere Akzeptanzrate riskieren oder zu einem späteren Zeitpunkt, wenn die Daten tatsächlich benötigt werden, was dann aber zu dem Zeitpunkt zum Verlust bestehender Nutzer führen kann.	Beispiel-Zitat Nr. 1 (S#10, mittleres Unternehmen, E-Commerce): *"Also sich nachträglich ein Einverständnis zu holen ist immer sehr schwierig. Weil man dann… dann stößt man die Leute auf einen bestimmten Aspekt, den man vielleicht mit den Daten machen möchte oder irgendwas Anderes und dann fragen sich die Nutzer natürlich schon: "Was geschieht jetzt damit?" und setzen sich damit stärker auseinander."* Beispiel-Zitat Nr. 2 (S#01, kleines Unternehmen, Nachrichten): "*Aber das Problem ist halt immer, was wir festgestellt haben ist immer, wenn man die App-Berechtigungen erhöht, mit einem neuen Release, dass die Nutzer dann wirklich zurückhaltend sind mit dem Upgrade [des Services]*."
Spannung 3: **Image-bezogene**	**Beschreibung**: Die Erhebung und Nutzung von Daten kann im Widerspruch zu	Beispiel-Zitat Nr. 1 (S#20, großes Unternehmen, Unterhaltungsservice):

Kosten der Nutzerdaten	dem Ziel eines Unternehmens stehen, ein positives Image zu erhalten.	*"Das ist auch so ein bisschen der ethische Gedanke, der in diesem Markennamen mit drinstecken muss. Wir können das nicht einfach tun [die Lokation der Kunden tracken ohne ihnen eine Wahl zu geben] und hinterher irgendwelche Shitstorms riskieren. Das geht nicht."* Beispiel-Zitat Nr. 2 (S#09, kleines Unternehmen, Gesundheit & Fitness): *"Das [Image] ist ein Thema. Da haben wir auch schon oft drüber diskutiert, was von den Nutzern aufgenommen wird und da haben wir auch schon auf Rückmeldungen der Kunden reagiert und quasi die erforderlichen Daten angepasst."*
Spannung 4: **Verlieren von Nutzern durch Datennutzung**	**Beschreibung**: Die Nutzung der verfügbaren Daten für zusätzliche Zwecke trägt zum Erfolg des Unternehmens bei, könnte aber gleichzeitig die Zahl der Kunden reduzieren, die den Service nutzen.	Beispiel-Zitat Nr. 1 (S#10, mittleres Unternehmen, E-Commerce): *"Also das bestimmte kritische Bereiche, die wir ja auch auf der Webseite haben, wenn die irgendwo als Banner im Retargeting wiederkommen, also, da muss man dort sehr vorsichtig sein, welche Daten man verwendet. Wie man damit umgeht. Aber also, wir haben uns im Vorfeld nicht darüber Gedanken gemacht. Wir machen uns dann im Nachhinein, wenn wir Daten anwenden wollen oder, wenn wir daraus bestimmte Schlüsse ziehen, dann machen wir uns Gedanken, welche Bereiche wir verwenden dürfen, welche nicht."* Beispiel-Zitat Nr. 2 (S#05, kleines Unternehmen, Gesundheit & Fitness): *"Es wäre relativ leicht da irgendwie oben oder unten oder irgendwo irgendwelche Werbung reinzupacken. (...) Das wäre durchaus denkbar. Das wäre aber von dem, was man damit verdienen würde, würde das nicht reichen um das Produkt zu finanzieren und das würde, glaube ich, zu viele Nutzer dann noch verprellen."*

Anhang 4: Überblick über die identifizierten Taktiken und zusätzliche Zitate

Ersatztaktik 1: **Verwendung verfügbarer Daten**	**Beschreibung**: Ein Unternehmen versucht ein Ziel zu erreichen, indem es bereits vorhandene Daten verwendet.	Beispiel-Zitat Nr. 1 (S#10, mittleres Unternehmen, E-Commerce): *"Darüber hinaus gibt es natürlich noch andere Daten, die man erhebt, die Verhaltensdaten auf der Webseite. Das machen wir insofern eigentlich auch nicht. Also wir setzen jetzt zum Beispiel Analytics ein, aber die Daten sind anonymisiert, sprich keiner Person zuordnungsbar."* Beispiel-Zitat Nr. 2 (S#18, mittleres Unternehmen, E-Commerce): *"Ja, klar, also am Ende liegt hinter so einer Entscheidung ja immer irgendein Ziel, das man verfolgt oder irgendein Bedürfnis, was man erfüllen möchte oder ein Wert, den man schaffen will. Und ich sag mal so, wenn das auf einem Weg nicht möglich ist, dann ist natürlich das Naheliegende, was dann auch immer passiert, dass man immer Alternativen sucht, ob man das halt irgendwie über andere Umwege quasi lösen kann, die dann gängig sind. (…) ob man eben andere Informationen nutzt, die irgendwie, sag ich mal vom Datenschutz her und von der Privatsphäre des Nutzers her in Ordnung sind zu benutzen, aber irgendwie ein annähernd gutes Ergebnis zulassen."*
Ersatztaktik 2: **Suche nach einer weniger aufdringlichen Alternative**	**Beschreibung**: Um seinen Nutzern ähnliche Funktionen oder Dienstleistungen anbieten zu können, implementiert ein Unternehmen eine weniger Privatsphäre-einschneidende Alternative.	Beispiel-Zitat Nr. 1 (S#09, kleines Unternehmen, Gesundheit & Fitness): *"Also wir haben ursprünglich mal die Adresse abgefragt, aber das haben wir jetzt beschränkt auf das Land. Und ja, eigentlich das und der Rest ist freiwillig. Also der [Rest] muss nicht angegeben werden."* *Interviewer: „Okay, und warum habt ihr das jetzt aufs Land beschränkt? Also nützt euch das dann auch was? Also was wolltet ihr ursprünglich?"* *„Ja, zusätzliche Services. Um einfach nachher, wenn wir so Trainingsauswertungen machen, dass man sich mit Leuten vergleichen kann (…)."* Beispiel-Zitat Nr. 2 (S#08, kleines Unternehmen, Lifestyle): *"(…) Bad Publicity und Abmahnungen von irgendwelchen Datenschutzmenschen und sowas das kommt halt dann alles damit dazu. Ich meine, oft ist es ja schon so, dass viele Leute oder manche Leute, die warten halt immer nur gerade auf so Gelegenheiten dann irgendwie da so irgendwie in die Kerbe zu schlagen und dann einfach zu sagen.*

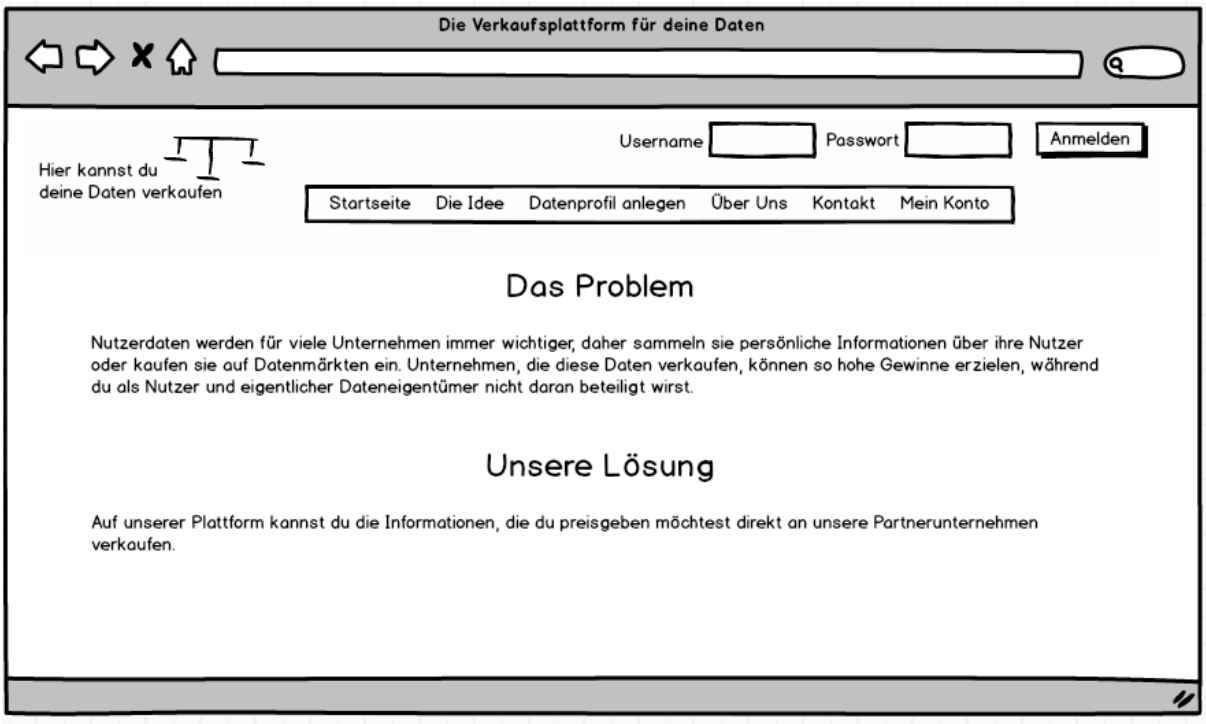
		"So, das ist jetzt der neue bad guy." (...) Das ist ja auch einfach ein Aufwand, den man auch irgendwie dadurch vermeiden kann, dass man sagt, wir verzichten einfach auf Klarnamen oder so."
Transparenz-taktik 1: **Vermeidung von Überbetonung**	**Beschreibung**: Informationen über die Datenerhebung und -nutzung stehen den Nutzern zur Verfügung, das Unternehmen betont diese Informationen jedoch nicht ausdrücklich.	Beispiel-Zitat Nr. 1 (S#01, kleines Unternehmen, Nachrichten): *"Mehr ins Detail gehen und sagen "Wir sammeln eure Daten und wissen was ihr lest", das kommt nicht so gut an. (...) Wir sagen zum Beispiel am Anfang jetzt sind wir jetzt am Überarbeiten. Wir sagen jetzt nicht mehr "Gib uns deine Daten. Sag was du gerne liest", sondern wir formulieren das um und sagen "Erstelle dein Magazin"."* Beispiel-Zitat Nr. 2 (S#19, großes Unternehmen, Spieleservice): *"Die Frage ist halt auch, stößt man die Leute dann da in die Richtung [indem man sie auf Datenschutz aufmerksam mach]. Ich glaube, dass Datenschutz für Spiele halt kein Verkaufsargument ist."*
Transparenz-taktik 2: **Anbieten von Erklärung**	**Beschreibung**: Ein Unternehmen bietet Hintergrundinformationen zu einer bestimmten Datenpraktik, um mögliche negative Folgen von Fehlinterpretationen oder Unverständnis der Nutzer zu vermeiden.	Beispiel-Zitat Nr. 1 (S#15, mittleres Unternehmen, Vermittlungsservice): *"Sehr wichtig war uns aber dieser Nutzerhinweis in den FAQs und in der Hilfe, dass es [die Lokationsdaten] eben tatsächlich nur während der Joberledigung aufgezeichnet wird und zum Beispiel nicht, wenn das Handy deaktiviert in der Tasche liegt oder den ganzen Tag über."* Beispiel-Zitat Nr. 2 (S#14, mittleres Unternehmen, Bewertungsservice): *"Wir erklären quasi dem User, wofür wir seine Daten brauchen. Nämlich genau eben um zu verifizieren, dass es sich um eine echte Bewertung handelt. Um ihm auch die Möglichkeit natürlich zu geben, wenn er mal Content auf der Plattform abgegeben hat, den auch wieder zu korrigieren, zu ändern, selbst zu verwalten. Also wir kommunizieren quasi den Vorteil dieser Datenabgabe und auch warum wir das brauchen."*
Segmentierungs-taktik 1: **Freiwillige Beiträge**	**Beschreibung**: Ein Unternehmen lässt die Nutzer entscheiden, ob sie Informationen zur Verfügung stellen oder sich auf bestimmte Praktiken einigen wollen.	Beispiel-Zitat Nr. 1 (S#03, kleines Unternehmen, Nachrichten): *"(...) dann haben wir den Login optional gemacht und dann ist die Conversion Rate viel höher geworden, also die hat sich verdoppelt."* Beispiel-Zitat Nr. 2 (S#02, kleines Unternehmen, Share Economy):

		"Optional, das ist aber keine Pflicht, kann noch [die Information] angegeben werden. Das ist halt so ein... das ist ein Datensatz, den wir für das spätere Bezahlsystem brauchen könnten (...)."
Segmentierungs-taktik 2: **Funktionale Versionierung**	**Beschreibung**: Als Gegenleistung für zusätzliche Informationen oder Nutzungszwecke bietet das Unternehmen zusätzliche Funktionen an.	Beispiel-Zitat Nr.1 (S#20, großes Unternehmen, Unterhaltung): *"Wir wollen, dass wir dem [Nutzer] sinnvolle Services zur Verfügung stellen. Und deshalb fragen wir ihn, ob er diesen Service nutzen möchte und dann kann er ihn ein- oder ausschalten. Sozusagen, man kann sagen, für den Service brauchen wir bestimmte Daten. Wenn er ihn nutzen will, muss er sie uns zur Verfügung stellen."* Beispiel-Zitat Nr. 2 (S#05, kleines Unternehmen, Gesundheit & Fitness): *"Ich glaube, man muss das [zusätzliche Sammeln von Daten] mit einem klaren Mehrwert für den Nutzer verbinden. (...) Also wenn man das so verkaufen kann: "Wir haben noch gezieltere Einsteigerprogramme, bei denen insbesondere auch euer Startgesundheitszustand noch besser berücksichtigt wird und dafür brauchen wir jetzt bitte Alter, Geschlecht, Gewicht, Vorerkrankungen usw.""*
Segmentierungs-taktik 3: **Diskriminierung ohne Selbstauswahl**	**Beschreibung**: Basierend auf der Analyse der Unternehmen wählt das Unternehmen diejenigen Nutzer aus, die eine bestimmte Praktik eher akzeptieren.	Beispiel-Zitat Nr. 1 (S#19, großes Unternehmen, Spieleservice): *"Diese automatisierte Werbung kann man ein bisschen, kann man testen. Machen wir dann auch um zu schauen, wann blenden wir das ein? Für welche User? Wie schnell gerade? usw."* Beispiel-Zitat Nr. 2 (S#22, großes Unternehmen, Nachrichten): *"[Angenommen] Sie surfen auf einer Sportseite, haben einen Sportinhalt gelesen. Wenn Sie dann unsere Seite liken, liken Sie den Sport-Channel von uns. Wir wissen über Sie, dass Sie Sportnutzer sind und die Information interessiert und dann bekommen Sie auch nur Sportmeldungen über Facebook. Und dann ist die Wahrscheinlichkeit geringer, dass Sie die Sportmeldungen irgendwann abbestellen."*

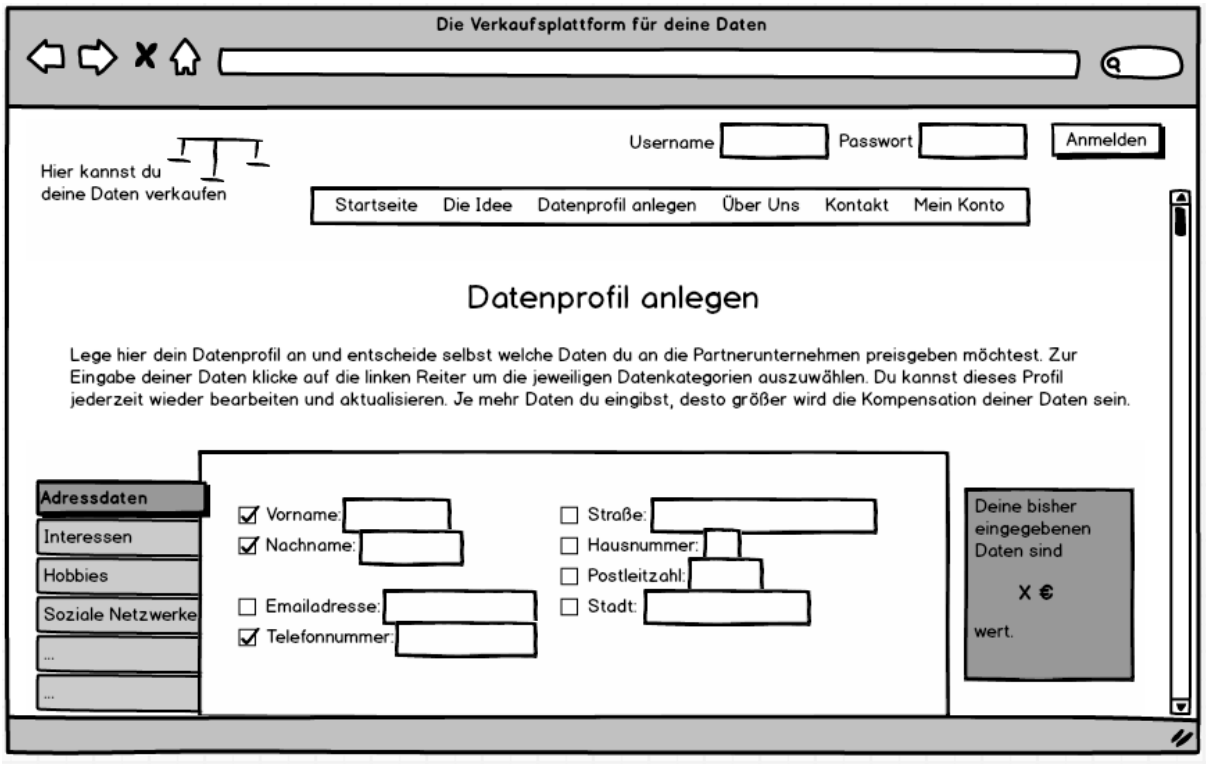
Anhang 5: Übersicht über die Studien der strukturierten Literaturrecherche

Tsai et al. 2011	Steinfeld 2015	Staiano et al. 2014	Spiekermann and Korunovska 2017	Spiekermann et al. 2012	Schreiner and Hess 2015	Rose 2005	Roeber et al. 2015	Regner and Riener 2017	Racherla et al. 2011	Pu and Grossklags 2016	Preibusch 2015	Preibusch 2013	Preibusch et al. 2013	Potoglou et al. 2013	Nguyen et al. 2016	Krasnova et al. 2014	Krasnova et al. 2009	Kamleitner et al. 2016	Jentzsch 2014	Huberman et al. 2005	Hann et al. 2007	Hann and Lee 2002	Grossklags and Acquisti 2007	Egelman et al. 2013	Egelman et al. 2009	Danezis et al. 2005	Cvrcek et al. 2006	Christin et al. 2013	Carrascal et al. 2013	Bughin 2011	Brush et al. 2010	Beresford et al. 2012	Bendorf and Normann 2014	Bauer et al. 2012	Barak et al. 2013	Acquisti et al. 2009			
		X																										X									Persönlichkeitsmerkmale	Person.	Untersuchungsfaktoren
		X				X	X			X	X			X		X	X			X	X	X	X	X	X		X	X	X	X	X					X	Demographische Begebenheiten		
						X	X																X					X									Allgemeine Daten	Datentyp	
	X		X	X	X					X						X	X													X			X	X			Soziale Netzwerkdaten		
		X							X															X		X	X	X			X				X		Standortdaten		
X								X					X	X											X							X				X	Kaufinformationen		
											X	X		X							X	X							X	X							Browserdaten		
																				X			X														Alter und Gewicht		
																			X				X														Testresultate (IQ Score)		
		X							X						X			X						X													Smartphone-Daten		
																		X					X													X	Endowment Effekt	.	
													X											X												X	Order Effekt		
X																									X												Datenschutzsymbole	Privatsphäre	
									X					X																							Datenschutzerklärung		
X	X	X		X	X			X	X	X	X	X	X		X	X				X			X	X	X			X	X		X	X				X	Privatsphäre-Bedenken		
		X					X				X	X		X		X		X							X	X	X	X	X		X		X		X		Sensitivität der Daten		
							X																			X	X	X	X		X						Verwendungszweck		
							X					X	X	X													X	X									Datenspeicherung		
																					X	X															Fehlerbegrenzung		
																					X	X															Unsachgemäßer Zugriff		
				X								X		X							X	X															Sekundäre Datennutzung		
	X							X			X								X										X				X		X	X	Identifizierung		
							X								X													X									Datenerhaltenden Instanz		
		X																																X			Nutzungsintensität	Individuell	
					X																																Wahrgenommene Kontrolle		
																				X																	Wahrgenommene Attraktivität		
			X	X														X																			Psychologie des Eigentums		
									X																												Soziale Norm	Sozial	
																					X	X														X	Zukünftiger Nutzen	Wertbez.	
			X	X																																	Wertbewusstsein		
	X						X				X										X	X	X												X		Monetäre Vergütung		
X				X	X	X		X	X	X		X	X	X	X	X	X	X					X	X	X					X		X		X		X	Zahlungsbereitschaft		Wert v. Daten
	X	X	X				X				X							X	X	X	X	X	X			X	X	X	X		X		X		X	X	Verkaufsbereitschaft		
	X		X	X					X									X					X					X								X	Offene Fragen	Umfragen	Messmethoden
	X					X																	X	X											X		Geschlossene Fragen		
							X			X							X				X	X								X							Conjoint-Analyse		
														X	X	X									X												DCM		
X								X			X	X	X												X								X				Laborexperimente	Experimente	
																																X				X	Feldexperimente		
		X																	X	X				X		X	X		X		X						Reverse VA		
					X																												X	X			BDM		
			X	X		X	X	X	X	X				X	X	X	X	X			X	X	X	X				X		X				X	X	X	Hypothetisch		Anreiz
X	X	X			X						X	X	X						X	X			X	X	X	X	X		X		X	X	X			X	Rrealistisch		

Anhang 6: Das Mockup beschreibt die Idee von Datenverkaufsplattformen



Anhang 7: Das Mockup zeigt wie ein Datenprofil angelegt werden kann



Anhang 8: Das Mockup bildet beispielhaft ein Nutzerkonto ab