Der Wert persönlicher Daten

Ist Datenhandel der bessere Datenschutz?

Berlin in September 2016

VerfasserInnen:
Walter Palmetshofer, Arne Semsrott, Anna Alberts - Open Knowledge Foundation Deutschland e.V.

Auftraggeber:
Der Sachverständigenrat für Verbraucherfragen
beim Bundesministerium der Justiz und für Verbraucherschutz

Inhaltsverzeichnis

1. Einführung

Die Informations- und Kommunikationstechnologien haben in den vergangenen Jahren eine starke Weiterentwicklung erfahren. Dieser Fortschritt führt dazu, dass die Erfassung persönlicher Daten inzwischen in vielen Lebensbereichen allgegenwärtig geworden ist. Es ist inzwischen gängige Praxis, dass es beispielsweise bei Einkäufen, Finanzdienstleistungen oder Arztbesuchen zu einer Erfassung von persönlichen Daten kommt. Sie können in großem Ausmaß digital gespeichert, verarbeitet und verwertet werden.

VerbraucherInnen haben die Möglichkeit, auf unterschiedlichen Online-Plattformen Profile zu erstellen, die wiederum von den dazugehörigen Unternehmen über verschiedene verwendete Geräte und Webseiten hinweg wiedererkannt werden können. Eine Vielzahl von elektronischen Geräten ist inzwischen mit Sensoren ausgestattet, welche wiederum mit dem Internet verbunden sind. Diese Verbindungen ermöglichen den BesitzerInnen der Daten umfassende Einblicke in das Konsumverhalten und Privatleben der Bevölkerung. Das Nutzungsverhalten sowie räumliche Bewegungen von VerbraucherInnen können dabei detailliert ausgewertet werden. Außerdem können die Persönlichkeit und Interessen der jeweiligen Personen analysiert und bewertet werden. Im Zeitalter von Big Data sind solche Handlungen teilweise schon aus rudimentären Metadaten automatisiert möglich.

Firmen, die in den Feldern der sozialen Netzwerke, der Online-Werbung sowie von mobilen Apps oder Fitness-Anwendungen tätig sind, arbeiten intensiv an der Optimierung von Geschäftsmodellen, die auf der kommerziellen Verwertung dieser gesammelten Profile beruhen. Insgesamt ist zu erwarten, dass derartige Verwertungsmodelle für die Wirtschaft schrittweise immer zentraler werden. Bereits heute werden Daten vielerorts als das „neue Öl" des 21. Jahrhunderts[1] bezeichnet.

Aus Sicht des Verbraucherschutzes interessiert dabei vor allem die Frage, von wem und wie Daten im Rahmen der neuen Geschäftsmodelle verwendet werden und wie dies reguliert werden sollte. Internationale Unternehmen agieren bei der Speicherung und Verarbeitung von Daten deutscher NutzerInnen schon jetzt oft unter Missachtung deutscher Datenschutzgesetze. Dabei gilt oft die Devise: Gemacht wird, was technisch möglich ist. In vielen Wirtschaftssektoren, von Marketing und Handel bis zur Versicherungs-, Finanz- und Personalwirtschaft, herrscht aufgrund der neuen Möglichkeiten Aufbruchsstimmung. Laut einer Studie von Digital Catapult beträgt das wirtschaftliche Potential der persönlichen Daten alleine für den britischen Markt 2017 etwa 15 Milliarden britische Pfund.[2]

Bei dem rasant wachsenden Markt für persönliche Daten stellt sich auch die Frage nach der sinnvollen Gestaltung von Rahmenbedingungen. Für einen langfristigen und nachhaltigen Umgang für BürgerInnen mit ihren Daten ist es wichtig, dass sie über ihre persönliche Daten aufgeklärt sind: Was sind persönliche Daten? Was sind meine Daten wert? Wie und unter welchen Voraussetzungen ist die kommerzielle Verwertung meiner persönlichen Daten möglich?

[1] Kroes, 2013
[2] Greenhalgh, 2015

Diese Fragen sollen mit dem vorliegenden Text beantwortet werden. Ziel dieser Studie ist, eine allgemein verständliche Übersicht zum Handel mit Daten zu erstellen, die den Wert von Daten strukturiert erfasst.

Mit dem Wissen um den Wert ihrer Daten werden VerbraucherInnen dazu ermächtigt, bessere, informierte Entscheidungen über den Umgang mit ihren persönlichen Daten zu treffen. Auf Basis der Erkenntnisse aus der Studie werden schließlich Empfehlungen für EntscheidungsträgerInnen aus Politik, Verwaltung, Wissenschaft und Wirtschaft formuliert, die dabei helfen können, das Potential persönlicher Daten zu nutzen und bestimmte persönliche Daten von VerbraucherInnen zu schützen.

1.1 Ziele und Fragestellung

Das Forschungsfeld zur Verwertung persönlicher Daten ist noch relativ neu. Daher gibt es noch keine gesicherten Erkenntnisse darüber, welches reale wirtschaftliche Potenzial von diesen persönlichen Daten für die VerbraucherInnen unter welchen Bedingungen entstehen kann. Bisher fehlen umfassende und langfristig empirisch erhobene Daten zum Handel von Individuen mit ihren persönlichen Daten.

Hier setzt diese Studie an. Die Kernfragen sind:

- Wie werden persönliche Daten bewertet?
- Wie funktionieren bestehende Marktsegmente für den Handel mit persönlichen Daten?
- Wie können NutzerInnen selbst an diesem Markt teilnehmen?

Da es in der vorliegenden Studie im Kern um den Markt für persönliche Daten geht, werden wir zunächst im zweiten Kapitel grundlegende Konzepte und Begriffe um „persönliche Daten” klären. Anschließend analysieren wir verschiedene Modelle und Werkzeuge, die eine Bewertung persönlicher Daten ermöglichen und vergleichen Schätzungen zum Wert von Daten.
Im dritten Kapitel wird zunächst dargestellt, welche Arten der Datenvermarktung heutzutage bereits etabliert sind und welche technischen Herausforderungen im Zusammenhang mit der Vermarktung persönlicher Daten bestehen. Anschließend gehen wir auf verbraucherzentrierte Modelle zum Datenhandel ein.
Im vierten Kapitel analysieren wir die drei Marktsegmente des Datenhandels mithilfe der Rollen in der Wertschöpfungskette von Daten: das Marktsegment des Datenhandels gegen Services, das Marktsegment für Datenspenden sowie das Marktsegment zum Datenhandel gegen Entgelt.
Wir evaluieren das Potenzial der verschiedenen Marktmodelle auf ihre Möglichkeiten der Wertschöpfung und zeigen, dass der Datenhandel gegen Entgelt noch nicht ausgereift ist. Deswegen schließen wir die Studie mit einem verbraucherpolitischen Ausblick und Empfehlungen für diesen Bereich.

1.2 Methodologie

Um Segmente des Datenmarktes darzustellen, wird die Wertschöpfungskette (Personal Data Value Chain, vgl. Abbildung 1)[3] als zentrales Analyseinstrument genutzt. Sie macht es möglich, eine Analyse der freiwillig bereitgestellten, beobachteten oder abgeleiteten Daten im Markt vorzunehmen und die verschiedenen Aktivitäten wie Datenerfassung, Speicherung, Anreicherung, Analyse und Gebrauch zu beobachten. Außerdem können durch sie diejenigen Bereiche identifiziert werden, in denen der Wert von persönlichen Daten generiert wird.

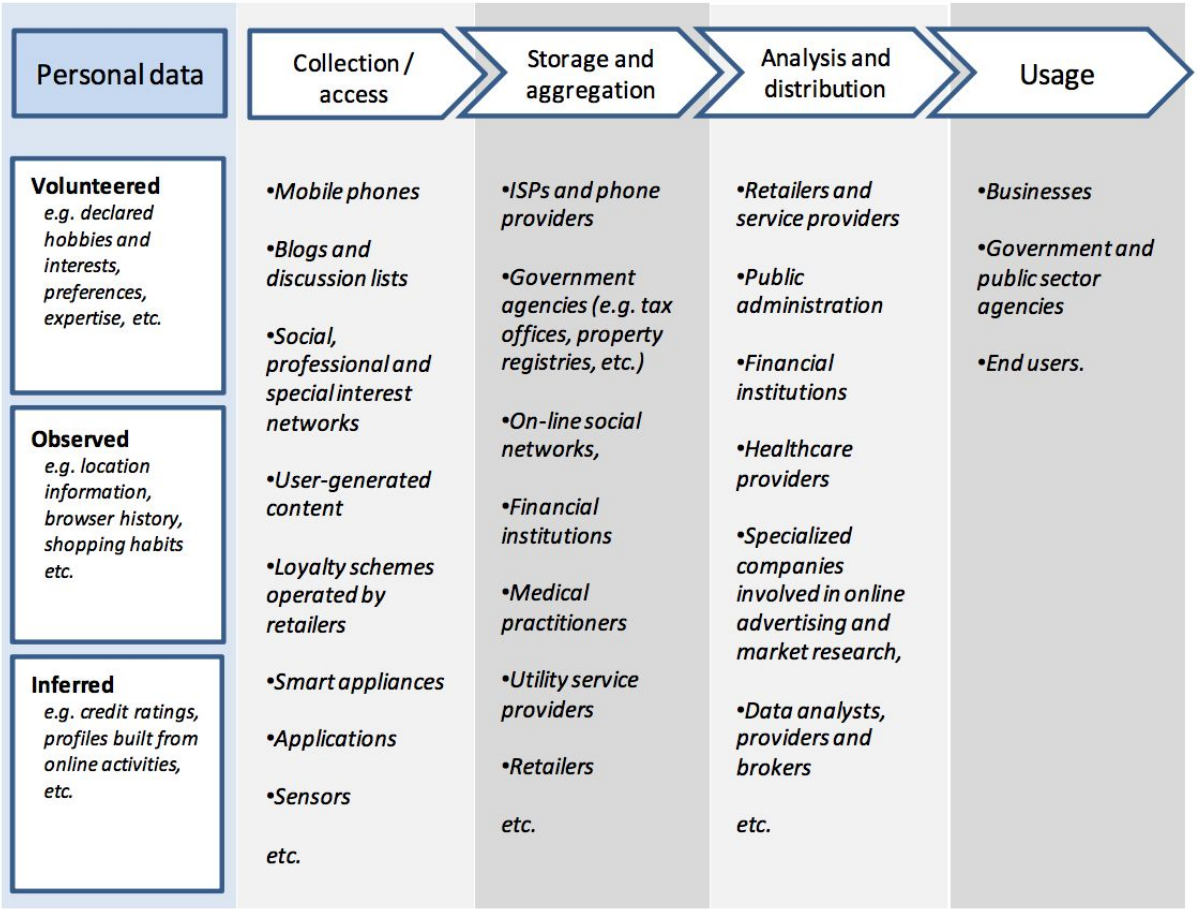

Abbildung 1: Personal Data Ecosystem[4]

Der Datenmarkt wird vor allem dadurch charakterisiert, dass die VerbraucherInnen zeitgleich sowohl das Produkt als auch die (Teil)-ProduzentInnen sind. Durch die Wertschöpfungskette kann analysiert werden, wie das jeweilige Wertschöpfungspotenzial der einzelnen Segmente des Datenmarktes aus Sicht der VerbraucherInnen ist.

[3] OECD, 2013a
[4] WEF, 2011 in OECD, 2013a

Unsere Analyse im zweiten und dritten Kapitel zum Wert von Daten und Möglichkeiten des Datenhandels stützt sich auf die Arbeit von Simon Bründl, Christian Matt und Thomas Hess. In ihrem Beitrag „Forschungsbericht Wertschöpfung in Datenmärkten"[5] verwenden sie ebenfalls die Wertschöpfungskette zur Analyse des Werts von persönlichen Daten und beschreiben die Determinanten für den monetären Wert von Daten aus Sicht der Unternehmen. Außerdem befassen sie sich mit den verschiedenen Rollen der jeweiligen Marktteilnehmer.
Die Zusammenführung der Themenbereiche leitet uns schließlich zurück zu unserer Gesamtanalyse - den Vergleich der Aspekte des Datenschutzes und der Rolle der VerbraucherInnen in den verschiedenen Marktsegmenten des Handels mit persönlichen Daten.

Methoden

Die vorliegende Studie basiert auf einer Vielzahl von verschiedenen Quellen: einer systematischen Literaturrecherche, gezielter Suche in internationalen Online-Archiven von Zeitungen und digitalen Medien sowie auf Webseiten von Unternehmen, Organisationen und zuständigen Behörden. Außerdem haben wir zahlreiche Gespräche geführt mit ExpertInnen für Verbraucherschutz, Datenschutz, Netzpolitik, IT-Sicherheit, Web-Technologie, Open and Big Data, Startups im Bereich Datenhandel, soziale Medien, Marketing, Quantified Self, Venture Capital und Ökonomie (vgl. Anlage IV). Die Interviews wurden größtenteils aufgezeichnet, transkribiert und evaluiert. Etliche Aussagen in den Interviews wurden durch die Literatur bestätigt. Die aktuellen Angebote zum Handel mit persönlichen Daten wurden analysiert und, wenn möglich, durch die Verfasser selbst über einen längeren Zeitraum genutzt. Manche behandelten Themen konnten umfangreicher analysiert, manche auch nur ansatzweise beschrieben werden. Da etliche Unternehmen im Bereich des Datenhandels nicht immer transparent agieren,[6] ist die Quellenlage oft nicht zufriedenstellend.

Aussagekraft der Ergebnisse

Zudem entwickelt sich der Markt rasant: Die vorhandenen wissenschaftlichen und journalistischen Recherche-Ergebnisse beziehen sich daher in wenigen Fällen auf Services oder Apps, die inzwischen nicht mehr zur Verfügung stehen oder weiterentwickelt worden sind.

[5] Bründl et al., 2015
[6] Dies betrifft vor allem konkrete Aussagen zu Preisen und Prognosen am Datenmarkt. Sind Angaben der Unternehmen die einzig vorhandenen Quellen, so sind diese nur teilweise valide. Da viele Unternehmen nicht nur auf VerbraucherInnen zugehen, sondern ihre Dienstleistungen auch an ihre kommerziellen KundInnen verkaufen müssen, lassen sich aus den dazugehörigen Werbedokumenten einige Erkenntnisse über ihre Arbeitsweise ziehen. Dieser Informationsfluss ist meist ergiebiger als die direkt an VerbraucherInnen gerichtete Kommunikation.

2. Datenarten und Datenwerte

In diesem Kapitel definieren wir den Begriff der „persönlichen Daten" und grenzen ihn von anderen Arten von Daten ab. Wir zeigen, wie Daten anhand des Datenspektrums des ODI klassifiziert werden können und wie Daten anonymisiert und pseudonymisiert werden. Beides ist für VerbraucherInnen wichtig, um die Signifikanz des Datenhandels besser einordnen zu können. Danach folgen konkreten Einschätzungen des Wertes persönlicher Daten aus Sicht von VerbraucherInnen sowie aus Sicht von Unternehmen, um die verschiedenen Ansätze als Ausgangsbasis für das Verständnis von Datenmärkten zu etablieren.

2.1 Definition und Abgrenzung des Begriffs „persönliche Daten"

Wie werden persönliche Daten definiert?

Laut OECD[7] werden unter persönlichen Daten und Metadaten sämtliche Informationen verstanden, die sich auf eines oder mehrere identifizierbare Individuen beziehen. Rose et al.[8] verstehen unter persönlichen Daten hingegen einschränkend nur alle digital verfügbaren Informationen, die über das Online- oder Offline-Verhalten einer Person bekannt sind. Das deutsche Bundesrecht definiert in § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) personenbezogene Daten als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Die entsprechenden landesgesetzlichen Definitionen haben den gleichen oder einen ähnlichen Wortlaut.[9]

Klassifikation persönlicher Daten

Wir verwenden das weitergehende Konzept der OECD für solche personenbezogenen Daten, die Soziodemografie betreffen (z.B. Geburtsdaten, Geschlecht, Familienstand, Haushaltsgröße, Bildung, berufliche Situation, Haushaltsnettoeinkommen), nutzer-generierte Inhalte (z.B. Postings auf Facebook, Blogartikel, Kommentare, Tweets), Verhaltensdaten im Internet (z.B. Suchanfragen, Reiseplanung), Daten des sozialen Umfelds (z.B. Bekannte, Familienmitglieder oder Arbeitskollegen) sowie weiterführende personenbezogene Identifikationsdaten (z.B. Reisepass und Ausweisnummern).

Diese persönlichen Daten entstehen bei der Nutzung des Internets unter anderem durch Cookies, digitale Fingerprints von Browsern, Betriebssysteme und Bildschirmauflösung und

[7] OECD, 2013b
[8] Rose et al., 2012
[9] Richtlinie 95/46/EG http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046

über Aktivitäten in Social Media Portalen wie Facebook, Twitter, Snapchat und Instagram. Weitere Möglichkeiten für die Entstehung solcher persönlichen Daten sind Einträge in Online-Foren oder Blogs, Anfragen bei Suchmaschinen, getätigte Transaktionen wie Online-Einkäufe, -Buchungen und -Banking. Des Weiteren werden durch die Nutzung von Sprachassistenten wie Siri, Cortana, Google und Amazon Echo massenhaft persönliche Daten aufgezeichnet. Diese Daten können mit Bewegungsdaten (GPS) von mobilen Endgeräten, Navigationsgeräten und Connected Cars verbunden werden. Daten aus dem öffentlichen Raum, beispielsweise durch Videoüberwachung oder andere Sicherheitssysteme können ebenfalls hierfür genutzt werden. Zusätzlich zeichnen auch mobile Apps, Smart TVs, Spielekonsolen und andere webfähige Multimedia-Anlagen sowie Fitness-Armbänder und -Tracker persönliche Daten auf.

Diese Daten werden übermittelt bzw. gespeichert auf drei Ebenen[10]:

- Unmittelbare Ebene: Freiwillige Übermittlung (z.B. durch Anmeldung bei einem Service)
- Mittelbare Ebene: Beobachtung von Daten, die eine Person preisgibt (z.B. Webbrowser-Verlauf, GPS-Positionen, Gesundheitstracker)
- Abstrakte Ebene: Ableitungen und Analysen von Daten, die von einer oder mehreren Personen freigegeben worden sind[11] (z.B. Online-Profile und Facebook-Likes)

Nach Schneier[12] können persönliche Daten insbesondere in sozialen Netzwerken unterteilt werden in Servicedaten (für die Anmeldung), offengelegte Daten (Postings, Bilder, ..) anvertraute Daten (Postings auf anderen Benutzerkanälen), anfallende Daten (Posting über eine Person von Dritten erstellt) sowie Verhaltensdaten (Metadaten über Interaktionen und weitere Aktivitäten). Die Kategorisierung der persönlichen Daten erfolgt oft auch durch die Verwendung der Daten, die für einen bestimmten Dienst gesammelt und analysiert oder an Dritte weiter vermittelt werden.[13]

Werden eine große Zahl von verschiedenen Diensten gemeinsam von einer Person genutzt, kann es zu einer annähernden Kompletterfassung, also der größtmöglichen Speicherung aller persönlichen Daten kommen, beispielsweise bei der Kombination der Daten aus einem Genetik-Test wie 23andme, Verwendung von Social Media, bargeldlosen Zahlungen und Fitnesstrackern.

Von vielen VerbraucherInnen wird die Sammlung persönlicher Daten stillschweigend akzeptiert. Das hängt zum einen mit fehlendem Wissen über den Umfang und die Verwendung der erfassten Daten zusammen. Vor allem die langfristige Nutzung von persönlichen Daten und Auswirkungen der Speicherungen über einen Lebenslauf sind VerbraucherInnen bei der Einwilligung zur Erfassung ihrer Daten in der Regel nicht präsent. Zum anderen führt das Gefühl der Ohnmacht über die Möglichkeiten der Mitbestimmung bei der Datenverwendung häufig dazu, dass VerbraucherInnen sich nicht näher mit einzelnen Bestimmungen zum Datenschutz beschäftigen („Facebook, Google und die NSA machen sowieso, was sie wollen. Das können wir gar nicht überprüfen.")

[10] WEF, 2012
[11] Mit der Analyse von Facebook-Likes ist es mit einer Wahrscheinlichkeit von über 75% möglich, das Geschlecht, Alter und sexuelle Präferenzen einer NutzerIn korrekt zu bestimmen (vgl. Kosinski et al., 2012)
[12] Schneier, 2009
[13] FTC, 2009

Um im Gegensatz dazu VerbraucherInnen zu ermächtigen, über ihre Daten selbstständig zu entscheiden, ist es wichtig, Möglichkeiten für die Berechnung des Werts von persönlichen Daten bereitzustellen. Dies kann Ausgangspunkt sein, um ihnen zunächst den Umfang von Datensammlungen bewusst zu machen und sie anschließend dazu zu ermutigen, sich für ihre Rechte einzusetzen.

Das Ausmaß der Datenerfassung durch Unternehmen ist in der Regel allgemein nicht bekannt.[14] Für die Nutzung kostenloser Angebote im Internet gilt jedoch die Grundregel:

> *'If you are not paying for it, you're not the customer; you're the product being sold'*
> *(Andrew Lewis und Richard Serra)*[15]

Die unabsichtliche Bekanntgabe von persönlichen Daten durch Dritte in sozialen Netzwerken durch Postings oder Analysen kann gravierende Nachteile selbst für eine Person haben, die selbst nicht die Daten freigegeben hat, sondern nur durch die Vernetzung mit der Person bewertet wird. Es ist etwa möglich, dass Daten über Facebook-Freunde in die Bonitätsberechnung eines Dritten einbezogen werden, darunter auch auf einem Rechner installierte Schriftarten, die ein Hinweis auf die Nutzung von bestimmten Online-Glücksspielen sein können (sog. Kredittech[16]).

[14] 84% der britischen VerbraucherInnen vermuten, dass weniger als 20 Organisationen persönliche Daten von ihnen speichern (vgl. Powell, 2016)
[15] http://www.metafilter.com/95152/Userdriven-discontent#32560467
[16] Seibel, 2015

Anonymisierung von persönlichen Daten

Aus datenschutzrechtlichen Gründen werden persönliche Daten meist entpersonalisiert. Zum einen können sie anonymisiert werden, d.h. Unternehmen entfernen einen konkreten Personenbezug. Nach dem Bundesdatenschutzgesetz ist **Anonymisieren** „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche und sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können." (BDSG §3 Abs. 6)

Zum anderen können sie pseudonymisiert werden. Bei der Pseudonymisierung werden Namen oder andere Identifikationsmerkmale durch Pseudonyme oder Codes ersetzt. Dabei werden Attribute weggelassen, jedoch bleiben Identifier für Personen übrig. Nach dem Bundesdatenschutzgesetz ist **Pseudonymisieren** „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren." (BDSG §3 Abs.6a)

Die Unterscheidung zwischen persönlichen und nicht-persönlichen Daten wird tendenziell immer schwieriger. Sobald einmal Daten mit einer Person bzw. ihrer wahren Identität verknüpft sind, ist die Anonymität der Person langfristig aufgehoben.[17]

Ohnehin sind Personen in der Regel schon mit dem Vorliegen weniger verknüpfter Daten individuell identifizierbar. Zum Beispiel sind Postleitzahl, Geschlecht und Geburtsdatum bei 216 von 248 Millionen und somit bei 87% der US-AmerikanerInnen einzigartig.[18] Der einfache Vergleich von gehashten privaten Daten[19] wie einer E-Mail-Adresse kann zum Tracking verwendet werden. Auch das „Apotheken-Beispiel" zeigt, wie wenige Daten für eine Identifizierung ausreichend (vgl. Anlage II).

Apple hat im Sommer 2016 die Verwendung von Differential Privacy angekündigt.[20] In dem Verfahren werden persönliche Daten mit randomisierten Daten ergänzt, um eindeutige Aussagen über bestimmte Eigenschaften der Daten unmöglich zu machen.[21] Sollte sich Differential Privacy durchsetzen, könnte es sich aufgrund der Größe von Apple auch in anderen Marktbereichen durchsetzen. Es gibt an dem Konzept allerdings auch Kritik.[22]

[17] Narayanan und Shmatikov, 2010
[18] Sweeney, 2002
[19] FTC, 2012
[20] Sherry, 2013
[21] Greenberg, 2016
[22] Bambauer et al., 2013

Open Data, Shared Data, Closed Data

Hilfreich zur allgemeinen Klassifizierung persönlicher Daten ist das Open-Shared-Closed-Datenspektrum des Open Data Institute (ODI, vgl. Abbildung 2). Danach sind Open Data solche Daten, auf die jede/r zugreifen kann und die jede/r nutzen und teilen kann. Closed Data sind Daten, die nur ihrer BesitzerIn zugänglich sind. Shared Data lassen sich in drei Varianten unterteilen: In Daten, die nur mit benannten Personen/Organisationen geteilt werden (Named access), Daten, die nur Gruppen gemäß spezifischer Kriterien zugänglich sind (Group-based access) und Daten, die allen zugänglich sind, jedoch nicht zu offenen Bedingungen (Public access).

Dieses Modell bringt zwar VerbraucherInnen nahe, wie deren Daten in Bezug auf ihre Freigabe und Weitergabe behandelt werden können (z.B. für die Öffentlichkeit oder Forschung). Für den Handel mit persönlichen Daten bedarf es allerdings der Umsetzung komplexerer und detaillierterer Modelle.[23]

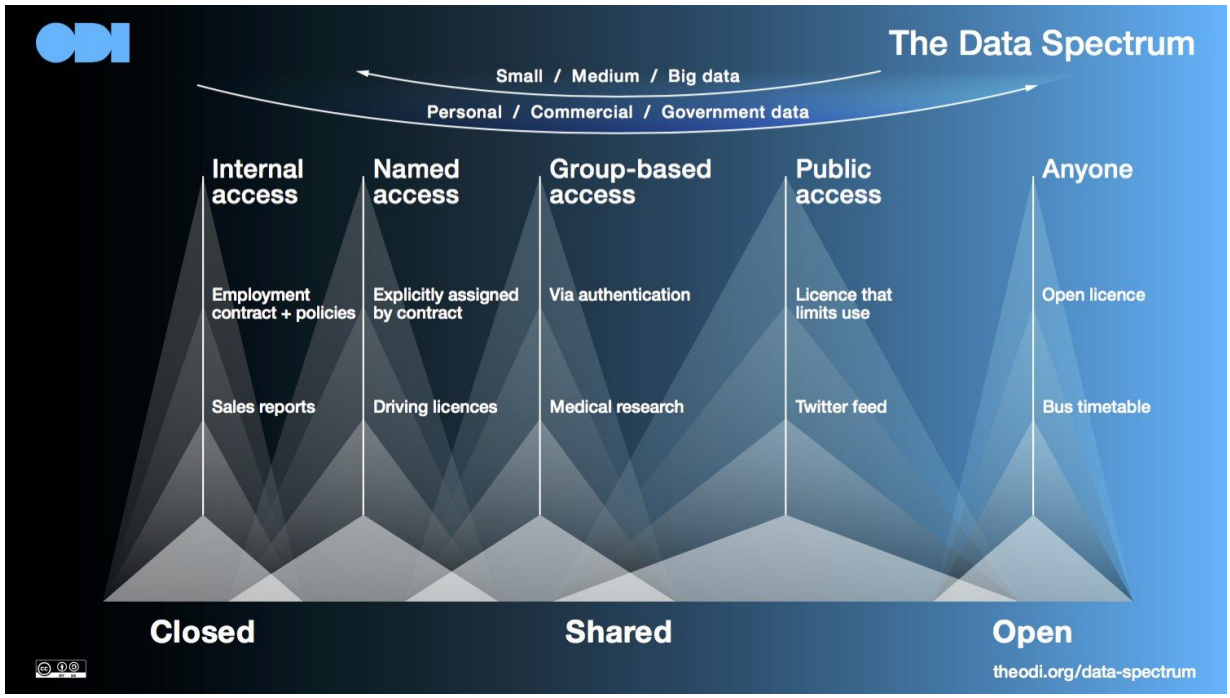

Abbildung 2: Datenspektrum nach ODI für Datenveröffentlichung von Benutzern[24]

[23] Ein Beispiel von User-Managed Access (UMA) zeigt Hardjono, 2015
[24] Broad, 2015

2.2 Einschätzung des Werts persönlicher Daten

Die genaue Bemessung des Wertes von persönlichen Daten[25] für VerbraucherInnen ist eine große Herausforderung: Es gibt keine allgemeingültige Methode, um einen solchen Wert festzustellen.[26] Die Annäherung des Wertes erfolgt bisher über Marktbewertungen von persönlichen Daten oder individuelle Einschätzungen des Werts persönlicher Daten.
Fest steht: persönliche Daten sind aktuell das Rückgrat der Internetökonomie. 90% des Umsatzes von Google und 95% des Umsatzes von Facebook sind an Werbung gekoppelt, die auf der Analyse persönlicher Daten basiert.[27] 2016 wird der Umsatz der beiden Firmen ca. 100 Mrd. US-Dollar umfassen.[28]

Grundsätzlich gilt: Je spezifischer, genauer und aktueller mit Kontext die Informationen sind, desto wertvoller sind sie und desto höher ist ihr Preis.[29] Besonders interessant für Unternehmen sind Wendepunkte im Leben der VerbraucherInnen wie etwa Heirat, Schwangerschaft oder eine Krankheit, weil sie den Eintritt in neue Märkte markieren und Potenzial für Neukunden schaffen.

Einschätzungen von VerbraucherInnen zum Wert ihrer Daten

81% der Verbraucher in Europa denken, dass ihre persönlichen Daten einen bestimmten Wert haben. Eine/r von drei VerbraucherInnen gibt falsche Informationen an, um ihre Privatsphäre zu schützen. 68% der Befragten sind bereit, ihre Privatsphäre für eine kostenlose App ein zu tauschen.[30] Männer schätzen den Wert ihres Browserverlaufs mit bis zu 1.057 britischen Pfund ein. Der vermutete Wert ist fast ein Drittel höher als bei Frauen.[31]
Das Vertrauen in den Datenschutz ist dabei gering: Laut dem Global Consumer Trust Report[32] gab im Jahr 2013 noch ein Fünftel der Befragten an, dass es seine Daten gerne mit einer App teilt. 2015 ist dieser Wert auf 6% gesunken. 39% der VerbraucherInnen sind mit dem Datenschutz nicht zufrieden, 38% teilen Ihre Daten gar nicht und 41% nur, weil sie keine andere Möglichkeit sehen.
Von allen Diensten vertrauen VerbraucherInnen am wenigsten sozialen Netzwerken. Gesundheitsapps vertrauen sie trotz der sensitiven Daten mehr. 26% sehen Finanzdaten als die sensibelsten Daten an vor Fotos (18%) und Kontakten (15%). 21% der VerbraucherInnen unternehmen nichts, um ihre Geräte zu sichern oder ihre Software zu aktualisieren.

[25] vgl. auch die Bezeichnung „Asset Class": WEF, 2011; bzw. „persönliche Daten als Währung": D-Cent, 2013
[26] OECD, 2013b
[27] Pollack, 2016
[28] Johnsen, 2016
[29] vgl. http://www.femtechleaders.com/oceania/katryna-dow-2/
[30] Gjermundrød, 2015
[31] Jardine, 2016
[32] Global Consumer Trust Report, 2016

2.2.1 Wert persönlicher Daten aus Sicht von VerbraucherInnen

Bei Untersuchungen zum Verhalten von VerbraucherInnen kristallisiert sich heraus, dass diese zwar generell ein gewisses Bewusstsein für den Schutz von Privatsphäre haben. Allerdings beeinflusst dies ihr Verbraucherverhalten nicht signifikant. So lehnt eine Mehrheit der Internet-NutzerInnen personalisierte Werbung ab,[33] [34] aber gleichzeitig verwendet die Mehrheit soziale Netzwerke und stellt Teile ihrer persönlichen Daten offen ins Netz. Dieses Auseinanderdriften von Einstellungen und konkretem Handeln in der digitalen Welt wird als Privacy Paradox bezeichnet[35] [36] und ist mehrfach empirisch belegt worden[37] [38], auch in Deutschland[39].

Unter verschiedenen Umständen sind VerbraucherInnen bereit, persönliche Daten preiszugeben. Dies kann mittels zweierlei gegensätzlicher Ansätze gemessen werden: Zum einen mit dem angenommenen Wert der persönlichen Daten, also dem Preis, für den die Person bereit ist, ihre Daten offenzulegen („Willingness to Accept“ - WTA). Zum anderen mit dem angenommenen Wert der Privatsphäre, also dem Preis, den die Person bereit ist zu bezahlen, um ihre persönlichen Daten zu schützen („Willingness to Pay“ - WTP).

Grundsätzlich sind weniger Personen bereit, Geld für Privatsphäre auszugeben (WTA) als sie bereit sind, für einen gleichen Preis einen Teil ihrer Privatsphäre aufzugeben (WTP).[40] Bei solchen Bewertungen sei darauf hingewiesen, dass sie stark kontextbezogen sind.[41]

Die folgenden Bewertungen aus Sicht von VerbraucherInnen und Unternehmen umfassen nur den monetären Wert und nicht den gesellschaftlichen oder volkswirtschaftlichen Wert von einzelnen Datensätzen bzw. persönlichen Daten eines/einer VerbraucherIn.

Zahlungsbereitschaft für Privatsphäre / willingness to pay

Kostenpflichtige Services, die die Privatsphäre ihrer NutzerInnen berücksichtigen, bilden ein Gegenmodell zu Gratis-Angeboten, die persönliche Daten kommerziell nutzen. Wie hoch liegt die WTP für solche kostenpflichtigen Services?
Die Antwort auf diese Frage hängt von den jeweiligen Daten ab, die geschützt werden sollen. VerbraucherInnen sind bereit, für den Schutz besonders sensibler persönlicher Daten regelmäßig niedrige einstellige Eurobeträge aufzubringen. Dies betrifft etwa Kommunikationsinhalte, Standortdaten und bestimmte Daten über das Internetverhalten (vgl. Tabelle 1).

[33] Rainie/Duggan, 2016
[34] Fittkau & Maaß, 2009
[35] Spiekermann et al., 2002
[36] SVRV, 2016
[37] Barnes, 2006
[38] Dienlin/Trepte, 2014
[39] Krasnova/Veltri, 2010
[40] Acquisti et al., 2009
[41] ebd.

Tabelle 1: Untersuchungswerte zur Zahlungsbereitschaft für Privatsphäre / WTP

Preis	**Erläuterung**
1 Euro	Ein Drittel der Nutzer von Online-Einkaufsplattformen ist in einer Feldstudie bereit, einen Euro mehr zu zahlen, um nicht die eigene Mobiltelefonnummer angeben zu müssen.[42]
2-3 Euro pro Monat	Durchschnittliche Bezahlung für E-Mail-Dienst und Suchservice[43]
15 Dollar im Jahr	Bereitschaft zur Zahlung, damit E-Mails nicht gescannt werden; bei einem Drittel der Befragten pro Jahr[44]
155 US-Dollar	Jährlicher Preis für ProtectMyID[45]
29,95 Euro	Kaufpreis für Third-party blocker services, z.B. „little snitch"
1,19 US-Dollar	einmalige Zahlung, um in einer App:[46] *- den persönlichen Standort nicht preiszugeben*
1,75 US-Dollar	*- die Mobiltelefon-ID schützen*
2,28 US-Dollar	*- die Browser-History zu schützen*
3,58 US-Dollar	*- die Verschlüsselung von Textnachrichten zu installieren*
4,05 US-Dollar	*- den Schutz vor dem Zugriff auf die Kontaktlisten zu gewährleisten*
2-3 US-Dollar im Monat	Theoretische Zahlungsbereitschaft für Services wie Facebook oder Google
ca. 0,50 Euro	Zahlungsbereitschaft für Schutz der Telefonnummer bei Kinokartenkauf[47]
ca. 5 Euro im Monat	Nutzungspreis für VPN-Service, u.a. um die eigene Herkunft beim Webseitenbesuch zu tarnen
mehr als 30 Euro	Gegenwert des Zeitaufwands, um Werkzeuge wie PGP, Signal, Telegram zu installieren, zu verstehen und zu nutzen

In den USA bietet das Unternehmen Reputation Defender zudem für 750 US-Dollar im Jahr eine Software an, mit der die Privatsphäre ihrer KundInnen geschützt werden sollen, insbesondere die auffindbaren Suchresultate über Suchmaschinen wie Google.[48] Dieser Preis kann für wohlhabende Schichten als Richtwert für die Bereitschaft gelten, die eigene Privatsphäre zu schützen.
Der Service Disconnect.me kostet 50 US-Dollar im Jahr. Er blockt auf bis zu drei Geräten alle Tracker und erhöht somit die Privatsphäre.[49] Ähnliche etablierte Services gibt es in Deutschland bisher nicht.

[42] Preibusch, 2013
[43] Schmidt, 2014
[44] Strahilevitz/Kugler, 2015
[45] vgl. https://www.protectmyid.com/
[46] Savage, 2013
[47] Preibusch, 2013
[48] vgl. https://uk.reputationdefender.com/protect-your-privacy/; Es gibt derzeit keinen ähnlichen Service in Deutschland.
[49] vgl. https://disconnect.me

Verkaufsbereitschaft für die Privatsphäre / willingness to accept

Nach dem WTA-Ansatz geben VerbraucherInnen den Preis an, für den sie bereit sind, ihre persönlichen Daten zu verkaufen oder Nutzungsrechte daran einzuräumen. Nach diesem Ansatz ergeben sich Preise von 15 bis 100 Euro für bestimmte Datensätze (vgl. Tabelle 2).

Tabelle 2: Untersuchungswerte und Studien zu WTA

Preis	**Erläuterung**
15 Euro	Kontaktdaten (umfasst Name, Adresse, Email, Telefonnummer)[50]
19 Euro	Facebookdaten (umfasst Name, About-Seite, Timeline)[51]
> 100 Euro	für *jeweils* Emailadresse, Location, Browserhistorie[52]

Die Werte des WTA-Ansatzes lassen sich leichter vergleichen, sind jedoch aus Labor-Experimenten entstanden. Sie haben keine Validierung am Markt. Verschiedene Studien zeigten, dass nur sehr wenige VerbraucherInnen bereit sind, Geld ausgeben, um ihre Daten zu schützen. Viele VerbraucherInnen lehnen jedoch das Angebot, zum gleichen Preis ihre persönlichen Daten zu verkaufen, ab.[53] Die Unterschiede zwischen WTA und WTP werden u.a. durch Besitztumseffekt und Verlustaversion erklärt.[54]

Eine weitere Möglichkeit, den Wert der persönlichen Daten aus Sicht der VerbraucherInnen zu veranschaulichen, ist die Bemessung des Schadens im Falle einer unerwünschten Offenlegung der persönlichen Daten und den materiellen und nichtmateriellen Auswirkungen. Hier zeigt sich, dass dies vor allem Preisnachteile nach sich ziehen kann (vgl. Tabelle 3).

Tabelle 3: Wertbemessung durch Nachteile bei Datenoffenlegung oder Schaden

Auswirkungen der Datenoffenlegung	**Ursache**
bis zu 30% Preisnachteil	Benachteiligung u.a. bei Hotel- und Flugbuchungen (vgl. Anlage II)
bis zu 33% bzw. bis zu 166% Preisnachteil	Dynamic Pricing anhand der Weiterleitung geografischer Daten[55]
weniger Auswahl bei Zahlungsoptionen	Zusammenwachsen - Risikomanagement mit Marketing (vgl. Anlage II)
Negatives Kreditrating bis hin zum Marktausschluss	unkorrekte Datensammlung bei SCHUFA oder Deltavista

[50] Benndorf und Normann (2015)
[51] ebd.
[52] vgl. http://www.totallymoney.com/personal-data/infographic/
[53] Acquisti et al., 2009
[54] Wang et al., 2013; Morando et al., 2014
[55] Mikians et al., 2012

2.2.2 Wert persönlicher Daten aus Sicht von Unternehmen

Der Wert persönlicher Daten wird von VerbraucherInnen und Unternehmen nach unterschiedlichen Kriterien eingeschätzt. Der Wert persönlicher Daten aus Sicht der Unternehmen richtet sich nach Bründl vor allem nach zwei Faktoren: dem Kontext und der Verwendung (vgl. Abbildung 3).

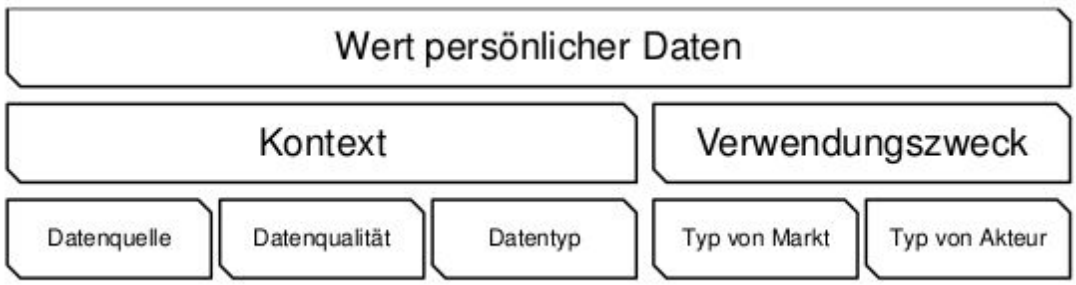

Abbildung 3: Determinanten des Wertes von persönlichen Daten[56]

Weitere Faktoren sind die Datenquelle und die Freiwilligkeit der Freigabe. Freiwillig bereitgestellte Daten haben einen höheren Wert als beobachtete. Diese wiederum sind mehr wert als abgeleitete Daten (vgl. Abbildung 1). Je höher die Datenqualität ist, desto höher ist ihr Wert. Die Datenqualität hängt unter anderem mit der Aktualität der Daten, der Verwendbarkeit, der Granularität sowie der Transparenz über die Herkunft der Daten zusammen. Der Wert hängt schließlich auch vom Verwendungszweck ab: Je teurer ein Produkt, desto wertvoller die enthaltenen Daten.

Der Wert von Daten kann pro NutzerIn oder pro Datensatz berechnet werden. Auch eine fallbezogene Berechnung des Wertes in Bezug auf Versicherungen bzw. bei Datenverlust ist möglich.

Wert der Daten nach Jahresumsatz von Firmen

Anhand des durchschnittlichen Erlöses eines Unternehmens pro VerbraucherIn pro Jahr[57] zeigt sich, dass pro VerbraucherIn das Unternehmen Twitter einen Datenwert von 5 US-Dollar festmachen kann, während der Wert bei Google um 40 US-Dollar liegt (vgl. Tabelle 4).

[56] Bründl, 2015
[57] Orcutt, 2011

Tabelle 4: Wert der persönlichen Daten anhand des durchschnittlichen Erlöses pro User (ARPU) von Services

Preis pro NutzerIn	Firma	Erläuterung
3 - 13 US-Dollar	Facebook	fürs erste Quartal 2016 ca. 3 US-Dollar weltweit, ca. 12 US-Dollar in den USA, ca. 4 US-Dollar in Europa [58]
6 US-Dollar	Experian	handelt mit Verbraucherdaten, Creditscoring[59]
38 - 45 US-Dollar	Google	Umsatz pro aktiver NutzerIn bei Google 2010 - 2015 [60]
ca. 5 US-Dollar	Twitter	Steigerung von ca. $1 in 2011[61] auf $5 in 2015[62]

Berechnet man den Wert einzelner Datensätze, die im Großhandel verkauft werden, ergibt sich ein stark differenziertes Bild zwischen einmaligen Abfragen für spezielle Kunden und dem Aufkauf von Datensätzen in großen Mengen. Die Spannbreite liegt hier zwischen wenigen Cent und 55 Euro (vgl. Tabelle 5). Die großen Unterschiede ergeben sich durch Verwendungszweck bzw. Einzel-/Massenhandel.

Tabelle 5: Wert der persönlichen Daten nach Datensatz[63]

Preis pro Datensatz	Erläuterung
ca. 1 Euro	Für einen Bulk-Datensatz über eine Person mit mehr als 30 Merkmalen (Vgl. für Details dazu den Datenrechner der Financial Times)[64]
bis zu 0,5 US-Dollar/Euro	Adressdatensatz (Name, Strasse, Postleitzahl)[65]
0,7 US-Dollar	Strecken- und Standortdaten eines Fahrradfahrers[66]
bis zu 2 US-Dollar/Euro	Geburtsdatum[67]
10 US-Dollar	Mobilfunkdaten[68] [69] pro Jahr und Benutzer
bis zu 55 US-Dollar	Gesamtdatensatz einer Person welcher Geburtsdatum, Adresse, Kredithistorie, umfasst[70]

Wert von Datensätzen für Preisnachlässe bei Versicherungen in den USA und Deutschland

Neben Datenhändlern haben auch Versicherungen ein großes Interesse daran, den Wert persönlicher Daten zu berechnen. Ersparnisse, die sich Versicherungen von der Verarbeitung der Kundendaten erhoffen, werden teilweise an die KundInnen weitergegeben.

[58] Stevens, 2016
[59] OECD, 2013
[60] http://marketrealist.com/2015/02/average-revenue-per-user-is-an-important-growth-driver/
[61] Digital Strategy Consulting, 2014
[62] vgl. https://www.statista.com/statistics/430874/twitter-annualized-advertising-arpu/
[63] vgl. https://www.brandeins.de/archiv/2014/beobachten/was-bin-ich-wert/
[64] Steel et al., 2013
[65] OECD, 2013
[66] Breithut, 2016
[67] OECD, 2013
[68] Kharif/Moritz, 2013
[69] Kaye, 2015
[70] OECD, 2013

In den USA lag dieser Wert 2016 bei bis zu 270 US-Dollar pro VerbraucherIn, in Deutschland bei bis zu 400 Euro im Jahr (vgl. Tabelle 6).[71]

Tabelle 6: Wert der persönlichen Daten anhand von Preisnachlässen bei Versicherungen

Preisnachlass nach Datensharing	**Versicherungssegment**
270 US-Dollar oder bis zu 30% Preisnachlass	Gesundheitsversicherung
199 US-Dollar oder bis zu 30% Preisnachlass	Autoversicherung
153 US-Dollar oder bis zu 5% Preisnachlass	Einbruchversicherung
50 Euro oder bis zu 16% Preisnachlass	Gesundheitsversicherung Deutschland (vgl. Anlage II)
400 Euro oder bis zu 30% Preisnachlass	Autoversicherung Deutschland (vgl. Anlage II)

Wertbemessung der persönlichen Daten nach Dateneinbrüchen

Auch Entschädigungen von Unternehmen im Zuge von Dateneinbrüchen geben einen Einblick in den Wert von persönlichen Daten. Je nach Umfang der gespeicherten Daten haben Unternehmen ihre NutzerInnen bisher mit zwei US-Dollar (Sony) bis 194 US-Dollar für den Verlust bzw. die Offenlegung von Daten entschädigt.[72] [73]

Die Boston Consulting Group hat vorhergesagt, dass der jährliche wirtschaftliche Nutzen von persönlichen Daten in Europa bis zum Jahr 2020 bis zu 330 Mrd. Euro betragen kann.[74] Umgerechnet auf die Bevölkerung würde das 2020 eine Summe von ca. 440 Euro pro Kopf bedeuten. Für die USA wird der Markt für persönliche Daten auf mehr als 150 Milliarden Dollar geschätzt.[75] Das entspricht ca. 470 US-Dollar pro VerbraucherIn.
Weitere Beispiele für den Datenhandel von Unternehmen finden sich in Anlage II.

2.3 Zusammenfassung

In den vorangegangenen Abschnitten haben wir das Konzept der „persönlichen Daten" definiert und anhand verschiedener Messansätze aufgezeigt, dass es derzeit keine einheitliche ökonomische Bewertung persönlicher Daten und einzelner Datensätze gibt. Außerdem haben wir die Spannbreite aufgezeigt, die bei der Bewertung des Preises persönlicher Daten zwischen der Sicht von VerbraucherInnen und von Unternehmen besteht.

[71] Brandeisky, 2015
[72] McAfee, 2015
[73] Sporck, 2016
[74] BCG, 2012
[75] Lemm, 2016

3. Datenhandel und Datenmärkte

„Alles, was gesammelt werden kann, wird schließlich gesammelt werden."
Max Levchin, CEO Affirm[76]

Datenmärkte sind Märkte, über die Daten zwischen Anbietern und Nachfragern ausgetauscht werden. Die Kernkomponente der Geschäftsmodelle daran teilnehmender Unternehmen sind Daten, die aggregiert oder veredelt werden oder aus denen Informationen extrahiert werden. Der Datenhandel unterscheidet sich vom normalen Handel, da Daten ein nicht-rivales Gut sind, d.h. die Daten werden bei der Nutzung nicht aufgebraucht und die Nutzung schließt andere Benutzer nicht aus. Außerdem können sie fast unendlich oft kopiert werden und die Grenzkosten, also zusätzliche Kosten für eine weitere Kopie sind sehr niedrig.[77] Dadurch ist auch deren Verbreitung im Gegensatz zu physischen Gütern relativ einfach.
Es gibt keinen konsolidierten Markt für persönliche Daten. Das Ökosystem ist dezentralisiert und komplex[78] und wird zunehmend von einer geringeren Anzahl an Firmen dominiert.[79]

In diesem Kapitel betrachten wir die Rolle der VerbraucherInnen in der Wertschöpfungskette und zeigen die Anforderungen an den Datenmarkt für VerbraucherInnen und Unternehmen auf. Danach werden die aktuellen Handelsmöglichkeiten in drei verschieden Marktsegmenten für die VerbraucherInnen betrachtet und drei verbraucherzentrierte Modelle vorgestellt.

[76] vgl. https://blog.mixpanel.com/2016/05/17/max-levchin-quantified-self-and-privacy
[77] Roberds/Schreft, 2009
[78] Olejnik et al., 2014
[79] Krishnamurthy und Wills, 2009; Dies liegt u.a. an den Eigenschaften der Datenverarbeitung und Skalierungs- und Netzwerkeffekten.

3.1 Rollen in der Wertschöpfungsstruktur

Die verschiedenen Rollen in der Wertschöpfungskette im deutschen Datenmarkt sind nach Bründl[80] die Advertiser, Publisher, Supply-Side-Plattform, Demand-Side-Plattform, Datensammler und Data-Management-Plattform (vgl. Abbildung 4).

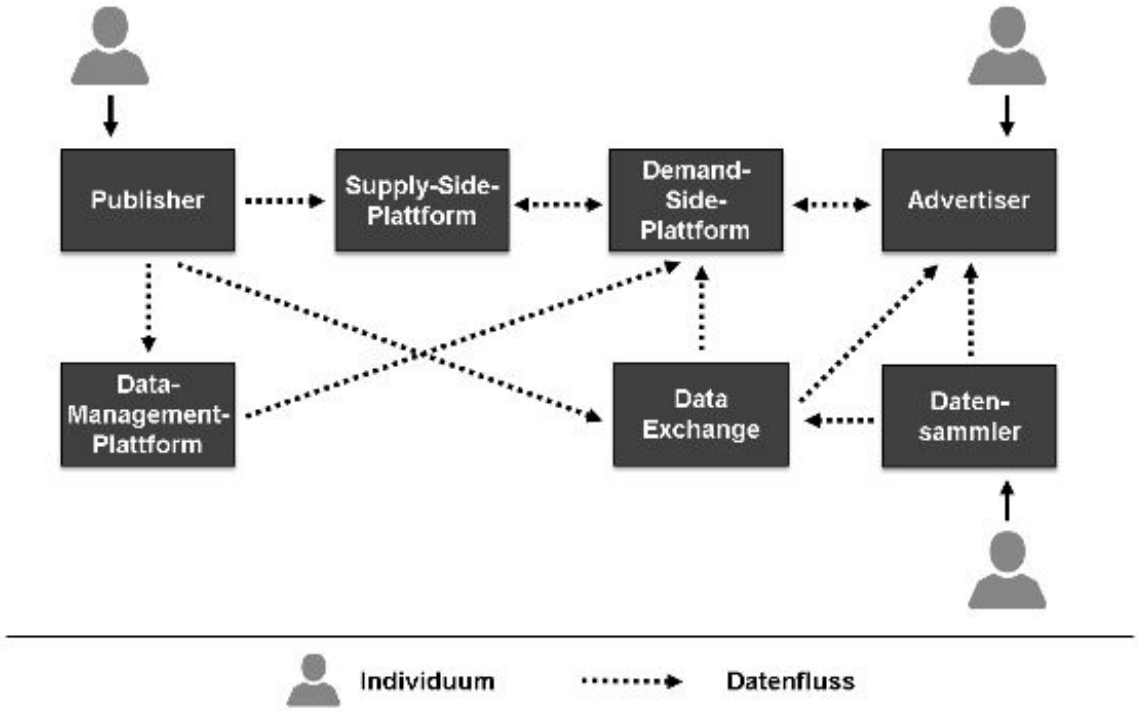

Abbildung 4: Rollen in der Wertschöpfungsstruktur[81]

Die VerbraucherInnen können lediglich mit den Publishern, Advertisern und Datensammlern in Kontakt treten. Eine aktive Rolle der VerbraucherInnen ist im Prozess nicht vorgesehen, Daten fließen von VerbraucherInnen an die Unternehmen, die sie ohne weitere Konsultation der VerbraucherInnen weiterverwenden.
Ganz im Gegenzug dazu stehen VerbraucherInnen im Zentrum, wenn es um die Vermarktung ihrer persönlichen Daten durch sie selbst geht (vgl. Kapitel 3.5).

[80] Bründl et. al., 2015
[81] ebd.

3.2 Anforderungen an den Datenmarkt

Um den Handel mit persönlichen Daten für VerbraucherInnen zu ermöglichen, bedarf es rudimentärer Anforderungen an den Datenmarkt bzw. die Handelsplattform.[82]
VerbraucherInnen sollte auf dem Datenmarkt bzw. der Handelsplattform in der Lage sein,

- angeben zu können, welches Unternehmen Zugriff auf die Daten haben kann, und auch eine Begrenzung bei der Drittverwertung ihrer Daten zu setzen
- die Lebensdauer ihrer Daten zu bestimmen bzw. die Löschung der Daten zu beantragen
- Unternehmen anzufragen, welche Daten gesammelt wurden und zu überprüfen, ob die gesammelten Daten noch korrekt bzw. relevant sind
- nachzuvollziehen, woher ihre Daten stammen und wohin sie verbreitet wurden

Diese Anforderungen sind, wie wir zeigen werden, noch nicht genügend für den Handel der VerbraucherInnen ihrer persönlichen Daten gegen Entgelt am Markt erfüllt.

Aus Sicht der Unternehmen sollte ein Datenmarkt folgende rudimentäre Eigenschaften haben:
Er sollte erstens eine technische Lösung bieten, die es für die Unternehmen einfach macht, Vorschriften wie die Recht auf Vergessen-Werden zu beachten. Zweitens sollte er Transparenz über den Ursprung der Daten für den Fall von Streitigkeiten über die Richtigkeit der persönlichen Daten bieten. Drittens sollte er akkurate, relevante und aktuelle Daten bereitstellen. Viertens sollte er die Möglichkeit bieten, Daten mit anderen Unternehmen zu handeln, dabei aber die Datenschutzbestimmungen einzuhalten. Fünftens sollte er eine Kombination von Kundendaten aus verschiedenen Quellen ermöglichen (basierend auf einem Kunden-Unique Identifier).
Die Mehrheit dieser Anforderungen ist bereits umgesetzt, etwa beim Handel zwischen Unternehmen oder beim Handel gegen Services.

[82] Gjermundrød, 2015

3.3 Handel mit persönlichen Daten

Selbst bei Vorliegen eines funktionierenden Datenmarkts, stellt der Handel mit persönlichen Daten einige Herausforderungen für VerbraucherInnen dar. Er wird vielfach als Lösungsansatz propagiert, um VerbraucherInnen am Wert ihrer persönlichen Daten verstärkt teilhaben zu lassen. Ob dies erfolgversprechend ist, ist derzeit nicht abzusehen. Hilfreich ist dieser Ansatz jedoch als eine Art Lerninstrument, um VerbraucherInnen auf den Wert der Daten aufmerksam zu machen.

Dabei stellen sich für VerbraucherInnen beim Handel mit persönlichen Daten hauptsächlich fünf Hindernisse: Erstens ist es für sie nur schwer möglich, einen angemessen, fairen Preises der Daten zu schätzen. Bei den aktuellen Verwertungs-Modellen wird der Preis mutmaßlich zu gering eingeschätzt.[83] Zweitens stellt sich die Frage der Wiederverwertbarkeit der Daten und damit die Frage, wem die Daten gehören. Dazu kommt drittens das Problem, dass die Daten erst mit weiterer Verknüpfung wertvoll werden, die womöglich nicht vorhanden ist.[84] Die VerbraucherInnen haben viertens nicht immer die technischen Möglichkeiten oder auch Optionen und Berechtigungen, ihre persönlichen Daten aus den jeweils verwendeten Diensten und Services einfach herunterzuladen. Selbst wenn dies möglich ist, bedarf es meistens trotzdem noch fortgeschrittener EDV-Kenntnisse, um die Daten mit anderen Daten zu verknüpfen oder aufzubereiten. Die Datenportabilität ist derzeit meist gering. Fünftens stehen die VerbraucherInnen damit auch mit den herkömmlichen DatenanbieterInnen teilweise in direkter Konkurrenz. Dieser Wettbewerb dürfte für VerbraucherInnen ohne regulatorische Unterstützung äußerst schwierig sein.
In den in Kapitel zwei angeführten Beispielen des Datenhandels haben die VerbraucherInnen zudem meist nur einen Handelspartner (1:1-Beziehung). Für eine bestmögliche Marktteilnahme müsste es auf Nachfrageseite mehrere Akteure geben (1:n-Beziehung).

[83] Acquisiti et.al., 2015
[84] ebd.

3.4 Aktuelle Möglichkeiten des Datenhandels

Auch aufgrund der hohen Hürden ist der Zugang zum Markt für den aktiven Handel mit persönlichen Daten für einzelne VerbraucherInnen bisher noch kaum eröffnet. Dagegen ist der Markt für den Handel von persönlichen Daten durch Firmen bereits ein Milliardengeschäft.[85] Da die VerbraucherInnen kaum direkten Einfluss auf den Datenhandel zwischen Unternehmen haben, wird dieser hier nicht näher beschrieben. Marktakteure und konkrete Beispiele für diesen Markt in Deutschland werden in Anlage III beschrieben.

3.4.1 Datenhandel gegen Services

Schon jetzt handeln VerbraucherInnen implizit mit ihren Daten. Bei etlichen bekannten Plattformen wie Facebook und Google werden Daten gegen Services getauscht. Auf der einen Seite bieten die Unternehmen Dienstleistungen und Produkte gratis online an, auf der anderen Seite sammeln sie Daten von den BenutzerInnen der Angebote, die sie dann wiederum Online-Werbern verkaufen können.

Der Gegenwert für die erbrachtenen Leistung lässt sich dann approximieren, wenn ein Vergleich von Gratis-Dienstleistungen mit ähnlichen, aber zahlungspflichtigen Services möglich ist. Während beispielsweise der E-Maildienst von Google gratis ist, fallen bei Anbietern, die Wert auf die Privatsphäre der KundInnen legen, ca. 12 bis 50 Euro pro Jahr an.[86] [87] [88] [89]
Aber auch wenn es nur einen Monopolisten in einem Marktsegment gibt, beispielsweise Facebook, lässt sich aus seinen erzielten Einnahmen der Wert der vermarkteten Daten ableiten. In diesem Segment haben Angebote mit größerem Anspruch an Datenschutz wie diaspora, app.net und Lifedash keinen Durchbruch am Markt erzielen können. Dadurch stehen VerbraucherInnen meist in einer direkten Abhängigkeit zu dem Unternehmen, welches die persönlichen Daten verarbeitet und verwertet.

Auch indirekte monetäre Vergütungen wie Rabatte[90] zählen zu dieser Form des Datenhandels. Einige Online-Plattformen versprechen im Gegenzug zur Freigabe persönlicher Daten, mithilfe von Rabatten bei verschiedenen Services bis zu 300 Euro im Jahr direkt zu sparen.[91] [92] Ein weiteres Beispiel ist der Preisnachlass von 348 US-Dollar im Jahr für komplettes Tracking des Highspeed-Internetverkehrs, den der Internetanbieter AT&T seinen KundInnen gewährt. Das Unternehmen argumentiert, sein Modell und der Preisnachlass mache wirtschaftlich Sinn und sei durch erhöhte Werbekosten gedeckt.[93]

[85] vgl. https://www.yodlee.com/blog/datacoup-aggregates-unlocks-value-data/
[86] vgl. https://www.fastmail.com/help/ourservice/pricing.html
[87] vgl. https://posteo.de/en
[88] vgl. https://www.pobox.com/pricing
[89] Speicherplatz und sonstige Services approximiert
[90] Eine ausführliche Analyse des Sektors liefert Christl, 2014
[91] vgl. https://ctrlio.com/how-it-works/
[92] Dwoskin, 2015
[93] Luckerson, 2015

Um weiteren Handel zu ermöglichen, könnte es für VerbraucherInnen und auch Unternehmen interessant sein, ihre Daten an Dritte weiterleiten zu können. Die „MiData”-Initiative will diese Möglichkeiten stärken.

MiData UK
In Großbritannien arbeitet die Regierung seit 2011 gemeinsam mit 26 verschiedenen Organisationen gemeinsam an der „Midata“-Initiative.[94] Diese macht es Privatpersonen möglich, anderen Personen und Organisationen eine Kopie ihrer gesammelten Daten in einer standardisierten Form zur Verfügung zu stellen.[95] Durch diese Datenportabilität sollen dem Verbraucher mehr Möglichkeiten offenstehen, einfacher zu anderen Anbietern zu wechseln, die zu ihrem Anforderungsprofil besser passen, etwa beim Wechsel eines Kontos oder Stromanbieters.

3.4.2 Datenhandel als Datenspende für gesellschaftlichen Mehrwert

Zwar entsteht für die freiwillige unentgeltliche Bereitstellung von persönlichen Daten kein klassischer Markt. Aus Sicht der VerbraucherInnen ist die „Spende” zum Beispiel von Bewegungs- oder Gesundheitsdaten für die Forschung jedoch sehr interessant. Der Gegenwert der Daten ist in diesem Zusammenhang nur schwer ökonomisch zu beziffern. Die Kooperative TheGoodData erzielt monatlich durch die Daten von etwa 300 NutzerInnen einen Erlös von 1.100 Euro, der für einen gemeinnützigen Zweck gespendet wird.[96] Man kann davon ausgehen, dass der gesellschaftliche Nutzen etwa von Gesundheitsprofilen zur Erforschung und Heilung von Krankheiten ungleich höher ist.

In Bezug auf Datenspenden werden mit Blick auf die Wertschöpfungskette einige technische und juristische Schwächen deutlich, die eine breite Anwendung derzeit noch unwahrscheinlich machen. Die Datensammlung, -Speicherung, -Analyse und -Verwendung sind derzeit noch nicht auf weitreichende Nutzung ausgelegt. Die Freigabe geschieht noch ohne rechtliche Absicherung oder unter einer freien Lizenz (vgl. Kapitel 2.1) und ist nicht immer nach Verwendungszweck[97] klassifiziert. Die bewusste Freigabe der persönlichen Daten ist förderwürdig - erstens zur Erhöhung des gemeinschaftlichen Wohls und zweitens zur Förderung der Technik und Infrastrukturen, die eine komplexe Datenfreigabe ermöglichen.

[94] vgl. http://www.gocompare.com/money/midata/
[95] vgl. https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment
[96] vgl. https://thegooddata.org/good-data
[97] nach Bründl, 2015

Freigabe von Gesundheitsdaten

Die schweizerische Organisation MIDATA.coop[98] versucht BürgerInnen dabei zu unterstützen, eine gemeinnützige Genossenschaft zu gründen. Ziel ist, es dass ihre Mitglieder ihre persönlichen Daten sicher speichern und verwalten und den Zugriff auf die Daten somit kontrollieren können. Den Schwerpunkt setzt MIDATA dabei zunächst auf die besonders sensiblen und wertvollen Gesundheitsdaten. Darunter fallen derzeit in zwei Pilotprojekten anonymisierte Gesundheitsdaten zu Multipler Sklerose und adipositas-chirurgischen Eingriffen, die gehandelt werden und als Gegenwert bessere Forschungsergebnisse erzielen sollen. Dieses Opt-In-Modell steht damit im Gegensatz zum Projekt care.data der NHS in Großbritannien, das die Gesundheitsdaten britischer PatientInnen zentral und für Firmen zugreifbar sammelt. Wollen PatientInnen daran nicht teilnehmen, müssen sie dies extra angeben (Opt-Out). Auch Googles Software Deepmind hat Zugriff auf 1,6 Millionen PatientInnenakten dieses Projektes.[99] Außerdem soll die NHS der Polizei Zugriff gewähren, sowie die Daten an Aktuariate verkaufen - also Unternehmen, die die Risiken von Versicherungen berechnen. Laut einem Bericht der NHS gibt es schließlich auch Zugriffe von Consultingfirmen sowie Pharmakonzernen, was angesichts der Datenart nicht verwundern sollte.[100]

3.4.3 Datenhandel gegen Entgelt

VerbraucherInnen können dann in einen Wettbewerb mit Unternehmen treten, wenn sie eine höhere Qualität ihrer Daten bieten können und selbst die freigegeben Datenquelle sind. Dies bezieht sich unter anderem auf die Möglichkeit, aktuellere, kontextbezogene und granulare Daten zur Verfügung zu stellen. Außerdem ist die Transparenz über die Herkunft und damit die Signifikanz der Daten größer.

In diesem Abschnitt wird aufgezeigt, welche Preise derzeit mit dem Handel persönlicher Daten durch VerbraucherInnen erzielt werden können. Die Daten sind das Ergebnis einer Marktbeobachtung im Sommer 2015.[101]

[98] vgl. https://midata.coop/
[99] New Scientist, 2016
[100] Lokshin, 2014
[101] Bründl, 2015

Aktuelle Möglichkeiten für VerbraucherInnen, mit ihren persönlichen Daten Geld zu verdienen:

- datacoup.com verspricht ca. 8 US-Dollar pro Monat für das Bereitstellen von Daten. Dazu werden Benutzerkonten wie von der Kreditkartenfirma (Transaktionen werden anonymisiert), Dienste wie Facebook, Twitter, LinkedIn, Foursquare, Google+, YouTube, Tumblr, Meetup, and Instagram verknüpft[102] und Datacoup erstellt damit ein Profil für den/die potenziellen DatenkäuferIn.
- datawallet.io verspricht bis zu 50 US-Dollar für den Verkauf von Datenprofilen, die NutzerInnen mit der datawallet-App verknüpfen. Der Dienst ist noch nicht etabliert.
- people.io bietet im Gegenzug für die Freigabe von Daten Geschenkgutscheine. Es berechnet 70% Beteiligung am Umsatz bei der Vermittlung zu neuen Geschäften Der Dienst citizenme.com bietet Discounts, Coupons und monetäre Entschädigung für die Freigabe von persönlichen Daten. Bis Ende September gab es noch keine konkreten Angaben zur Höhe der Entschädigung.
- digi.me gibt ebenfalls keine konkreten Zahlen preis, ist jedoch mit 300.000 NutzerInnen in 140 Ländern, die ihren Social Network-Steam zu Verfügung stellen, eines der größten Unternehmen in diesem bereich.
- meeco.me verspricht bis zu 50% Umsatzbeteiligung bei Weiterverwendung von Daten. Dieser Wert wird derzeit noch getestet.
- datafairplay.com prognostizierte eine Entschädigung von 30 bis 40 Euro. Aktuell ist keine Teilnahme möglich.
- handshake.uk.com hat einen Erlös von mehreren hundert Euro pro NutzerIn angekündigt[103]. Dies hat sich jedoch nicht rentiert, der Betrieb wurde eingestellt.

Die Dienste sind allerdings noch nicht ausgereift, wie sich auch an der hohen Fluktuation auf dem Markt zeigt. Sie eignen sich noch nicht für die Anwendung durch DurchschnittsverbraucherInnen, bestenfalls für FrühanwenderInnen zum Experimentieren.[104] Dies wurde von beteiligten Unternehmen mehrfach eingestanden.[105] Auch mithilfe der Dienste ist es nicht möglich, konkrete Werte für Datensätze aktuell zu bestimmen.[106]
Aber auch aktuelle Indikatoren für Nutzerzahlen zeigen, dass der Markt bisher noch in einem frühen Anfangsstadium steht. Nach optimistischer Schätzung scheint derzeit maximal ein Erlös von 100 Euro im Jahr für die durchschnittliche VerbraucherIn möglich zu sein.[107]
Diese Handelsangebote sind im Vergleich zu den folgenden dargelegten ambitionierten Modellen in Kapitel 3.5.3 in Puncto Design und technischer Umsetzung unausgereift.

[102] vgl. https://datacoup.com/docs#how-it-works
[103] vgl. http://www.veristorm.com/blog/how-much-your-data-worth
[104] Einschätzung von InterviewpartnerInnen aus dem Unternehmensbereich
[105] Etwa bei verschiedenen Vorträgen auf der MyData2016-Konferenz Anfang September in Finnland
[106] vgl. dazu auch Kapitel 2.2.2
[107] Unter Berücksichtigung mehrerer Szenarien und Personenprofile mit unterschiedlichen Eigenschaften im Rahmen dieser Untersuchung, ohne Berücksichtigung des dafür nötigen Zeitaufwands. Die Kosten pro VerbraucherIn zum Betreiben einer dafür nötigen Infrastruktur betragen ca. 2 Euro pro Monat.

3.5. Modelle für verbraucherzentrierten Datenhandel

Im Gegensatz zu den oben angeführten Beispielen, der aktiven Beteiligung am Handel auf dem Datenmarkt, sind bei den nachfolgenden Modellen (MyData aus Finnland, VRM - Vendor Relationship Management aus USA, HAT Hub of All Things aus UK)[108] die VerbraucherInnen im Zentrum des Handelsgeschehens. Damit verändern sich nicht nur die Handelsbeziehungen und -bedingungen. Es wird auch ein neues Marktsegment geschaffen.[109]

Diese Modelle sind aktuell entweder noch in der Planungsphase, Umsetzungphase oder erst am Anfang des Markteintrittes. Daher ist eine Bewertung bzgl. ihrer Marktreife schwierig. Die Auswirkungen bei einem Marktdurchbruch wären vermutlich vergleichbar mit dem Aufkommen der Sharing (Renting) Economy. Diese Modelle haben gemeinsam, die Abhängigkeit der VerbraucherInnen von einer Schnittstelle zu überbrücken (vgl. Kapitel 3.4.4).[110]

3.5.1 MyData

Das in Finnland entworfene Modell MyData verspricht VerbraucherInnen, ihre persönlichen Daten selbst zu kontrollieren. An der Umsetzung des Ansatzes wird derzeit gearbeitet (vgl. Abbildung 5).

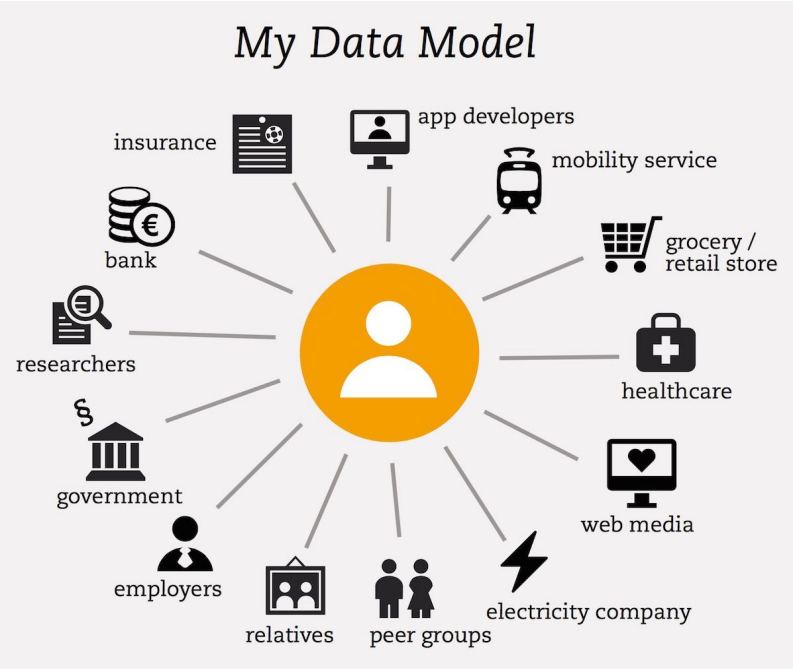

Abbildung 5: MyData-Modell - Verbraucherzentriertheit[111]

[108] Die Konzepte spiegeln lokale kulturelle Präferenzen wider. So erkennt man bei Mydata den nordischen „wohlfahrtsstaatlichen Ansatz" (sharing economy) bzw. den marktbasierten Lösung von VRM und HAT (renting economy).
[109] Bezeichnungen für das Segment sind u.a.personal cloud, API-of-Me, internet of me, me2b, personal data vault, PIMs Personal Information Management (vgl. http://www.nesta.org.uk/publications/personal-information-management-services-analysis-emerging-market)
[110] In der Endstufe beim Ausbau kommt es zu einer peer2peer Version; Die Analogie sind ursprüngliche Internetprotokolle: Dies bedeutet auch die Aufhebung der Abhängigkeit.
[111] vgl. https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/

Im Vordergrund des MyData-Modells steht die Beseitigung einzelner „Datensilos" bei Unternehmen und die Zusammenführung in ein von VerbraucherInnen selbst kontrolliertes System. MyData formuliert folgende Rechte für die VerbraucherInnen:

- Das Recht zu wissen, welche persönlichen Informationen vorliegen
- den tatsächlichen Inhalt der persönlichen Daten zu sehen
- falsche Daten korrigieren zu können
- zu prüfen, wer Zugriffe und auf die personenbezogene Daten hat und warum
- persönliche Daten zu erhalten und sie frei zu verwenden
- persönliche Informationen an Dritte zu teilen oder verkaufen
- zu entfernen oder persönliche Daten zu löschen.

Die technischen Voraussetzungen für MyData sind teilweise bereits vorhanden, darunter Personal Information Management.[112] Die Anwendungen, deren Marktreife und die Marktnachfrage werden sich aber erst noch zeigen müssen.

3.5.2 Vendor Relationship Management (VRM)

Ein ähnlicher Ansatz wie MyData ist das Modell Vendor Relationship Managements (VRM bzw. Lieferantenbeziehungsmanagement).[113] Es soll den VerbraucherInnen die Möglichkeit bieten, ihre Daten aus Beziehungen zu Unternehmen und anderen Organisationen ganzheitlich und auf Basis ihrer eigenen Bedingungen zur Verwaltung und Gestaltung zu übergeben. Das Modell von VRM basiert auf der Überzeugung, dass freie Kunden, die sich aktiv ihre Geschäftspartner aussuchen können, wertvoller sind als Kunden ohne diese Auswahlmöglichkeit.[114] VerbraucherInnen sollen von passiven Marktteilnehmern zu aktiven Marktteilnehmern des Beziehungsmanagements werden. VRM ermöglicht VerbraucherInnen die Sammlung der persönliche Daten und das selektive Teilen jener Daten, die Kontrolle über die Verwendung ihrer Daten durch Dritte. Außerdem können VerbraucherInnen die eigenen Geschäftsbedingungen zur Verwendung der Daten gestalten. Durch VRM wird Hilfestellung bei der Artikulation von Nachfragen (Intent-casting) und Rückmeldungen (Produktverbesserungen) in einem offenen Marktumfeld geleistet. Das VRM-Modell stützt sich auf Applikationen auf Basis offener Standards, offener APIs und offener Quellcodes. VRM ist ein vielversprechendes komplexes Forschungsfeld,[115] das bisher aber noch nicht vollständig umgesetzt wurde. Die technischen Voraussetzungen (PDS, PDX personal data storage/exchange) sind teilweise vorhanden[116], zentrale Komponenten aber noch in der Entwicklung.[117]

[112] CTRL-Shift, 2014
[113] vgl. http://projectvrm.org
[114] VRM-Konzept, Interview Doc Searls
[115] vgl. http://cyber.law.harvard.edu/projectvrm/VRM_Development_Work
[116] vgl. Umsetzung auf https://mydex.org/
[117] XDI, JLink, UMA als Protokolle bzw. darauf basierende Applikationen zum dezentralen Datenaustausch in der Umsetzungsphase

3.5.3 Hub of All Things (HAT)

Mit dem britischen Konzept und Forschungsprojekt „Hub of All Things" (HAT) sollen VerbraucherInnen die Möglichkeit haben, an einem zentralen Ort alle persönlichen Daten lokal oder als Container in der Cloud zu speichern. Dazu gibt es einen Browser (Rumpel) für die eigenen Daten und einen Marktplatz zum Verkauf der Daten. Jedoch fehlen noch die Marktteilnehmer auf der Nachfrageseite. Das Projekt ist aktuell noch in der Beta-Phase und ist aus technischer Sicht noch im Anfangsstadium. Allerdings sammelte es kürzlich per Crowdfunding 50.000 Euro, was für ein großes Interesse an der Idee spricht.[118]

Der HAT soll für die VerbraucherInnen alle Schritte der Daten-Wertschöpfungskette von der Datensammlung über die -Speicherung und -Analyse bis hin zur -Verwendung ermöglichen. Im Vergleich zu MyData und VRM zeigt sich beim HAT ein marktfokussierter Ansatz.[119] Zentral ist außerdem die Idee, dass nicht mehr wie bei traditionellen Datenmärkten VerbraucherInnen pro Transaktion handeln, sondern in eine längerfristige Beziehung mit einem Unternehmen treten. Dies geht, wie auch bei VRM, über den herkömmlichen Datenmarkt hinaus.[120]

Auch aktuelle Entwicklungen im Blockchain-Sektor könnten interessante Perspektiven für den Markt persönlicher Daten bereithalten.[121] Technologien in diesem Umfeld sind technisch dafür geeignet, besonders sensible Daten davor zu schützen, in die Hände von Unbefugten zu gelangen.[122] Die technische Grundlagen der Technologien entwickeln sich rasant, es fehlt jedoch noch an konkreten Anwendungen für VerbraucherInnen.

3.6 Zusammenfassung

Wir wir gezeigt haben, sind die verschiedenen Marktsegmente des Datenmarktes sehr heterogen. Es gibt unterschiedliche Möglichkeiten der Datenvermarktung für VerbraucherInnen. Der Handel gegen Services ist bereits stark verbreitet, während sich Datenspenden und der Datenhandel gegen Entgelt noch im Anfangsstadium befinden. Die erzielbaren Erlöse in diesen Segmenten sind dementsprechend niedrig. Den dazugehörigen Plattformen fehlen technisch notwendige Grundlagen, einfache Benutzerführung und konkrete Möglichkeiten, Erlöse zu erzielen. Nichtsdestotrotz versprechen verschiedene verbraucherzentrierte Modelle eine Stärkung der Marktsegmente in der Zukunft.

[118] vgl. https://www.indiegogo.com/projects/hat-claim-your-data-organise-visualise-control-technology#/
[119] Ng, 2016
[120] Die geschätzten Kosten pro Beziehung von VerbraucherIn zu Unternehmen belaufen sich auf durchschnittlich 3-6 Euro bei geschätzten ca. 60 Beziehungen pro VerbraucherIn. Zur Veranschaulichung des Potentials dienen die Kosten im Finanzbereich für die Handhabung einer Beziehung von über 50 Euro.
[121] Neben dem aktuellen Hype liegt es u.a. aufgrund der Dezentralisierung nahe, dass sich etliche Projekte für die Anwendung in nächster Zeit demnächst anbieten könnten, darunter permission-based blockchain, Consensus für Zustimmung, Provenance für die Nachvollziehbarkeit, DAO für gemeinnütziches Data-sharing. Wie für alle Themen empfehlen sich hier die Präsentationen auf http://mydata2016.org.
[122] Bitcoin ist seit Jahren am Markt sicherheitstechnisch geprüft (vgl. Zyskind et al., 2014)

4. Diskussion und Ausblick

Für die Diskussion und den langfristigen Ausblick kombinieren wir die in den vorigen Kapiteln dargestellten Aspekte mit den Ergebnissen der Experteninterviews und weiteren Recherchen im Rahmen dieser Arbeit. Wir betrachten die zuvor im dritten Kapitel vorgestellten Marktsegmente in Bezug auf die Frage, ob im jeweiligen Marktsegment der Handel aus Sicht der VerbraucherInnen der bessere Datenschutz ist. Wir zeigen die Aussichten für die Entwicklung dieses Marktes auf, die vor allem durch EU-Regulierung für den Datenschutz geprägt sein werden. Anschließend geben wir einen Ausblick auf Preisentwicklungen von persönlichen Daten und schließen mit Handlungsempfehlungen zur Stärkung der Position der VerbraucherInnen am Datenmarkt.

4.1 Analyse: Vergleich von Marktsegmenten

Im dritten Kapitel haben wir anhand der Wertschöpfungskette drei Marktsegmente des Datenhandels untersucht: Datenhandel gegen Services, Datenspenden und Datenhandel gegen Entgelt.

Im Allgemeinen sehen die im Rahmen dieser Studie interviewten Personen die Möglichkeit des Handels mit persönlichen Daten positiv. Jedoch wurde auch deutlich, dass der Handel nicht den Datenschutz an sich ersetzen kann. Auch die Mehrheit der InterviewpartnerInnen aus Unternehmen hält einen rein marktbasierten Ansatz für Datenschutz für „optimistisch". Diese würde nur dann Sinn machen, wenn die VerbraucherInnen gleichberechtigte MarktteilnehmerInnen sind. Gleichberechtigt können sie allerdings nur dann sein, wenn die VerbraucherInnen in allen Rollen der Wertschöpfungskette eingebunden sind. Findet der Datenhandel zwischen Unternehmen untereinander statt, ist dies nicht der Fall. Datenhandel kann und soll die Wichtigkeit des Datenschutzes hervorheben und stärken, jedoch kann er nicht Datenschutz ersetzen. Der effektivste Datenschutz ist zunächst die Datensparsamkeit von VerbraucherInnen, also die Preisgabe ausschließlich der notwendigsten persönliche Daten.

Am aktuell größten Marktsegment der in dieser Studie vorgestellten Bereiche, dem Datenhandel von Daten gegen Services, nimmt ein großer Teil der NutzerInnen durch die Akzeptanz von werbefinanzierten Dienste bereits teil. Diese Situation entstand allerdings nicht auf freiwilliger Basis, sondern vielmehr aus Mangel an Alternativen und fehlendem Bewusstsein für den Wert der Daten.[123] Auch Gewinne durch die Nutzung der Dienste - etwa leichterer Informationszugang und erhöhte Produktivität - spielen dabei eine Rolle. Das Marktsegment des Datenhandels gegen Services ähnelt am meisten den betrachteten Modellen von der OECD und Bründl. Inwiefern dieser Tausch jedoch langfristig ökonomisch sinnvoll für die VerbraucherInnen ist, ist unter den InterviewpartnerInnen umstritten.[124] Der

[123] 40% teilen die Daten wegen mangelnder Alternativen (vgl. Global Consumer Trust Report, 2016)
[124] Die Bewertungen nicht immer quantifizierbar und abhängig von der Einstellung zur eigenen Privatsphäre.

Erfolg hängt auch davon ab, ob aktuelle Preisnachlässe für die VerbraucherInnen (z.B. Preisnachlässe bei Datentausch) langfristig bestehen bleiben.
Für das Marktsegment der „Datenspenden" bedarf es abgestufter Regulierungen von Zugriffsrechten in der granularen Verwertungskette.
Es wird sich noch zeigen, ob sich das Marktsegment zum Datenhandel gegen Entgelt künftig etablieren wird. Dazu sind, wie bereits gezeigt, noch technische Voraussetzungen notwendig, um in einem verbraucherzentrierten Markt mit dem herkömmlichen Markt konkurrieren zu können.

In dieser Studie wurden verschiedene Einschätzungen zu möglichen erzielbaren Preisen bei „Datenhandel gegen Entgelt" aufgelistet. Grundlage hierfür waren andere Studien, die aktuelle Marktsituation sowie die Prognosen der interviewten Personen. Insgesamt zeigt sich, dass die erzielbaren Marktpreise für VerbraucherInnen bisher nur selten den großen Zeitaufwand und die Einbußen von Privatsphäre für VerbraucherInnen rechtfertigen können. Aus rein ökonomischer Sicht ist aktuell der Handel mit persönlichen Daten mit einem Erlös von max. 100 Euro im Jahr noch nicht ergiebig.[125] Theoretisch sind die notwendigen technischen Voraussetzungen und Frameworks für die dazu notwendige Datenverarbeitung vorhanden.[126] Dies gilt auch die für Modelle der Umsatzbeteiligung.[127] Die Preisbewertung der persönlichen Daten ist jedoch ein komplexer Vorgang, der selbst für Unternehmen und Ökonomen noch nicht klar nachvollziehbar ist. Die Verantwortung, diese Preisfestlegung nachzuvollziehen, kann von VerbraucherInnen kaum selbst übernommen werden. Diese Einschätzung wurde in den ExpertInneninterviews bestätigt.
Ein weiterer wichtiger Aspekt ist, dass nicht alle VerbraucherInnen am Verkauf der Daten teilnehmen. Meist gehören diejenigen VerbraucherInnen, die ihre Daten verkaufen wollen, nicht zu der Gruppe der stark nachgefragten MarktteilnehmerInnen. Jene VerbraucherInnen, die nicht am Markt teilnehmen wollen, gilt es zu schützen. Dies kann nicht alleine über Marktmechanismen erfolgen.

Für alle Marktsegmente zeigt das OECD-Modell, dass bei jeder Marktteilnahme die herrschenden Skaleneffekte und Netzwerkeffekte in der gesamten Wertschöpfungskette zu berücksichtigen sind. Dies ist aktuell ein klarer und eklatanter Nachteil für verbraucherzentrierte Wertschöpfung von persönlichen Daten, da diese noch nicht technisch umsetzbar sind.

Wir möchten trotzdem darauf hinweisen, dass etliche der adressierten Probleme durch zukünftige technische Lösungen und einer Verschiebung hin zu einer verbraucherzentrierten System entschärft oder sogar gelöst werden könnten.[128] Die Vision und Vorstellung einer globalen Micropayment-Infrastruktur, in der im Rahmen einer Data Ownership Society die VerbraucherInnen für Ihre digitalen Werte bzw. Daten anteilsmäßig bezahlt werden, ist jedoch aktuell noch nicht greifbar.[129]

---

[125] Der in dieser Studie durchgeführte Feldversuch weist aktuell für den Handel im monetären Sektor noch ein negatives Konto auf, bedingt durch Investitionen in einen HAT. Die im Rahmen dieser Studie getauschten persönlichen Daten für die Verwendung diverser Dienste lassen sich nicht genau ermitteln, können jedoch durch den Zeitgewinn das Konto ins Positive wenden.
[126] Spiekermann, 2015
[127] Li, 2012
[128] Spiekermann, 2015
[129] vgl. http://declineofscarcity.com/?p=2952

4.2 EU-Datenschutz-Grundverordnung: Schaffung eines neuen Markts

Nur mit einer starken Regulierung des Datenschutzes ist es möglich, dass persönliche Daten ein wertvolles Gut in einem Verkäufermarkt werden können. Aktuell ist dieser Markt aber noch unterentwickelt. Mit der neuen EU-Datenschutz-Grundverordnung, die 2018 in Kraft treten wird, könnte sich dies durch ein strengeres Opt-in und eine höhere Datenportabilität ändern.[130] Verarbeiten Unternehmen persönliche Daten, müssen sie nach Inkrafttreten dieser Verordnung dazu eine ausdrückliche Zustimmung von ihren Kunden einholen. Diese können dann jederzeit Auskunft über die gespeicherten Daten einfordern oder ihre Einwilligung zurückrufen. Außerdem wird damit der europäische Datenmarkt erstmals EU-weit reglementiert, was Anreize in diesem Sektor für neue Geschäftstätigkeiten schafft. Einige Interviewpartner meinen, dass viele Regelungen der neuen Datenschutzverordnung so allgemein formuliert sind, dass auf den ersten Blick nicht klar ist, wie sie in der Praxis umgesetzt werden sollen.[131] Eventuell kommt es nach Inkrafttreten der Grundverordnung zunächst zu einer gewissen Rechtsunsicherheit durch mögliche Öffnungsklauseln. Im schlechtesten Fall erfolgt ein Rückfall zu Einzelregelungen für jedes der aktuell noch 28 Länder der EU.

Es ist derzeit auch noch unklar, wann Unternehmen ein „berechtigtes wirtschaftliches Interesse" an der Speicherung von Daten haben. Beispielsweise ist nicht geklärt, ob Buchhandlung nach der Lieferung eines Buches weiterhin Daten der BestellerIn speichern dürfen. Mit der Verordnung wird aber zumindest das sogenannte „Recht auf Vergessen" für alle Unternehmen verbindlich. Sie müssen zukünftig persönliche Daten auf Wunsch der Betroffenen löschen.

Eine zentrale Frage bleibt aber vorerst offen: Wem gehören persönliche Daten? Wer speichert wie lange zum Beispiel die Daten von vernetzten Autos? Die Antwort auf diese Fragen wird wahrscheinlich in verschiedenen Kontexten immer wieder neu verhandelt werden, etwa bei zukünftigen Freihandelsabkommen.[132] Diese Situation hat auch Auswirkungen auf kommende Generationen - durch die fehlende Regulierung von jetzt anfallenden Daten scheint eine vollkommene Kontrolle derzeit aussichtslos zu sein.

Zum Datenschutzstandard der Europäischen Verordnung sei angemerkt, dass dieser Vorbildcharakter für den Rest der Welt haben kann und damit den Datenschutzstandard weltweit heben könnte. Für deutsche bzw. europäische Unternehmen könnte die Verordnung einen Wettbewerbsvorteil in aufstrebenden Ökonomien bieten. Zusätzlich wäre auch aus Sicht der VerbraucherInnen eine freiwillige Selbstverpflichtung zu höheren Datenschutzstandards durch die teilnehmenden Unternehmen begrüßenswert, wie dies etwa

[130] ICO, 2016
[131] vgl. https://www.bitkom.org/Presse/Presseinformation/Datenschutzverordnung-sollte-einheitlich-angewendet-werden.html
[132] Leonard, 2016

bei E-Mail-Anbietern in Bezug auf mehr Sicherheit bei der konventionellen E-Mail-Kommunikation zu beobachten ist.[133]

4.3 Prognose zur Entwicklung des Wertes von persönlichen Daten

Die EU-Datenschutzgrundverordnung wird zur Erweiterung des Marktes für persönliche Daten beitragen. Ergänzend wird die Menge an persönlichen Daten voraussichtlich immer weiter ansteigen, da beispielsweise durch technologische Trends wie IoT (Internet der Dinge) und Big Data verstärkt Daten erhoben werden. Diese Veränderungen werden zu einer Ausweitung des Angebots um die persönlichen Daten führen. Daher ist längerfristig eine Preissenkung für solche Daten wahrscheinlich, die nicht mit Kontextdaten angereichert werden oder spezifische, selten erhobene Informationen beinhalten.[134]
Im Gegensatz hierzu ist es möglich, dass die Preise für Daten von Individuen ansteigen, sofern diese aufgrund erhöhter Datenqualität für Unternehmen interessant sind oder sie ihre Daten bisher außergewöhnlich gut geschützt haben.[135]

Weitere Trends in diesem Zusammenhang sind die Steigerung des Nutzens einzelner Datensätze durch bessere Analyse- und Verknüpfungsmöglichkeiten (u.a. Machine-Learning, AI). Beispielsweise wird Approximierung durch verknüpfte Familienmitglieder und soziale Kontakte zunehmen, etwa mithilfe von sozialen Netzwerken und Genetik-Daten.
Big Data macht aus „präzisen Zahlen Wahrscheinlichkeiten" und löst folgende drei große Umwälzungen aus, wie sie Mayer-Schönberger sieht[136] :

- Erstens die nicht nur auf kleine Stichproben beschränkte Analyse sehr großer Datenmengen bezogen auf ein konkretes Problem oder eine bestimmte Fragestellung.
- Zweitens die Akzeptanz einer gewissen Unschärfe im Gegensatz zu Exaktheit.
- Drittens der „wachsende Respekt" für Korrelationen anstatt der Suche nach Kausalitäten.

Damit wären nicht immer persönliche Daten eines/r Verbrauchers/in für seine/ihre Bewertung notwendig.

Einzelne TrendforscherInnen sagen einen Wandel des werbefinanzierten Internets zu einem versicherungsfinanzierten Internet voraus.[137] Durch eine Massentauglichkeit von Quantified-Self-Anwendungen und etwa billigeren Gen-Tests wird der Markt der persönlichen Daten deutlich wachsen. Für die IT-Branche typisch könnte es dadurch zu fallenden Grenzkosten kommen.
Sollten sich die VerbraucherInnen vermehrt um den Schutz ihrer persönlichen Daten sorgen bzw. deren Weitergabe sparsamer handhaben, würde dies laut verschiedenen Bewertungen in den ExpertInneninterviews wahrscheinlich preissteigernd auswirken.

[133] vgl. http://www.postbranche.de/2015/11/18/verschluesselte-e-mails-fuer-jedermann/
[134] Bründl, 2015
[135] Dies ist die Annahme der Modelle von VRM, Mydata und HAT bzw. Prognosen und Determinanten-Ansatz
[136] Mayer-Schönberger et al., 2013
[137] Myslewski, 2014

Somit gibt es bei der Prognose über den zukünftigen Wert der persönlichen Daten auch keine klare Aussage. Jedoch liegt die Vermutung nahe, dass der Wert steigen könnte und dieser Grundlagen für neue Geschäftsmodelle sein könnte. Diese Einschätzung spiegelte sich auch in den Interviews wider.
Viel wird davon abhängen, wie der gesellschaftliche Umgang mit der Privatsphäre sich verändert. Es ist schwierig, diese Entwicklungen abzuschätzen, wobei es vorsichtige Prognosen für das Jahr 2025 gibt.[138] Ein nicht zu unterschätzender Faktor werden dabei die regulativen Maßnahmen sein, vor allem die EU-Datenschutz-Grundverordnung, die zu signifikanten Veränderungen und auch neuen Möglichkeiten für die VerbraucherInnen in den Datenmärkten führen wird.

[138] Rainie/Anderson, 2014

4.4 Empfehlungen

Wir empfehlen zur Sicherung des Wertes persönlicher Daten für VerbraucherInnen:

Verbraucherzentriertheit stärken
VerbraucherInnen sollten die Entscheidungshoheit über den Umgang mit ihren persönlichen Daten haben. Dazu braucht es einen starken Datenschutz. Falls sie den Handel selbst betreiben wollen, sollten sie die Möglichkeit haben, eine aktive Rolle im Zentrum des Handels einzunehmen. Dafür ist Aufklärung nötig: zum einen über die Bedeutung von Datenaufkommen, zum anderen über mögliche Verschiebungen des Marktzentrums hin zu den VerbraucherInnen.

Um dies zu erreichen, müssen Unternehmen

Transparenz schaffen und gewährleisten bei der Datenverarbeitung **-**
z.B. mit einem Ampelsystem zur schnellen Übersicht über die Verwendung von Daten. [139] Transparenz ist aber auch bezüglich der eingesetzten statistischen Algorithmen erforderlich. Dazu gehört auch die Forderung nach der Offenlegung von bisher intransparenten Mechanismen wie der Schufa und arvato infoscore.

Für VerbraucherInnen muss

MyData als Standard gesetzt sein. Die Sicherstellung und Förderung von Portabilität und Datenaustausch ist für VerbraucherInnen besonders wichtig. Persönliche Daten sollten für VerbraucherInnen von jedem verwendeten Service einfach erhältlich sein, auch die ko-produzierten Daten,

und im Idealfall dann in so vielen wie möglich

dezentralen Strukturen gesammelt, gespeichert, analysiert und weiterverwendet werden können. Dazu bedarf es der Unterstützung von dezentralen Technologien und Handelsplattformen, die mehr Kontrolle über persönliche Daten einräumen (Forschungs- und Förderebene). Damit können sich verbraucherzentrierte Märkte ergeben.

Ohne monetäre Vergütung, aber mit gesellschaftlichem und wirtschaftlichem Nutzen ließe sich dies am schnellsten umsetzen durch die Errichtung einer

Infrastruktur für Datenspenden von VerbraucherInnen. Mit dem Aufbau und der Förderung einer dezentralen Infrastruktur für freiwillig gespendete persönliche Daten würde die Forschung, Wirtschaft und Gesellschaft in diesem Bereich gestärkt werden. Unter Einbindung der Stakeholder aus Zivilgesellschaft, Verwaltung, Wissenschaft und Wirtschaft könnte ein Bewusstsein für den Wert persönlicher Daten für das Individuum, aber auch für die Gesellschaft gestärkt werden.[140]

Damit kann ein Gegenentwurf zum bisherigen Datenmarkt geschaffen werden, der verbraucherzentriert ist und gleichzeitig Wert auf Datenschutz legt.

[139] vgl. Anlage I
[140] Anwendungen wären z.B. Preisvergleichsportale oder Dienstleistungsmonitoring zu Verspätungen

5. Fazit

In dieser Studie haben wir gezeigt, dass persönliche Daten einen Wert haben, der derzeit nur schwer zu konkretisieren ist. Fest steht aber: Der Markt um den Handel persönlicher Daten wächst rasant. Wir haben verschiedene Ansätze untersucht, um den Wert der Daten aus Sicht der VerbraucherInnen und Unternehmen zu schätzen. Die Spannweite der Bewertungen ist dabei enorm - von Erlösen im einstelligen Eurobereich bis hin zu mehreren Hundert Euro jährlich. Nach Markteinschätzungen kann der Wert persönlicher Daten in naher Zukunft für den europäischen Markt bis zu 440 Euro pro VerbraucherIn pro Jahr betragen.

Anhand verschiedener Modelle haben wir aufgezeigt, welche aktuellen und zukünftigen Möglichkeiten es für VerbraucherInnen gibt, am Wert der Daten teilzuhaben und sich aktiv am Markt zu beteiligen. Dazu haben wir die Rollen der VerbraucherInnen in drei Marktsegmenten untersucht: Beim größten Marktsegment, dem Handel gegen Services, nimmt der/die VerbraucherIn eine passive Rolle ein und erhält für ihren Handel Services. Dieses Marktsegment wird weiterhin bestehen. Es gilt, verstärkt auf damit zusammenhängende Datenschutzrisiken hinzuweisen und den Datenschutz dahingehend zu adaptieren.
Das Marktsegment für Datenspenden entsteht derzeit. Es hat einen potentiell hohen gesellschaftlichen Nutzen, zeigt aber noch vor allem die technischen Limitationen der dazugehörigen Plattformen auf. Aufgrund seiner Verankerung in der Zivilgesellschaft und der technischen Experimentierfreudigkeit der Community wird dieser Bereich aber relativ schnell wachsen. Eine Vielzahl innovativer Projekte ist zu erwarten.
Das dritte Marktsegment, der Handel gegen Entgelt, hat einige Herausforderungen zu bewältigen. Erstens müssen noch technische Hindernisse zur Herstellung eines Marktes überwunden werden. Zweitens ist unsicher, ob der von VerbraucherInnen zu erwirtschaftende Preis ausreichen wird, damit es zu einem funktionierenden Markt kommt. Drittens stellt sich die Frage, ob dieses Marktsegment aufgrund von Netzwerk- und Skaleneffekten im Vergleich zum Datenhandel zwischen Unternehmen konkurrenzfähig ist. Aktuell liegen optimistische Schätzungen für einen künftigen monetären Erlös bei maximal 100 Euro. Unter diesen Umständen würde sich für VerbraucherInnen kaum der Aufwand lohnen, um aktiv am Markt teilzunehmen. Als Konsequenz könnten VerbraucherInnen auch hier in eine passive Rolle geraten. Angesichts steigender Datenmengen könnte es aber ein entscheidender Wettbewerbsvorteil für VerbraucherInnen sein, in einer aktiven Rolle der Wertschöpfungskette als Determinanten des Wertes und direkt bereitstellende Datenquelle eine bessere Datenqualität zu ermöglichen. Solange die Rolle der VerbraucherInnen allerdings nicht geklärt ist, kann auch nicht beantwortet werden, ob über Datenhandel ein besserer Datenschutz hergestellt werden kann.

Dies könnte in der Zukunft dann der Fall sein, wenn die VerbraucherInnen in das Zentrum des Handelsgeschehens rücken, wie wir anhand der drei Modelle MyData, VRM und HAT dargelegt haben. Dafür ist es notwendig, dass VerbraucherInnen den Zugriff auf ihre Daten haben. Die kommende europäische Datenschutz-Grundverordnung ist ein Schritt auf dem Weg zur Herstellung dieses Ziels.

'You have to fight for your privacy or you will lose it'.
Eric Schmidt[141]

Neben den in dieser Studie untersuchten ökonomischen Fragen und zugrundeliegenden technischen Voraussetzungen ist der Datenschutz vor allem eine rechtliche und ethische Herausforderung. Dieser Aspekt konnte in dieser Studie nicht behandelt werden, sind aber trotzdem essentiell. Der Datenhandel ist eng verknüpft mit Fragen sozialer Ungleichheit und dem unterschiedlichen ökonomischen Druck innerhalb der Bevölkerung, Daten gegen Services bzw. gegen Geld zu handeln. Rechtliche Bedingungen des Handels mit Daten, insbesondere im Zusammenhang mit informationeller Selbstbestimmung, konnten hier ebenfalls nicht erläutert werden.

Einstellungen zum Datenschutz sind innerhalb der Gesellschaft nicht statisch, sondern können sich zügig verändern. Manche Kommentatoren sprechen von „Wellen des Datenschutzes".[142] Es gilt dabei zu berücksichtigen, dass ein schwacher Datenschutz langfristige Auswirkungen auf eine Gesellschaft nach sich zieht, die kaum rückwirkend aufgehoben werden können.

Letztlich ist ein starker Datenschutz auch eine Vertrauensfrage in die ihr zugrundeliegende Technologie, die Datenschutzgesetze und ihre Einhaltung. Kulturell ist Deutschland beim Datenschutz weltweit in einer Vorreiterrolle. Diese Position gilt es zu halten - zumal dies auch ein wirtschaftlicher Standortvorteil für Unternehmen werden könnte.

[141] vgl. http://www.telegraph.co.uk/technology/eric-schmidt/10076175/Eric-Schmidt-interview-You-have-to-fight-for-your-privacy-or-you-will-lose-it.html
[142] Acquisti, 2016

6. Literaturverzeichnis

AD: Abfragedatum

Acquisti et al., 2009: Acquisti, A.; John, L. and Loewenstein, G. | What is Privacy Worth? http://pages.stern.nyu.edu/~bakos/wise/papers/wise2009-6a1_paper.pdf | AD: 15.05.2016

Acquisti et al., 2016: Acquisti, Alessandro; Taylor, Curtis R.; Wagman, Liad | The Economics of Privacy
http://people.duke.edu/~crtaylor/Privacy_Survey.pdf | AD: 18.05.2016

Bambauer et al., 2013: Bambauer, Jane R.; Muralidhar, Krish and Sarathy, Rathindra | Fool's Gold: an Illustrated Critique of Differential Privacy | September 15, 2013 | In: Vanderbilt Journal of Entertainment & Technology Law 16 | Arizona Legal Studies Discussion Paper No. 13-47 Available at SSRN: http://ssrn.com/abstract=2326746 | AD: 26.06.2016

BCG, 2012: The Boston Consulting Group | The Value of Our Digital Identity - Liberty Global Policy Series
http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf | AD: 26.06.2016

Benndorf und Normann, 2014: Benndorf, Volker und Normann, Hans-Theo | The willingness to sell personal data
https://www.uni-duesseldorf.de/home/fileadmin/redaktion/DUP/143_Benndorf_Normann.pdf | AD: 19.08.2016

Brandeisky, 2016: Brandeisky, Kara | The Risks of Selling Your Personal Data | In: Time, 2016 | 26. Juli 2016 | | AD: 27.07.2016
http://time.com/money/4397280/sell-data-better-insurance-rate/

Breithut, 2016: Breithut, Jörg | Wie Fitness-Apps Radwege besser machen sollen | In: Spiegel Online | 1. Oktober 2016
http://www.spiegel.de/netzwelt/apps/fahrradwege-fitness-apps-sollen-die-stadtplanung-verbessern-a-1113258.html | | AD:01.10.2016

Broad, 2015: Broad, Ellen | Closed, shared, open data: what's in a name?
https://theodi.org/blog/closed-shared-open-data-whats-in-a-name | | AD: 10.09.2016

Bründl, 2015: Bründl, Simon; Matt, Christian und Hess, Thomas | Wertschöpfung in den Datenmärkten
https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/Forschungsbericht-LMU-Wertschoepfung-in-Datenmaerkten_FP_3Sept15.pdf | | AD: 11.07.2016

Buchmann, 2012: Johannes Buchmann (Hrsg.) | Internet Privacy - Eine multidisziplinäre Bestandsaufnahme, acatech Studie

http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Projektberichte/acatech_STUDIE_Internet_Privacy_WEB.pdf | AD: 16.06.2016

Bughin und Manyika, 2014: Bughin, Jacques and Manyika, James | The mobile Internet's consumer dividend | McKinsey Quarterly, February 2014
http://www.mckinsey.com/industries/high-tech/our-insights/the-mobile-internets-consumer-dividend | AD: 26.08.2016

Christl, 2014: Christl, Wolfie | Kommerzielle digitale Überwachung im Alltag. Studie im Auftrag der Bundesarbeitskammer Wien | November 2014
http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf | AD: 30.09.2016

CTRL-Shift, 2014: CTRL-Shift | Personal Information Management Services: An analysis of an emerging market
https://www.nesta.org.uk/sites/default/files/personal_information_management_services.pdf AD: 15.05.2016

Dienlin und Trepte, 2014: Dienlin, Tobias and Trepte, Sabine | Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors | In: European Journal of Social Psychology 45 (3)

Digital Strategy Consulting, 2014: How much are you worth? Average revenue per user at Google, Facebook and Twitter | 18. Juni 2015
http://www.digitalstrategyconsulting.com/intelligence/2014/06/ad_revenue_per_user_google_facebook_twitter.php | AD: 30.06.2016

Duhigg, 2012: Duhigg, Charles | How Companies Learn Your Secrets
http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html | AD: 10.08.2016

D-Cent, 2013: Research on Identity Ecosystem
http://www.nesta.org.uk/sites/default/files/research_on_digital_identity_ecosystems.pdf | AD: 20.08.2016

Dwoskin und Gryta, 2015: Dwoskin, Elizabeth and Gryta, Thomas | AT&T Offers Data Privacy - for a Price | In: Wall Street Journal | 18. Februar 2015
http://blogs.wsj.com/digits/2015/02/18/att-offers-data-privacy-for-a-price/?mod=WSJ_TechWSJD_NeedToKnow | AD: 10.08.2016

Fittkau und Maaß: Fittkau & Maaß Consulting | Personalisierte Werbung im Internet Akzeptanz oder Reaktanz? Studie
http://www.fittkaumaass.com/internetworld/W3B29_Werbung_InternetWorld.pdf | AD: 26.09.2016

Friedewald et al., 2014: Friedewald, Michael; van Lieshout, Marc; Rung, Sven; Ooms, Merel and Ypma, Jelmer | Privacy and Security Perceptions of European Citizens: A Test of the Trade-off Model?

http://prismsproject.eu/wp-content/uploads/2015/04/IFIP_2014_20_Proceedings.pdf | AD: 30.08.2016

FTC, 2009: Federal Trade Commission | Self-Regulatory Principles for Online Behavioral Advertising | Washington DC
http://www.ftc.gov/opa/2009/02/behavad.shtm | AD: 20.08.2016

FTC, 2012: Federal Trade Commission | Does Hashing Make Data Anonymous?
https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous AD: 10.08.2016

FTC, 2014: Federal Trade Commission | Data Brokers - A Call for Transparency and Accountability | Washington DC
https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf | AD: 10.08.2016

Garner, 2015: Garner, Patricia | Average revenue per user is an important growth driver | In: Market Realist | 11. Februar 2015
http://marketrealist.com/2015/02/average-revenue-per-user-is-an-important-growth-driver/ AD: 10.08.2016

Gjermundrød, 2015: Gjermundrød, Harald | An Ecosystem for Private Customer Data Management
http://www.observatoire-fic.com/an-ecosystem-for-private-customer-data-management/ AD: 10.09.2016

Greenberg, 2016: Greenberg, Andy | Apple's 'Differential Privacy' Is About Collecting Your Data—But Not Your Data | In: Wired | 13. Juni 2016
https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/ AD: 20.06.2016

Greenhalgh, 2015: Greenhalgh, Hugh | Sell your personal data | In: Financial Times 16. Oktober 2015
https://www.ft.com/content/8e51ecd4-7327-11e5-bdb1-e6e4767162cc | AD: 10.09.2016

Hardjono, 2015: Hardjono, Thomas | User-Managed Access (UMA) Profile of OAuth 2.0 | Boston: MIT | https://docs.kantarainitiative.org/uma/rec-uma-core.html | AD: 10.09.2016

Information Commissioner's Office UK, 2016: What you can do now to prepare for the General Data Protection Regulation: a checklist
https://dpreformdotorgdotuk.files.wordpress.com/2016/03/preparing-for-the-gdpr-12-steps.pdf AD: 06.09.2016

Jardine, 2016: Jardine, Alana | What's your personal data worth? | In: IT Pro Portal
http://www.itproportal.com/2016/07/24/whats-personal-data-worth/ AD: 17.08.2016

Johnsen, 2016: Johnsen, Lauren | Google's Ad Revenue Hits $19 Billion, Even as Mobile Continues to Pose Challenges Up 19 percent since last year | In: Adweek | 28. Juli 2016
http://www.adweek.com/news/technology/googles-ad-revenue-hits-19-billion-even-mobile-continues-pose-challenges-172722 | AD: 17.09.2016

Kaye, 2015 :Kaye, Kate | The $24 Billion Data Business That Telcos Don't Want to Talk About In: Advertising Age | 26. Oktober 2015
http://adage.com/article/datadriven-marketing/24-billion-data-business-telcos-discuss/301058/ AD: 13.08.2016

Kharif et al., 2013: Kharif, Olga and Moritz, Scott | Carriers Sell Users' Tracking Data in $5.5 Billion Market | In: Bloomberg Technology | 6. Juni 2013
https://www.bloomberg.com/news/articles/2013-06-06/carriers-sell-users-tracking-data-in-5-5-billion-market | AD: 13.08.2016

Klosowski, 2013: Klosowski, Thorin | How to avoid
http://lifehacker.com/5973689/how-web-sites-vary-prices-based-on-your-information-and-what-you-can-do-about-it | AD: 22.07.2016

Kosinski et al., 2012: Kosinski, Michal; Stillwell, David; Kohli, Pushmeet; Bachrach,Yoram and Graepel, Thore | Personality and Website Choice | ACM Web Sciences
https://www.microsoft.com/en-us/research/publication/personality-and-website-choice/ AD: 04.08.2016

Krasnova et al., 2010: Krasnova, Hanna and Veltri, Natasha | Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA | 43rd Hawaii International Conference on System Science

Krishnamurthy and Wills, 2009: Krishnamurthy, Balachander and Wills, Craig
On the Leakage of Personally Identifiable Information Via Online Social Networks
http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf | AD: 24.07.2016

Kroes, 2012: Kroes, Neelie | Digital Agenda and Open Data | Rede 12/149 in Bratislava am 05. März 2012
http://europa.eu/rapid/press-release_SPEECH-12-149_en.htm | AD: 14.05.2016

Lemm, 2016: Lemm, Karsten | Dieses Startup verspricht euch Geld für eure Daten | In: Wired 25. Juni 2016
https://www.wired.de/collection/business/geld-verdienen-mit-facebook-und-twitter-datawallet-will-nutzer-fuer-ihre-daten | AD: 24.07.2016

Leonard, 2016:Leonard, John | TTIP vs GDPR - who will win the data protection wars? | In: Computing | 25. Januar 2016
http://www.computing.co.uk/ctg/analysis/2443135/ttip-vs-gdpr-who-will-win-the-data-protection-wars | AD: 24.06.2016

Li,2012: Li, Chao ; Yang, Li Daniel; Miklau, Gerome and Suciu, Dan | A Theory of Pricing Private Data | http://arxiv.org/abs/1208.5258 | AD: 24.07.2016

Lokshin, 2014: Lokshin, Pavel | Der elektronische englische Patient | In: Zeit, 9. April 2014 http://www.zeit.de/digital/datenschutz/2014-04/big-data-gesundheitswesen-nhs/komplettansicht AD: 20.05.2016

Luckerson, 2015: Luckerson, Victor | How AT&T Wants You to Pay For Your Privacy | In: Time | 18. Februar 2015 | http://time.com/3713931/att-privacy-charge/ | AD: 13.06.2016

Mayer-Schönberger et al., 2013: Mayer-Schönberger, Viktor and Cukier, Kenneth | Big Data: A Revolution That Will Transform How We Live, Work, and Think | Hodder & Stoughton, 2013

McAfee, 2015: The Hidden Data Economy http://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf | AD: 13.07.2016

Mikians al., 2012: Mikians, Jakub; Gyarmati, László; Erramilli, Vijay; Laoutaris, Nikolaos | Detecting price and search discrimination on the internet | Proceedings of the 11th ACM Workshop on Hot Topics in Networks. ACM.

Morando et al,. 2014: Morando, F.; Iemma, R. and Raiteri, E. | Privacy Evaluation: What Empirical Research on Users' Valuation of Personal Data Tells Us | In: Internet Policy Review (3:2), S.1-12.

Myslewski, 2014: Myslewski, Rik | The Internet of Things helps insurance firms reward, punish | In: The Register | 23. Mai 2014. http://www.theregister.co.uk/2014/05/23/the_internet_of_things_helps_insurance_firms_reward_punish/ | AD: 08.06.2016

Narayanan and Shmatikov, 2010: Narayanan, A. and Shmatikov, V. | Privacy and security Myths and fallacies of "Personally identifiable information" | Communications of the ACM, vol. 53 (6)

New Scientist, 2016: Revealed: Google AI has access to huge haul of NHS patient data | In: New Scientist| 29. April 2016 https://www.newscientist.com/article/2086454-revealed-google-ai-has-access-to-huge-haul-of-nhs-patient-data/ | AD: 15.05.2016

Ng, 2016:Ng, Irene | HATs and Rights | In: Biz Researcher | 6. Mai 2016 https://bizresearcher.wordpress.com/2016/05/06/hats-and-rights/ | AD: 17.06.2016

OECD, 2013a: Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value | OECD Digital Economy Papers 220 | OECD Publishing, Paris

OECD, 2013b: Working Party on the Information Economy Working Party on Information Security and Privacy

http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/IE/REG(2011)2/FINAL&docLanguage=EN | AD: 23.05.2016

Olejnik et al., 2014:. Olejnik, L.; Minh-Dung, T.; Castelluccia, C. | Selling off privacy at auction https://hal.inria.fr/hal-00915249/PDF/SellingOffPrivacyAtAuction.pdf | AD: 15.05.2016

Orcutt, 2011: Orcutt, Mike | How Much Is a User Worth? | MIT Technology Review, 12. Juli 2011 | https://www.technologyreview.com/s/424650/how-much-is-a-user-worth/ | AD: 03.05.2016

Pollack, 2016: Pollack, Lisa | What is the price for your personal digital dataset? | In: Financial Times | 10. Mai 2016.
https://www.ft.com/content/1d5bd1d0-15f6-11e6-9d98-00386a18e39d | AD: 15.05.2016

Powell, 2016: Powell, Rachel | UK customers severely underestimate the quantity of personal data stored about them | In: Retail Risk | 01. September 2016
http://news.retailrisk.com/news/uk-customers-severely-underestimate-the-quantity-of-personal-data-stored-about-them/ | AD:25.08.2016

Preibusch, 2013: Preibusch, Sören | Big Data, Small Money, No Privacy?
http://preibusch.de/publications/Preibusch__Big-Data_Value-of-Privacy_digma-2013.pdf | AD: 15.05.2016

Quirk, 2013: Quirk, Mary Beth | Data Broker Acxiom's New Site Allows Users To View And Edit The Marketing Info It's Collected
https://consumerist.com/2013/09/04/data-broker-acxioms-new-site-allows-users-to-view-and-edit-the-marketing-info-its-collected/ | AD: 17.05.2016

Rainie und Janna, 2014: Rainie, Lee and Anderson, Janna | The Future of Privacy
http://www.pewinternet.org/2014/12/18/future-of-privacy/ | AD: 16.06.2016

Rainie, Lee und Doggan, Maeve 2016: Privacy and Information Sharing
http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf
AD: 22.07.2016

Roberds und Schreft, 2009: Roberds, William and Schreft, Stacey L. | Data security, privacy, and identity theft: The economics behind the policy debates
https://www.chicagofed.org/publications/economic-perspectives/2009/1qtr2009-part4-roberds-schreft | AD: 22.08.2016

Sachverständigenrat für Verbraucherfragen (Hrsg.), 2016: Verbraucher in der Digitalen Welt - Verbraucherpolitische Empfehlungen | Januar 2016
https://www.bmjv.de/SharedDocs/Downloads/DE/Artikel/01192016_Digitale_Welt_allgemein.pdf?__blob=publicationFile&v=4 AD: 18.06.2016

Savage und Waldman, 2013: Savage, Scott and Waldman, Donald M. | The Value of Online Privacy
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2341311 | AD: 24.07.2016

Schmidt, 2014: Schmidt, Holger | Die Menschen würden fürs Netz viel mehr Geld zahlen
https://netzoekonom.de/2014/03/01/die-menschen-wuerden-fuer-das-internet-170-mrd-dollar-mehr-zahlen/ | AD: 27.06.2016

Schneier, 2009: Schneier, Bruce | A Taxonomy Of Social Networking Data
https://www.schneier.com/blog/archives/2009/11/a_taxonomy_of_s.html | AD: 14.05.2016

Schütz und Karaboga, 2015: Schütz, Phili und Karaboga, Murat | Akteure, Interessenlagen und Regulierungspraxis im Datenschutz - Eine politikwissenschaftliche Perspektive - Abeitspapier
https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/Schuetz-und-Karaboga-Akteure-Interessenlagen-und-Regulierungspraxis-im-Datenschutz-2015.pdf | | AD: 29.06.2016

Seibel, 2015: Seibel, Karsten | Gegen Kreditech ist die Schufa ein Schuljunge | In: Die Welt, 17. Mai 2015
https://www.welt.de/finanzen/verbraucher/article139671014/Gegen-Kreditech-ist-die-Schufa-ein-Schuljunge.html | AD: 20.09.2016

Sherry,2016: Sherry, Frank | Differential privacy for dummies
https://github.com/frankmcsherry/blog/blob/master/posts/2016-02-03.md | AD: 20.09.2016

Spiekermann et al., 2002: Spiekermann, S.; Grossklags, J. and Berendt, B. | E-privacy in 2nd generation E-Commerce | ACM Conference on Electronic Commerce (EC'01) | Ed. ACM New York, 38-47 | Tampa, Florida: ACM Press

Spiekermann et al., 2015: Spiekermann, Sarah; Böhme, Rainer; Acquisti, Alessandro and Hui, Kai-Lung | The Challenges of Personal data markets and Privacy | In: Electronic Markets | June 2015, Volume 25, Issue 2, 91–93
http://link.springer.com/article/10.1007/s12525-015-0190-1 | AD: 20.05.2016

Sporck, 2016: Sporck, Lauren | 8 of the Largest Data Breaches of All Time | In: Opswat 18. Januar 2016. https://www.opswat.com/blog/8-largest-data-breaches-all-time | AD: 22.06.2016

Steel et al., 2013: Steel, Emily; Locke, Callum; Cadman, Emily and Freese, Ben | How much is your personal data worth? | In: Financial Times, 13. Juni 2013
http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz4M1axQmov | AD: 291.08.2016

Stevens, 2016: Stevens, Adrian: How Is Facebook’s Average Revenue per User Trending? | In: Market Realist, 24. Mai 2016.

http://marketrealist.com/2016/05/facebooks-average-revenue-per-user-trending/ | AD: 21.08.2016

Strahilevitz und Kugler, 2015: Strahilevitz, Lior and Kugler, Thomas | Is Privacy Policy Language Irrelevant to Consumers? | 6. Oktober 2015 http://www.law.uchicago.edu/files/file/strahilevitz_kugler_is_privacy_policy_language_irrelevant_to_consumers.pdf | AD: 21.08.2016

Sweeney, 2000: Sweeney, Latanya | Simple Demographics Often Identify People Uniquely | Carnegie Mellon University | Data Privacy Working Paper 3 | Pittsburgh 2000 http://dataprivacylab.org/projects/identifiability/paper1.pdf | AD: 30.07.2016

Sweeney, 2002: Sweeney, L. | k-anonymity: a model for protecting privacy | In: International Journal on Uncertainty, Fuzziness and Knowledge-based Systems,10 (5), 2002; 557-570. http://epic.org/privacy/reidentification/Sweeney_Article.pdf | AD: 30.07.2016

Tsai et al., 2007: Tsai, Janice Y.; Egelman, Serge; Cranor, Lorrie and Acquisti, Alessandro | The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study http://www.econinfosec.org/archive/weis2007/papers/57.pdf | AD: 28.05.2016

Tsai et al., 2010: Tsai, Janice Y.; Egelman, Serge; Cranor, Lorrie and Acquisti, Alessandro | The effect of online privacy information on purchasing behavior: an experimental study http://www.heinz.cmu.edu/~acquisti/papers/acquisti-onlinepurchasing-privacy.pdf | AD: 23.05.2016

Wang et al.,2013: Wang, Y.; Leon, P. G.; Chen X.; Komanduri, S.; Norcie, G.; Scott, K.; Acquisti, A.; Cranor, L. F. and Sadeh, N. | The second wave of global privacy protection: From Facebook regrets to Facebook privacy nudges | Ohio State Law Journal 74, 1307–1334

WEF, 2011: World Economic Forum Personal Data: The Emergence of a New Asset Class http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf | AD: 05.05.2016

WEF, 2012: World Economic Forum Rethinking Personal Data: Strengthening Trust http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf | AD: 05.05.2016

Zyskind, et al., 2014: Zyskind, Guy; Nathan, Oz; Pentland, Alex | Decentralizing Privacy: Using Blockchain to Protect Personal Data. http://web.media.mit.edu/~guyzys/data/ZNP15.pdf | AD: 06.09.2016

7. Abbildungs- und Tabellenverzeichnis

8. Anhang

Anlage I: Werkzeuge zum Wert von Daten und weiterführende Links

Wert der persönlichen Daten - Rechner und Werkzeuge

Wert einzelner Daten im britischen Markt:
http://ig.ft.com/features/2013-06-12_personalData/

Infografik zum geschätzten Wert der persönlichen Daten
http://www.totallymoney.com/personal-data/

Was bin ich wert? - Grafik zum Wert persönlicher Daten
https://www.brandeins.de/archiv/2014/beobachten/was-bin-ich-wert/

Überblick zur Ansammlung von persönlichen Daten

Digitaler Fußabdruck beim Provider von Cookie-Services
http://www.bluekai.com/registry/
Das zu Oracle gehörende Unternehmen BlueKai gibt an, 750 Millionen BenutzerInnen-Profile von Internetuser zu haben und verarbeitet mehr als 30.000 Eigenschaften von und zu diesen BenutzerInnen. Es bezeichnet sich selbst als größter Datenhändler. An einem durchschnittlichen Tag tätigt BlueKai über 75 Millionen Online-Auktionen für die persönliche Information.

Nachvollziehbarkeit von Daten-Tracking-Tools

Mit jedem Klick hinterlassen wir Spuren im Internet. Einige Online-Tools machen das Tracking verständlich.

Bunte Datenblumen machen die Datenspuren sichtbar und zeigen, wer die Wege durchs Netz trackt.
http://datenblumen.wired.de

Das interaktive Karte Trackography zeigt an, wohin und zu welchen Firmen Daten gesendet werden, wenn man Nachrichtenseiten liest.
https://www.tacticaltech.org/projects/trackography

MyShadow visualisiert die digitalen Schatten, die NutzerInnen im Internet werfen.
https://myshadow.org/tracking-data-traces

MyPersonality erstellt eine Prognose von sensiblen Persönlichkeitseigenschaften, die sie aus Facebook-Likes generiert.
http://mypersonality.org/wiki/doku.php

TakeThisLollipop ist ein Projekt zur Darstellung der von Facebook gesammelten Information - mit Unterhaltungswert.
http://www.takethislollipop.com/

Die Visualisierung von Vorratsdaten des Politiker Malte Spitz.
http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz

Datenschutzampel: Anregung und Vorschlag

Viele InterviewpartnerInnen fordern die Einführung einer „Datenschutzampel“.[143] [144] Sie zeigt für Webseiten, Apps, Software und Social Media an, ob es ohne ausdrückliche Zustimmung zu

- keiner Erfassung
- keiner Verarbeitung
- keiner Profilbildung
- keiner Weitergabe der Daten an Dritte

bei einer Website, Apps, Software etc. kommt. Der Prototyp der Datenschutzampel kann folgendermaßen skizziert werden:

„Datenschutz-Ampel“

Neben einer detaillierten Ausarbeitung dieser Ampel ist unklar, welche Organisation oder öffentliche Stelle eine solche Zertifizierung vornimmt und auch prüft.[145]

Werkzeuge für mehr Datenschutz

Das Projekt TOSDR (Terms of Service; Didn't Read) bietet auf seiner Plattform und als Browser-Addon eine übersichtliche Auflistung der Datenschutzbedingungen gängiger

[143] vgl. http://www.heise.de/ct/ausgabe/2014-4-Technische-Loesungen-fuer-mehr-Datenschutz-2094551.html
[144] Auf Anregung von Alexander Sander von https://digitalegesellschaft.de/
[145] vgl. https://netzpolitik.org/2014/bundesregierung-sucht-die-politik-eines-neuen-betriebsystems/

Services und bewertet sie. Dies könnte auch als Vorbild für die oben genannte Datenschutzampel dienen.
https://tosdr.org/

Mit der Android-App „SRT AppGuard" können auf einem Gerät installierte Apps überwacht und nachträglich Berechtigungen geändert werden. So können einer App bestimmte Zugriffe, wie z.B. auf die Kontakte, untersagt werden.

Sonstige Links

Automatisierte Auskunftsformulare, die VerbraucherInnen ermächtigen, von Firmen und Behörden ihre Daten zu bekommen.
https://selbstauskunft.net/

„How-To Analyze Everyone" - Web-Serie von netzpolitik.org
https://netzpolitik.org/?s=How-To+Analyze+Everyone

Blog zu Adresshandel und Scoring in Deutschland
https://safeaddress.wordpress.com/

Interview mit dem CEO von Google, Eric Schmidt, über die Macht des Konzerns
http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/#video

Mindreader - Experiment
Social media und wie sich Leute fühlen wenn Sie erfahren wenn ein fremder Ihre persönlichen Daten kennt - Video
https://www.youtube.com/watch?v=F7pYHN9iC9I

The Eternal Value of Privacy - Bruce Schneier 2006
https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html

Kunstprojekt Data-arbitrage
http://www.dataarbitrage.org/

Online-Datenhandel für VerbraucherInnen

Auflistung von untersuchten, beobachten oder betrachteten Online-Handelsmöglichkeiten und Services:

https://citizenme.com
https://datawallet.io
https://datacoup.com
http://handshake.uk.com/hs/index.html
https://www.datafairplay.com

https://meeco.me
https://midata.coop
https://people.io
https://digi.me
http://Personal.com[146]
https://cozycloud.cc
https://mydex.org
https://fr.umanlife.com
https://ctrlio.com
https://mypermissions.org
https://www.hatdex.org
https://datalocker.com/

Weiteres Beispiel:
Frederico Zannier verkaufte seine persönliche Daten für $2,733[147] auf einer Crowdfunding-Plattform. Diesen Wert sollte man als Einzelfall betrachten.

[146] Die Firma beendete trotz eines Budgets von 14 Mio. US-Dollar sein ursprüngliches Geschäftsmodell des persönlichen Datenhandel für VerbraucherInnen und fokussiert sich nun auf Datenschutz im Geschäftskundensegment (vgl. https://www.technologyreview.com/s/517356/if-facebook-can-profit-from-your-data-why-cant-you/)
[147] vgl. https://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth

Anlage II: Fallbeispiele des Datenhandels

Beispiele des Handels persönlicher Daten von Unternehmen

Axicom vertreibt folgende 6 Merkmale Besonderheit (Alter, Geschlecht, Bildung, Familienstand), Wohnung (Eigenheim oder Miete), Auto (Marke und Modell, Versicherung), Ökonomisch (Einkommen, geschätzte Käufe mit verschiedenen Kreditkarten), Kaufverhalten (Anzahl und Menge der Käufe in Kategorien (on- und offline, Versand und Produktarten) und Interessen (eine Liste Interessen langen Liste von Möglichkeiten) über eine Person[148]. Selbstauskunft kann man über https://aboutthedata.com/ erfolgen. Acxiom ist eine $1.1 Milliarden großes Unternehmen welches ca. 12% Marktanteil im $11 Milliarden großen Direkt-Marketing-Services-Markt hat und mehr als 190 Millionen individuelle VerbraucherInnen-Profile und mehr als 126 Millionen Haushaltsprofile.[149]
Seien es die US Präsidentschaftswahlen, Brexit-Kampagne oder europäische Wahlen auch hier spielen die persönlichen Daten von potenziellen WählerInnen und deren politischen Präferenzen und Ansichten eine Rolle und werden gekauft und verkauft.[150]
Echtzeit-Werbe-Versteigerungsplattformen sind eine Weiterentwicklung des klassischen BieterInnen-Prozesses für die Auslieferung von Online-Werbung. Mit Real Time Bidding kann auf jede einzelne Ad Impression in Echtzeit, also noch während der User die jeweilige Webseite aufruft, individuell massgeschneidert für den/die jeweilige/n BesucherIn angeboten werden. Dieser Markt beläuft sich in Deutschland auf 138 Mio. Euro[151].

Beispiel 1: Fraud-Detection und Kredit-Scoring

Beim Online-Shopping führt die Bewertung der Kreditwürdigkeit zu einem Marktausschluss, der zum Beispiel eine Begrenzung der Zahlungsmöglichkeiten zur Folge hat[152]. Das Risiko der Diskriminierung bestimmter Bevölkerungsgruppen ist hier besonders hoch. In diesem Fall spielen unter anderem Geodaten eine Rolle, z.B. Postleitzahlen. Es gibt auch weitere Fälle, wo bereits das äußere Aussehen des Hauses einer Adresse das Kreditrating beeinflusst.

Beispiel 2: Preisdiskriminierung

Von Preisdiskriminierung spricht man, wenn dasselbe Produkt für unterschiedliche VerbraucherInnen zu unterschiedlichen Preisen angeboten wird. Eine spanische Studie (vgl. Mikians et al. 2012) hat in einem aufwändigen Forschungsdesign 600 Produkte in 35 Produktkategorien in 200 großen internationalen Online-Shops untersucht und dabei eine individualisierte Preisgestaltung bzw. eine individuell unterschiedliche Auswahl von billigeren oder teureren Produkten in den Suchergebnissen beobachtet. Ein konkretes Beispiel dazu ist die Abfrage bei der Urlaubsbuchung bzw. Flugbuchung. Aufgrund der Diskriminierung anhand verschiedener Datenpunkte kann es zu einem Nachteil von bis 30 US-Dollar pro

[148] vgl. http://www.forbes.com/sites/metabrown/2015/09/30/your-personal-datas-for-sale-but-is-it-accurate/2/#25817e9a7193
[149] vgl. http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html
[150] vgl. https://next.ft.com/content/fc1879be-1ed4-11e6-b286-cddde55ca122
[151] vgl. http://www.statista.com/statistics/245720/rtb-digital-display-ad-spending-in-germany/
[152] vgl. http://www.boniversum.de/bonima/

Buchung oder 30% des Preises kommen.[153] Oder bei Apple-BenutzerInnen ein höheres Preis angezeigt wird, da ein höheres Einkommen angenommen wird.[154]

Beispiel 3: Suchdiskriminierung
Bei der Suchdiskriminierung werden dem/der VerbraucherIn aufgrund spezifischer Parameter nur bestimmte Optionen angeboten oder zumindest prioritär angezeigt (teurere Produkte zuerst, billiger weiter hinten gelistet).

Beispiel 4: Wearables und Gesundheitsdaten
Versicherungen und Krankenkassen fördern zunehmend die Nutzung von Wearables und Fitness-Apps. Die damit verbundenen Problemfelder des Datenschutzes erhalten allerdings nur wenig Aufmerksamkeit. Auch stellt sich die Frage, ob in Zukunft das fehlende Einverständnis zur Datenfreigabe dazu führen kann, dass KundInnen Preisnachteile befürchten müssen.
Aktuelle Beispiele:

- AOK Nordost fördert mit bis zu 50 Euro den Kauf von „Quantified-Self-Hardware“.[155]
- Generali belohnt Benutzer der Vitality-App, ein Fitness-Trackern mit bis zu 16% günstigeren Tarifen.[156]

Beispiel 5: Tracking über verschiedene Geräte
Dabei geht es um die Zusammenführung von Online und Offline-Daten eines/einer Verbrauchers/in. Beim Crossdevice-tracking wird versucht den/die BenutzerIn und sei/ihr Verhalten über mehrere Geräte zusammenführen (Smartphone, Pad, Laptop, …). Eine der führenden Firmen auf diesem Gebiet ist Datalogix, welche digitale Medien und Offline-Einkäufe nutzt, um aussagekräftige Erkenntnisse und Datenanalysen und für VermarkterInnen zu schaffen. Datalogix 2015 für 1.2 Milliarden USD von Oracle gekauft worden.

Beispiel 6: Vernetztes Auto
Im Connected Car kann viel gespeichert werden, wie schnell gefahren wird, Drehzahl des Motors und Verwendung der Bremsen, die Müdigkeit des/der Fahrers/in, wie viele Mitfahrer/innen, der angehörte Musik, etc. Genauso umfangreich sind die legalen und illegalen Möglichkeiten der Weiternutzung dieser Daten, um Autos in das herstellereigene Werkstattnetz zu lotsen, Werbeeinschaltung für den nächsten Parkplatz, Restaurant, Tankstelle oder Hotel (durch Standortbestimmung).Wenn der/die Autofahrer/in seinen/ihren Fahrstil mit einer im Auto installierten Blackbox oder On-Board-Units überwachen lässt, zahlt er niedrigere Versicherungsbeiträge.[157] Dies kann für FahranfängerInnen bis zu 400 Euro Ersparnis (oder bis zu 30 % der Versicherungsgebühren) bedeuten.[158] Wenn ein/e AutoherstellerIn glaubhaft versichert, dass die gesammelten Daten für die Verbesserung des Produktes verwendet werden, sind 76 Prozent der befragten Personen im Gegenzug bereit ihre Daten weiter zu leiten, 21 Prozent stimmen dem Datentransfer nur zu, wenn die Daten

[153] vgl. http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html
[154] vgl. http://www.oiat.at/files/DynamicPricing_OIAT.pdf
[155] vgl. https://nordost.aok.de/inhalt/aok-gesundheitskonto/
[156] vgl. https://www.generali-vitalityerleben.de/
[157] vgl. http://www.sueddeutsche.de/auto/telematik-tarife-bei-kfz-versicherungen-viel-ueberwachung-fuer-ein-bisschen-ersparnis-1.2486679
[158] ebd.

nicht an Dritte weitergegeben werden und 55 Prozent würden ohne Einschränkungen zustimmen.[159] Die Mehrheit der VerbraucherInnen wollen laut Umfragen einer der FIA die Datenhoheit beim Connected Car und die dafür notwendigen gesetzlichen Regelungen.[160]

Beispiel 7: Gendaten

Die Gentest-Webseite 23AndMe hat 2015 die Gen-Datensätze von 3.000 Kunden mit Parkinson-Krankheit für insgesamt 60 Millionen US-Dollar an den Pharmakonzern Genentech verkauft, der zu Roche gehört. Das entspricht einem Wert von 20.000 US-Dollar pro Datensatz. 23AndMe analysiert im Auftrag seiner/ihrer EinzelkundInnen Genome, die man für den Preis von 99 US-Dollar pro Testkit bei der Firma einsenden kann. Somit verdient 23AndMe doppelt - zum einen mit der Analyse im Auftrag von EinzelkundInnen und im Verkauf seiner Testdaten an andere Unternehmen[161].

Beispiel 8: Rezeptdaten

Das apotheker-eigene Rechenzentrum VSA verkaufte jahrelang[162] Rezeptdaten an Marktforschungsfirmen. Diese unverschlüsselte und nicht gesetzeskonform „anonymisierte" Daten wurden von den beteiligten Firmen übermittelt, abgerufen und gespeichert.[163] Dabei ging neben der Frage um die Legalität auch die Frage der Legitimität. Welches Interesse sollten PatientInnen und Ärzte daran haben, dass ihre Rezeptdaten überhaupt an Marktforscher weitergegeben werden, egal ob unverschlüsselt oder anonym? Würde der Weitergabe der Daten zugestimmt werden wenn man die Patienten dazu befragen würde?[164]

[159] vgl. http://vernetzte-welt.com/mckinsey-vernetzung-im-auto-auf-dem-vormarsch/
[160] vgl. http://www.oeamtc.at/portal/oeamtc-risiken-der-digitalisierung-ndash-europaeer-wollen-datenhoheit-im-auto+2500+1640684
[161] vgl. http://www.forbes.com/sites/matthewherper/2015/01/06/surprise-with-60-million-genentech-deal-23andme-has-a-business-plan/#1799ac8c7927
[162] vgl. http://www.spiegel.de/spiegel/print/d-83977268.html
[163] vgl. http://www.spiegel.de/netzwelt/netzpolitik/rezeptdaten-verkauf-bayerisches-apothekenrechenzentrum-in-der-kritik-a-993106.html
[164] vgl. http://www.spiegel.de/spiegel/spiegelblog/vsa-verkauft-rezeptdaten-an-marktforschungsfirmen-a-920845.html

Anlage III: Beispiele für Datenhandel in Deutschland

Bei vielen der oben angeführten Beispiele stehen die Praktiken von US-Firmen im Fokus. Dies liegt zum einen an den rasanten Marktentwicklungen vor allem im Silicon Valley und den nicht so strengen Datenschutzbestimmungen im Vergleich zu Deutschland (vgl. Abbildung 6). Zum anderen werden diese Unternehmen besonders intensiv von den Medien beobachtet.

Abbildung 6: Übersichtsgrafik deutscher vs. amerikanischer Datenschutz von Seniorbook

Allerdings haben auch Unternehmen in Deutschland einen großen Markt im Zusammenhang mit dem Daten- und Adresshandel, Scoring und Online-Tracking aufgebaut. Anhand von drei großen MarkteilnehmerInnen und deren Aktivitäten soll hier die Erfassung, Analyse und Verknüpfung von Daten skizziert werden, um die Verwertung persönlicher Daten im deutschen Sprachraum darzustellen (vgl. Abbildung 7).[165]

[165] vgl. http://wolfie.crackedlabs.org/dl/Studie_Datenhandel_DE_Inhalt.pdf

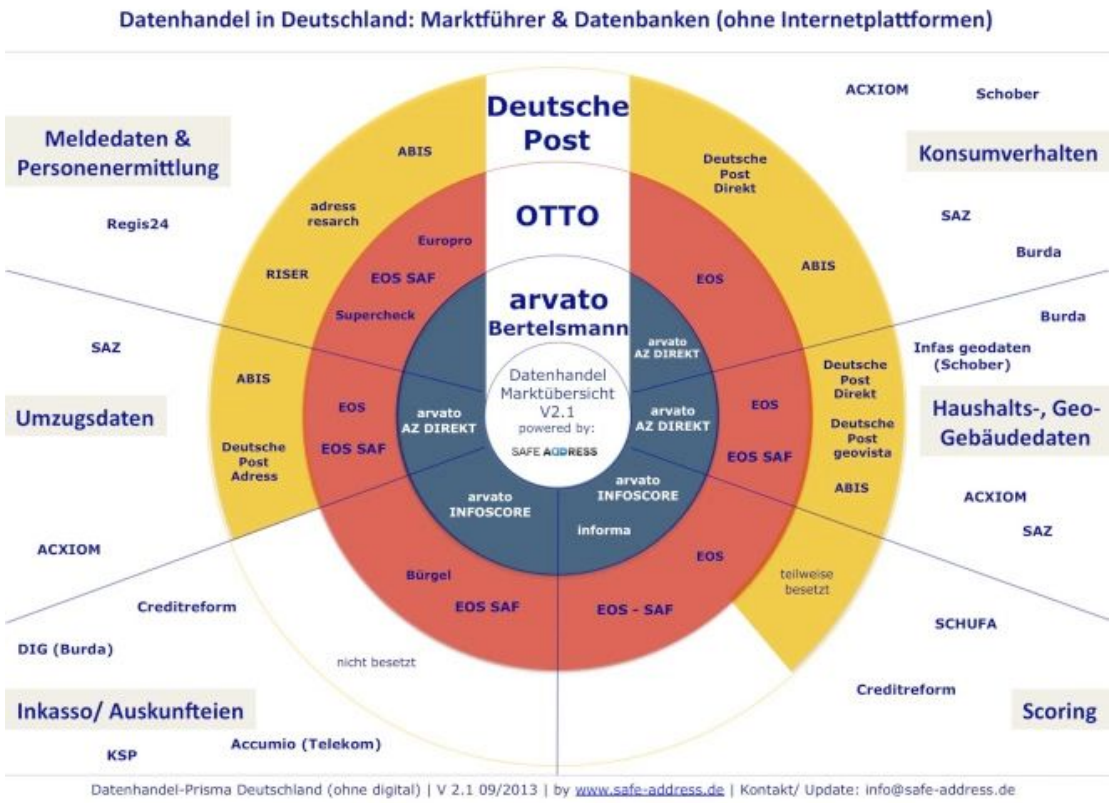

Abbildung 7: Datenhandel in Deutschland, von Safe-Adress.de

Beispiele der Bertelsmann-Gruppe umfassen arvato AZ Direct: Adressen, Geo- und Marketingdaten (System „AZ DIAS“: 600 Merkmale über 70 Millionen Menschen, Analyse und Anreicherung von Kundendaten, Verknüpfung von Online und Offline), arvato infoscore (Bonitäts- und Risikobewertung von Privatpersonen) und weitere Angebote von Kundenkartensystemen bis zu Sperrlisten.

Beispiele der Creditreform-Gruppe umfassen Boniversum, die Bonitäts- und Risikobewertung von Privatpersonen (Scoring-Angebote von Boniversum, Echtzeit-Bonitätsbewertung von VerbraucherInnen, Integrierte Software von Bonität über Inkasso bis Online-Zahlung), microm für Adressen, Geo- und Marketingdaten (36 Millionen Adressen, 40 Millionen Haushalte und 1.000 Merkmale, Anreicherung, Analyse und Klassifikation von Kundendaten; Verknüpfung von Online und Offline).

Beispiele der Deutschen Post umfassen Deutsche Post Direkt für Adressen, Geo- und Marketingdaten (Namen, Adressen und Umzugsdaten; eine Milliarde qualifizierter Merkmale, über 37 Millionen Adressen; Scoring, Analyse und Anreicherung von Kundendaten; Online-Tätigkeiten und Verknüpfung mit Offline-Daten;) sowie Gemeinschaftsunternehmen mit Bertelsmann die Deutsche Post Adresse (Adressrecherche, -aktualisierung und Stammdatenpflege; Europäische Melderegisterauskunft RISERID; ABIS: Adressen-basierte Informationsdienstleistungen www.abis-online.de)

Anlage IV: Interviews

Mit folgenden Person wurden zur Erstellung der Studie Interviews und Hintergrundgespräche geführt. Bei Interviewpartnern aus dem Wirtschaftssektor galt teilweise die Chatham-House-Regelung für konkrete Bewertungen. Alle Personen werden kategorisch ohne akademische Titel angeführt und alphabetisch geordnet.

- Benjamin André, CEO cozycloud, Personal Data Economy, technische Aspekte
- Andreas Berger, Humada Inc., technische Aspekte und Personal Data Economy
- Malte Beyer-Kaltenberger, EC DG Connect, Personal Data Economy and Policy
- Alfred Büllesbach, ehemaliger Landesdatenschutzbeauftragter von Bremen, Datenschutz, informelle Selbstbestimmung
- Wolfie Christl, datadealer.net, Datenschutz, Wert der Daten
- Nicolas Debock, Balderton Capital, UK, Personal Data Economy
- Katryna Dow, CEO meeco, Personal Data Economy
- Jan Gerber, Systemadministrator und Programmierer, technische Aspekte
- André Golliez, MIDATA.COOP – CititzenControlled Reuse of
- Max Kasy, Ökonom, Harvard University, Wert der Daten
- Constanze Kurz, CCC Berlin, Datenschutz, informationelle Selbstbestimmung
- Irene Ng, Warwick University, Personal Data Economy und HAT
- Dietmar Offenhuber, MIT / Northwestern University, Personal Data Economy
- Antti Poikola, MyData, Personal Data Economy, mydata
- Rufus Pollock, Founder OKFN, Personal Data Economy
- Markus Sabadello, Personal Data Economy, Technische Herausforderungen,
- Molly Schwartz, OKFN, MyData, Personal Data Economy
- Michael Seemann, Kulturwissenschaftler, Berlin, postprivacy & Datenschutz, informationelle Selbstbestimmung
- Alexander Sander, GF Digitale Gesellschaft, Datenschutz, informationelle Selbstbestimmung
- Doc Searls, Center for Information Technology & Society (CITS), USA, Datenschutz, Wert der Daten, Personal Data Economy
- Felix Stalder, Dozent für Medienökonomie Universität Zürich, Personal Data Economy

Folgende Fragestellungen wurden erörtert und diskutiert:

1. Welche Art von Datenvermarktung gibt es aktuell, wie stehen Sie dazu? (Präferenzen für Datenschutz, Handelsmöglichkeiten)
2. Wie schätzen Sie die Möglichkeiten des Handels mit persönlichen Daten ein?
3. Welche Angebote gibt es heute schon im Internet zum Handel mit persönlichen Daten?
4. Können VerbraucherInnen transparent nachvollziehen, welcher Wert sich mit den Verkauf ihrer Daten ergeben kann? Gibt es Beispiele und Richtwerte?
5. Welche Rahmenbedingungen benötigt dieser Handel (technische Plattformen, ...?)
6. Falls mögliche, detaillierte Besprechung bzgl. notwendiger technischer Lösungen.
7. Einschätzung, wie der Handel mit persönlichen Daten den VerbraucherInnen den Wert jener näher bringen könnte und somit den Datenschutz stärkt.