Lasarov, Wassili; Hoffmann, Stefan

Paradoxes Datenschutzverhalten

HMD Praxis der Wirtschaftsinformatik

Provided in Cooperation with:
Springer Nature

Suggested Citation: Lasarov, Wassili; Hoffmann, Stefan (2021) : Paradoxes Datenschutzverhalten, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden, Wiesbaden, Vol. 58, Iss. 6, pp. 1535-1551, https://doi.org/10.1365/s40702-021-00706-2

This Version is available at:
https://hdl.handle.net/10419/287544

HMD (2021) 58:1535–1551
https://doi.org/10.1365/s40702-021-00706-2

SPEKTRUM

Paradoxes Datenschutzverhalten

Diskrepanz zwischen Datenschutzbedenken und nachlässigem Umgang mit digitalen Dienstleistungen

Wassili Lasarov · Stefan Hoffmann

Eingegangen: 18. November 2020 / Angenommen: 29. Januar 2021 / Online publiziert: 18. Februar 2021

Zusammenfassung Einhergehend mit der Digitalisierung vieler Lebensbereiche werden große Mengen persönlicher Daten von Konsument*innen durch Unternehmen und Institutionen erfasst und analysiert. Daher ist der verantwortungsvolle Umgang mit diesen Daten eines der drängendsten Themen der Gegenwart. Zwar gibt es zahlreiche gesetzliche Verordnungen (z. B. GDPR) sowie eine zunehmende Anzahl von Unternehmen, die sich freiwillig dem Datenschutz verpflichten, allerdings nutzen auch viele Unternehmen und Institutionen die Unachtsamkeit von Konsument*innen aus. Dies wird dadurch begünstigt, dass viele Konsument*innen zwar angeben, dass sie auf ihre Privatsphäre achten, aber nur wenige die dafür notwendigen Maßnahmen ergreifen. Diese Einstellungs-Verhaltens-Diskrepanz (Privatsphäre-Paradoxon) lässt sich einerseits durch ein rationales Kosten-Nutzen-Kalkül erklären, in dem Konsument*innen den Nutzen bestimmter Produkte (z. B. durch Personalisierung) mit der Preisgabe ihrer Daten verrechnen. Andererseits können situative Einflüsse (z. B. wenig Zeit) oder kognitive Verzerrungen (z. B. Kontrollillusion) Datenschutzbedenken in diesen Situationen verringern. Vor diesem Hintergrund führen wir in das Privatsphäre-Paradoxon ein und zeigen den Stand des Schrifttums auf, wobei wir auf situative und kognitiven Verzerrungen fokussieren. Abschließend wird das Konzept der drei Privatsphäre-Gaps eingeführt und ein Rahmen für zukünftige Forschung entwickelt.

Schlüsselwörter Datenschutz · Datensicherheit · Privatsphäre · Konsumentenverhalten

W. Lasarov (✉) · S. Hoffmann
Professur für Marketing, Christian-Albrechts-Universität zu Kiel, Westring 425, 24118 Kiel, Deutschland
E-Mail: lasarov@bwl.uni-kiel.de

S. Hoffmann
E-Mail: stefan.hoffmann@bwl.uni-kiel.de

Paradoxical Privacy Behavior

Discrepancy Between data Privacy Concerns and Careless use of Digital Services

Abstract In the digital age, many companies and institutions collect and analyze unprecedented quantities of personal data amounts. Therefore, the responsible handling of this data is one of the most pressing issues of our time. Although many countries have adopted data protection laws and many companies voluntarily commit to data protection, there are still many organizations that are exploiting the lack of consumer awareness in situations where data privacy is relevant. Although consumers often state their concerns about their online privacy, only a small share of them actually take the necessary actions to preserve their privacy, referred to as the privacy paradox. On the one hand, the privacy paradox can result from an individual rational calculus where consumers offset the benefits of certain products against the protection of their data. On the other hand, there exist many situational influences (e.g., little time) or cognitive biases (e.g., control illusion) that might reduce consumer's privacy concerns in certain situations. Against this backdrop, the paper first discusses the privacy paradox and captures the current state of privacy scholarship, focusing on the situational and cognitive biases. Finally, we introduce the concept of three privacy gaps and develop a framework for future research.

Keywords Data protection · Data security · Privacy · Consumer behavior

1 Einleitung

Im Zuge der Digitalisierung vieler Lebensbereiche haben sich die Konsumgewohnheiten sowie die Vermarktung von Produkten grundlegend verändert (Kannan 2017; Kumar 2018; Rust 2020). Diese Entwicklungen wurden besonders durch den Einsatz von personalisierten Such- und Entscheidungshilfen sowie personalisierten Produkten und Dienstleistungen (z. B. personalisierte Playlists auf Spotify) vorangetrieben. Mit einer effektiven Personalisierung geht allerdings auch einher, dass große Mengen persönlicher Daten von Verbraucher*innen durch Unternehmen und Institutionen erfasst und automatisch analysiert werden (z. B. Bewegungsdaten, Satariano 2019; Gesichtserkennungssoftware, Feng 2019). Angesichts der automatisierten Verarbeitung dieser unüberschaubaren Datenmengen ist der verantwortungsvolle Umgang mit sensiblen Daten durch Unternehmen und öffentliche Institutionen eines der drängendsten Themen der Gegenwart (Acquisti et al. 2015). In diesem Sinne wurden in den vergangenen Jahren gesetzliche Verordnungen erlassen, die den Umgang von Organisationen mit persönlichen Daten regeln (z. B. Datenschutz-Grundverordnung der Europäischen Union, GDPR). Manche Unternehmen setzen sich freiwillig für den Schutz der Privatsphäre ihrer Mitarbeiter*innen und Kund*innen in einem Maß ein, das über die gesetzlichen Bestimmungen und Regulierungen hinausgeht (BMJV 2020; Lobschat et al. 2020). Damit einhergehend sehen viele Konsument*innen Politik und Wirtschaft in der Verantwortung – und weniger sich selbst (PWC 2020). Dieses verbraucherseitige Abgeben von Verantwortung führt in vielen Situationen zu einem unachtsamen Umgang der Verbraucher*innen mit ihren Daten, was wie-

derum von einigen Unternehmen ausgenutzt wird (z. B. durch „Dark Patterns“, Gray et al. 2018). Dies wird an dem folgenden Beispiel deutlich: Internetauftritte von Firmen haben oftmals sehr ausführliche Allgemeine Geschäftsbedingungen (AGB), die selten von den Besucher*innen einer Webseite vollständig gelesen und verstanden werden, was oft zu einer „blinden“ Einwilligung verführt (Acquisti et al. 2020; SVRV 2017). Zwar gibt es Bestrebungen, die Länge und Komplexität der angezeigten AGB zum Schutze der Verbraucher*innen zu reduzieren (wie bspw. vom Sachverständigenrat für Verbraucherfragen vorgeschlagen, SVRV 2016), allerdings existieren bisher keine bindenden gesetzlichen Regelungen hierfür. Ebenso gibt es Diskussionen darüber, wie stark die Default-Einstellungen bei Cookies auf den Schutz der Privatsphäre ausgerichtet sein sollten (Acquisti et al. 2017, 2020). Konsument*innen haben wiederum selten die notwendigen Kapazitäten (z. B. Zeit, Wissen, technische Kapazitäten), um das „geeignete“ Verhalten in datenschutzrelevanten Situationen zu bestimmen. Erschwerend kommt hinzu, dass die individuellen Grenzkosten für zusätzlichen Datenschutz für Konsument*innen rapide ansteigen, u. a. durch sog. *Lock-in Effekte*. So liegt der Nutzen von sozialen Netzwerken gerade im hohen Engagement einer wachsenden Anzahl an Nutzer*innen, die wiederum den Einfluss dieser Netzwerke stärkt und eine Nichtnutzung der Netzwerke für einzelne Nutzer*innen erschwert. Diese sog. „Privacy Externality“ kann zudem dazu führen, dass das gesellschaftliche Bedürfnis nach mehr Datenschutz verschwindet und Konsument*innen, die ein verstärktes Interesse an der Sicherung ihrer Daten haben, immer mehr Zeit und Geld dafür aufbringen müssen (Acquisti et al. 2016).

Aufgrund dieser Entwicklungen sollten sich Konsument*innen ihr Recht auf informelle Selbstbestimmung und ihre Verantwortung für die Verwendung ihrer Daten bewusstmachen (Trabandt und Lasarov 2020). Tatsächlich existieren in Deutschland einige Initiativen, die Konsument*innen in solchen Vorhaben unterstützen, u. a. indem sie zahlreiche Informationsangebote bereitstellen (z. B. Selbstdatenschutz.info 2020; datenschutz.rlp.de 2020; bfdi.bund.de 2020). Zudem geben Konsument*innen oft an, dass sie insgesamt auf ihre Privatsphäre achten und möglichst oft kontrollieren, welche persönlichen Daten sie preisgeben. Allerdings legen Beobachtungen aus Forschung und Praxis nahe, dass das Wissen über datenschutzrelevante Themen (z. B. Instrumente zum Schutz persönlicher Daten, Wissen über die Konsequenzen bei Missbrauch) und eine allgemein positive Einstellung zum Datenschutz in vielen konkreten Situationen dennoch wirkungslos sind und von den Konsument*innen nicht in konkretes Verhalten umgesetzt werden (Acquisti et al. 2015, 2020; Martin und Murphy 2017). So gehen selbst jene Konsument*innen in manchen Situationen nachlässig mit dem Schutz ihrer persönlichen Daten um, die im Allgemeinen besorgt um ihre Datensicherheit sind (Acquisti et al. 2015).

Vor diesem Hintergrund führt der vorliegende Beitrag zunächst in das Privatsphäre-Paradoxon ein und zeigt anschließend den Stand des Schrifttums auf, wobei insbesondere auf situative und kognitive Verzerrungen fokussiert wird, welche zur Erklärung der Diskrepanz zwischen den persönlichen Datenschutzbedenken und dem tatsächlichen, oft sorglosen Verhalten bei digitalen Dienstleistungen beitragen können. Abschließend wird mit dem Konzept der drei Privatsphären-Gaps ein Rahmen für die zukünftige Forschung entwickelt.

2 Das „Privatsphäre-Paradoxon“

Zahlreiche Studien zum Datenschutzverhalten drehen sich um die oben beschriebene Beobachtung, dass sich Konsument*innen oftmals besorgt um ihre Datensicherheit zeigen, diese Sorge sich allerdings in vielen Situationen nicht in konkretem Handeln ausdrückt. Diese Beobachtung ist in der Literatur auch als sog. Privatsphäre-Paradoxon (engl. „Privacy Paradox“) bekannt und beschreibt die Diskrepanz zwischen allgemeinen (positiven) Einstellungen von Konsument*innen zum Datenschutz und ihrem tatsächlichen (nachlässigen) Verhalten (Aguirre et al. 2015; Norberg et al. 2007). Diese Einstellungs-Verhaltens-Diskrepanz lässt sich einerseits durch ein rationales Kosten-Nutzen-Kalkül erklären, in dem Konsument*innen den Nutzen bestimmter Produkte und Dienstleistungen (z. B. durch Personalisierung) mit der Preisgabe ihrer Daten gegenrechnen. Eine rationale Erklärung hierfür liefert die Theorie der rationalen Entscheidung (Behavioral Decision Theory, Kahneman 2003), nach der Konsument*innen ihre Entscheidungen in komplexen, unsicheren und risikobehafteten Situationen auf ein rationales Kosten-Nutzen-Kalkül stützen, also in unserem Fall den Nutzen eines Produkts, der mit der Personalisierung einhergeht, gegen die damit verbundenen Kosten bei der Preisgabe persönlicher Daten abwägen (Aguirre et al. 2015; Dinev und Hart 2004; Mothersbaugh et al. 2012). Andererseits können situative Einflüsse oder kognitive Verzerrungen individuelle Datenschutzbedenken in bestimmten Situationen verringern. Zu diesen psychologischen Verzerrungen zählen bspw. Gewöhnungseffekte (Adjerid et al. 2018; Melumad und Meyer 2020), der Einfluss der sozialen Umwelt (Acquisti et al. 2012; Carbone und Loewenstein 2020; Chellappa und Sin 2005; Schumann et al. 2014; White 2004) oder die Illusion der vollständigen Kontrolle über die Preisgabe der eigenen Daten (Acquisti et al. 2013; Bleier und Eisenbeiss 2015a, b; Martin et al. 2016; Mothersbaugh et al. 2012; Tucker 2014; Xu et al. 2012).

Aus angrenzenden Forschungsgebieten (z. B. nachhaltigem Konsumentenverhalten, White et al. 2019) ist die Lücke zwischen selbst berichteten allgemeinen Einstellungen und dem Verhalten in konkreten Situationen bekannt (Webb and Sheeran 2006). Allerdings vermittelt der Terminus „Paradoxon“ für diese Einstellungs-Verhaltens-Lücke einen missverständlichen Eindruck, da hinsichtlich digitaler Dienstleistungen durchaus der Fall eintreten kann, dass aus Sicht der Konsument*innen der aus der Datenabgabe gewonnene Nutzen die damit verbundenen Kosten übersteigt und ein scheinbar nachlässiges Verhalten nicht paradox, sondern rational ist. Selbst strikte Einstellungen zum Datenschutz stehen nicht im Widerspruch zu einem freizügigen Umgang mit Daten in bestimmten Situationen, wenn andere Bedürfnisse ungleich wichtiger sind (z. B. in medizinischen Notfällen). Daher wird besonders in jüngster Zeit zunehmend in Frage gestellt, ob das Paradoxon in dieser Form auf der individuellen Ebene überhaupt existiert (Norberg et al. 2007; Solove 2011; Solove und Schwartz 2020). Angesichts möglicher langfristiger negativer Effekte und der immensen Bedeutung für Gesellschaft und Wirtschaft, sollte die Debatte über das Privatsphäre-Paradoxon nichtsdestotrotz fortgesetzt werden (Martin 2020). Zudem lassen sich zahlreiche paradoxe Verhaltensweisen nicht einfach auf rationale Kosten-Nutzen-Abwägungen zurückführen, weil es vorkommt, dass Konsument*innen unverhältnismäßig viele persönliche Daten preisgeben, ohne eine nennenswerte Ge-

genleistung oder einen subjektiven Nutzen zu erwarten. Mehrere psychologische Modelle helfen, dieses paradoxe Verhalten zu erklären. Die zentralen Faktoren sollen im Folgenden anhand der vorliegenden Literatur diskutiert werden.

3 Überblick über die Literatur

Zahlreiche Studien aus den Gebieten Psychologie, Verhaltensökonomie sowie Konsumentenverhaltensforschung beschäftigten sich in den vergangenen Jahren mit den psychologischen Einflussfaktoren auf datenschutzrelevantes Verhalten von Konsument*innen. Diese Faktoren erweitern das rationale Kosten-Nutzen Kalkül um situative und kontextuale Einflüsse bis hin zu emotionalen und irrationalen Entscheidungen (Acquisti et al. 2020). Tab. 1 fasst die einschlägigen konzeptionellen und empirischen Studien der vergangenen Jahre zusammen. Die Tabelle umfasst eine Kurzbeschreibung der jeweiligen psychologischen Einflussfaktoren und der datenschutzrelevanten Verhaltenskonsequenzen auf und verweist auf die einschlägige Literatur dazu.

Im weiteren Verlauf gehen wir zunächst auf Studien zu den verhaltensrelevanten Konsequenzen ein. Bisherige Studien befassten sich im Wesentlichen mit zwei Verhaltenskonsequenzen. Zum einen wurde untersucht, inwiefern datenschutzrelevante Faktoren die Konsumbereitschaft für ein bestimmtes Produkt beeinflussen. Zum anderen wurde erforscht, in welchem Ausmaß (wie viel, an wen, etc.) Konsument*innen ihre persönlichen Daten preisgeben. Mit Blick auf die Einflussfaktoren betrachten wir den persönlichen Nutzen, der durch die Nutzung digitaler Dienstleistungen entstehen würde, sowie die Datenschutzbedenken und die angestrebte Privatsphäre der Nutzer*innen. Diese fließen in das Kosten-Nutzen-Kalkül der Konsument*innen ein. Das Kernstück des Literaturüberblicks betrifft Erkenntnisse zu situativen und kognitiven Verzerrungen bei der Abwägung des Nutzens und der Datenschutzbedenken.

3.1 Verhaltenskonsequenzen

Sicherung der Privatsphäre. Zunächst unterscheiden sich Konsument*innen hinsichtlich ihrer Bereitschaft, persönliche Daten in bestimmten Situationen preiszugeben. Die Menge der bereitgestellten persönlichen Daten kann wiederum die Nutzungsqualität digitaler Produkte und Dienstleistungen beträchtlich beeinflussen, z. B. in sozialen Netzwerken. Ein typisches Anwendungsbeispiel ist auch die Nutzung von Smart Home Objekten, deren sinnvoller Einsatz nur durch die Verarbeitung persönlicher Daten möglich ist (z. B. passives Mithören intelligenter Lautsprecher eines sprachgesteuerten, internetbasierten Assistenten) (Adjerid et al. 2018; Carbone und Loewenstein 2020; Acquisti et al. 2012; Brandimarte et al. 2012, 2013; Goldfarb und Tucker 2012; John et al. 2011; Mothersbaugh et al. 2012; Wirtz und Lwin 2009).

Nutzung digitaler Produkte oder Dienstleistungen. Mit Blick auf die Nutzung digitaler Dienstleistungen wird in der Literatur oftmals die gesamte Customer Journey, d. h. auch Prozesse der Informationsbeschaffung, des Kaufs von Produkten und Dienstleistungen, sowie deren Weiterempfehlung betrachtet. So eruierten Untersu-

Tab. 1 Tabellarischer Literaturüberblick

Thema	Kurzbeschreibung	Literatur
Verhaltenskonsequenzen		
Sicherung der Privatsphäre	Bereitschaft von Konsument*innen, ihre persönlichen Daten in bestimmten Situationen preiszugeben	Acquisti et al. 2012; Adjerid et al. 2018; Brandimarte et al. 2012, 2013; Carbone and Loewenstein 2020; Goldfarb und Tucker 2012; John et al. 2011; Mothersbaugh et al. 2012; Wirtz und Lwin 2009
Konsum digitaler Produkte oder Dienstleistungen	Dem Kauf vorgelagertes Interesse an weiteren Informationen oder einem möglichen Erwerb eines Produktes oder einer Dienstleistung	Aguirre et al. 2015; Bleier und Eisenbeiss 2015a; Schumann et al. 2014; Tucker 2014
	Erwerb eines digitalen Produktes oder einer Dienstleistung	Goldfarb und Tucker 2011a, b; Tsai et al. 2011; Miyazaki 2008
	Positive oder negative Empfehlungen eines Produktes oder einer Dienstleistung oder des anbietenden Unternehmens von Konsument*innen an andere Konsument*innen	Miyazaki 2008
Kosten-Nutzen-Kalkül		
Persönlicher Nutzen	Der wahrgenommene Nutzen eines Produktes oder einer Dienstleistung beeinflusst datenschutzrelevantes Verhalten von Konsument*innen	Aguirre et al. 2015; Awad und Krishnan 2006; Bleier und Eisenbeiss 2015a; Gabisch und Milne 2014; Goldfarb und Tucker 2011a, b; Lasarov 2020; Mothersbaugh et al. 2012; Norberg und Horne 2007; Tucker 2014; White et al. 2008
Datenschutzbedenken	Allgemeine und situative Bedenken von Konsument*innen gegen den Umgang mit ihren personenbezogenen Daten beeinflussen datenschutzrelevantes Verhalten von Konsument*innen	Aguirre et al. 2015; Acquisti et al. 2015; Goldfarb und Tucker 2012; Malhotra et al. 2004; Martin 2015; Sheehan und Hoy 2000; Smith et al. 1996; Xu et al. 2012
Situative und kognitive Verzerrungen		
Informationsasymmetrien	Wissensnachteile von Konsument*innen gegenüber Unternehmen und Institutionen, z. B. wie und von wem ihre Daten gesammelt und verarbeitet werden	Martin und Nissenbaum 2016; Habib et al. 2018; Acquisti et al. 2013; Mothersbaugh et al. 2012; Hoofnagle und Urban 2014; Martin 2015; Vail et al. 2008
Vertrauen und Transparenz	Vertrauen von Konsument*innen in Organisationen; ist besonders beeinflusst durch Glaubwürdigkeit und Transparenz von Organisationen	Gabisch und Milne 2014; Martin und Murphy 2017; Lasarov 2020; Lockamy und Mothersbaugh 2020; Malhotra und Malhotra 2011; Martin et al. 2016; Norberg und Horne 2014; PWC 2020; Romanosky et al. 2014; White 2004; Wirtz und Lwin 2009
Kontrollillusion	Die wahrgenommene Kontrolle über die eigenen Daten kann dazu führen, dass diese durch Konsument*innen leichtfertiger geteilt werden	Acquisti et al. 2013; Barassi 2019; Bleier und Eisenbeiss 2015a, 2015b; Brandimarte et al. 2012, 2013; Draper und Turow 2019; Martin et al. 2016; Mothersbaugh et al. 2012; Schouten et al. 2008; Tsai et al. 2011; Tucker 2014; Xu et al. 2012

Tab. 1 (Fortsetzung)

Thema	Kurzbeschreibung	Literatur
Soziale Umwelt	Die soziale Umwelt kann einerseits als Referenz für das „richtige" Verhalten dienen, andererseits durch Erwartungen Entscheidungen von Konsument*innen beeinflussen	Acquisti et al. 2012; Carbone und Loewenstein 2020; Chellappa und Sin 2005; Schumann et al. 2014; White 2004
Habituation	Der Umgang von Konsument*innen mit ihren persönlichen Daten hängt davon ab, wie sehr sie sich an bestimmte Gegebenheiten und Situationen gewöhnen	Adjerid et al. 2018; Melumad und Meyer 2020
Wahrgenommene Vulnerabilität	Das von Konsument*innen wahrgenommene potenzielle Risiko, das mit der Offenlegung persönlicher Daten einhergeht	Aguirre et al. 2015; Awad und Krishnan 2006; Dinev und Hart 2004; Petronio 2002; Martin und Murphy 2017; Raab und Bennet 1998

chungen zur Akzeptanz personalisierter Angebote u. a. das dem Kauf vorgelagerte Interesse an weiteren Informationen oder den möglichen Erwerb des Produktes (Aguirre et al. 2015; Bleier and Eisenbeiss 2015a; Schumann et al. 2014; Tucker 2014). Häufig untersuchte Verhaltenskonsequenzen in diesem Kontext sind Click Through Rates (Aguirre et al. 2015; Bleier and Eisenbeiss 2015a; Tucker 2014), der Kauf des Produktes (Goldfarb und Tucker 2011a, b; Miyazaki 2008; Tsai et al. 2011) sowie die Weiterempfehlungsbereitschaft der Konsument*innen bzw. deren Bereitschaft, ihre negative Meinung über das Produktmit anderen zu teilen (word-of-mouth). Miyazaki (2008) zeigt beispielsweise, dass der verdeckte Einsatz von Technologien zur Sammlung von Daten (z. B. Cookies) zu negativer Mundpropaganda führen kann.

3.2 Kosten-Nutzen-Kalkül

Persönlicher Nutzen durch Nutzung digitaler Produkte oder Dienstleistungen. Konsument*innen wägen in datensensiblen Situationen oft den Nutzen ab, den sie mit der Preisgabe ihrer persönlichen Daten „bezahlen". Studien bestätigen dementsprechend, dass Menschen anders mit dem Schutz ihrer persönlichen Daten umgehen, wenn sie ein bestimmtes Produkt als nützlich erachten (Aguirre et al. 2015; Awad und Krishnan 2006; Bleier und Eisenbeiss 2015a; Gabisch und Milne 2014; Goldfarb und Tucker 2011a, b; Lasarov 2020; Mothersbaugh et al. 2012; Tucker 2014; White et al. 2008). White et al. (2008) zeigen bspw., dass ein hoher Nutzen eines Produktes zu geringeren Sorgen bei der damit verbundenen Offenlegung der Privatsphäre führt. Dieser Nutzen kann einerseits monetär sein: Gabisch and Milne (2014) zeigen, dass Nutzer*innen eher zur Offenlegung ihrer Daten bereit sind, wenn damit finanzielle Anreize verbunden sind. Andererseits kann der Nutzen auch andere persönliche Interessen betreffen, bspw. gesundheitliche Interessen bei der Nutzung der Corona Warn-App (Dehmel et al. 2020; Lasarov 2020). Darüber hinaus kann eine erhöhte Personalisierung und das individualisierte Maßschneidern von Produkten

und Dienstleistungen als sehr nützlich erachtet werden. Gabisch und Milne (2014) untersuchen bspw., ob bei Konsument*innen das Gefühl entsteht, dass sie durch die Personalisierung von Dienstleistungen und Online-Produkten genügend Nutzen erfahren, der die Offenlegung ihrer persönlichen Daten rechtfertigt. Ein hohes Maß an Personalisierung kann aber auch Misstrauen gegenüber dem Unternehmen und Reaktanz auslösen, was die Nutzung der Produkte des Unternehmens wiederum verringert (White et al. 2008). Auch hier ist dementsprechend ein paradoxer Effekt sichtbar, da Personalisierung einerseits den Nutzen erhöht, andererseits aber auch Reaktanz und Misstrauen auslösen kann.

Datenschutzbedenken. Die allgemeinen und situativen Bedenken gegen den Umgang mit ihren personenbezogenen Daten beeinflussen das Verhalten von Konsument*innen in datenschutzrelevanten Situationen maßgeblich (Aguirre et al. 2015; Acquisti et al. 2015; Goldfarb und Tucker 2012; Martin 2015; Sheehan und Hoy 2000). Die allgemeinen Datenschutzbedenken beziehen sich auf Überzeugungen, Einstellungen und Wahrnehmungen der Konsument*innen zu ihrer Privatsphäre (Smith et al. 1996). In der Forschung werden diese oftmals mit der sog. „consumer privacy concern scale“ erfasst (Smith et al. 1996; Malhotra et al. 2004). In der bisherigen Literatur wurden Datenschutzbedenken sowohl als Prädiktoren, aber auch als Moderatoren und datenschutzrelevante Konsequenzen untersucht (Xu et al. 2012).

3.3 Situative und kognitive Verzerrungen

Situative und kognitive Verzerrungen beschreiben Einflussfaktoren, die die konkreten datenschutzrelevanten Handlungen von Konsument*innen über rationale Kosten-Nutzen-Abwägungen hinaus beeinflussen und zu Abweichungen von ihren eigentlichen (allgemeinen) Einstellungen, Überzeugungen und Intentionen führen. Dies können die Anwendungsumgebung (z. B. die genutzte technologische Plattform, Melumad und Meyer 2020) oder auch Emotionen (Dowling et al. 2020) sein. Die bisherigen Studien betrachteten unter anderem Informationsasymmetrien, Vertrauen und Transparenz, Kontrollillusionen, die soziale Umwelt, Habituation sowie die wahrgenommene Vulnerabilität.

Informationsasymmetrien. Konsument*innen wissen häufig nicht, zu welchen Gelegenheiten, auf welche Arten und in welchem Umfang Unternehmen ihre Daten sammeln und verarbeiten und welche weiteren Dienste und Unternehmen ebenfalls Zugriff auf diese Daten haben. Der Hauptgrund hierfür liegt darin, dass den Konsument*innen zumeist die notwendigen (kognitiven, zeitlichen) Kapazitäten im Alltag fehlen oder sie nicht das notwendige technische oder juristische Hintergrundwissen besitzen, um bspw. komplexe Datenschutzbestimmungen zu verstehen. Diese sogenannten *Informationsasymmetrien* und die daraus entstehenden Folgen (z. B. Misstrauen gegenüber Unternehmen, geringe Kaufbereitschaft) lassen sich nur sehr schwer wieder abbauen (Acquisti et al. 2013; Habib et al. 2018; Hoofnagle und Urban 2014; Martin und Nissenbaum 2016; Mothersbaugh et al. 2012; Martin 2015). So kann die bloße Benachrichtigung über die Datenschutzrichtlinien des Unternehmens nicht zwangsläufig verhindern, dass Konsument*innen Informationsasymmetrien wahrnehmen und den Datenschutz kritisch sehen (Martin 2015). Darüber

hinaus spielt es eine Rolle, wie datenschutzrelevante Informationen durch Unternehmen an die Konsument*innen vermittelt werden. Vail et al. (2008) zeigen bspw., dass „traditionelle“ und ausführliche Datenschutzrichtlinien von Konsument*innen eher als vertrauenswürdig angenommen werden, obwohl solche Richtlinien aufgrund ihrer Länge und Komplexität keine Informationsasymmetrien abbauen. Somit kann eine Maßnahme, die eher nachteilig für die Verringerung der Informationsasymmetrien ist, paradoxerweise das Vertrauen der Konsument*innen in das Unternehmen erhöhen.

Vertrauen und Transparenz. Das Vertrauen in Organisationen kann maßgeblich beeinflussen, inwieweit Konsument*innen ihre persönlichen Daten mit diesen teilen (Martin und Murphy 2017). Hierbei wurde in der Literatur besonders eine glaubwürdige und transparente Datenschutzpolitik als vertrauensbildender Erfolgsfaktor untersucht. So kann eine glaubwürdige Datenschutzpolitik des Unternehmens das Vertrauen von Konsument*innen stärken (Lockamy und Mothersbaugh 2020), z. B. durch unabhängige Datenschutzsiegel und freiwillige Angaben zum Datenschutz (Gabisch und Milne 2014; White 2004). Mit einem hohen Vertrauen geht allerdings auch eine erhöhte Erwartungshaltung der Konsument*innen an die Datensicherheit der Unternehmen einher, deren Nichterfüllung sich negativ auf das Verhältnis zwischen Konsument*innen und Unternehmen auswirken können (Martin 2015; Gabisch and Milne 2014). So kann ein nachlässiger Umgang mit den Kundendaten zu einem Glaubwürdigkeitsverlust von Unternehmen führen und bedeutende negative finanzielle und juristische Konsequenzen nach sich ziehen (Malhotra und Malhotra 2011; Romanosky et al. 2014). Andererseits kann ein transparenter Umgang des Unternehmens mit den verwendeten Daten das Vertrauen der Konsument*innen stärken (Martin et al. 2016; Norberg und Horne 2014; Wirtz und Lwin 2009).

Kontrollillusion. Die wahrgenommene Kontrolle der Konsument*innen über die eigenen Daten gilt als bedeutende Einflussgröße auf deren Verhalten in datensensiblen Situationen (Acquisti et al. 2013; Bleier und Eisenbeiss 2015a, b; Martin et al. 2016; Mothersbaugh et al. 2012; Tucker 2014; Xu et al. 2012). Einerseits kann das Gefühl von Kontrolle bei Konsument*innen Reaktanz und Datenschutzbedenken gegenüber dem Unternehmen abbauen (Acquisti et al. 2020) und damit das Verhältnis von Konsument*innen zu den Unternehmen verbessern (Tsai et al. 2011). Allerdings kann die wahrgenommene Kontrolle auch einen paradoxen Effekt auslösen, der in der Literatur als sog. Kontrollparadoxon eingeführt wurde (Brandimarte et al. 2013): Die wahrgenommene Kontrolle über die eigenen Daten führt dazu, dass diese durch Konsument*innen leichtfertiger offengelegt werden (Brandimarte et al. 2012, 2013; Norberg und Horne 2014). Im Hinblick auf die Kontrolle über die eigenen Daten, kann auch eine gegenteilige Wahrnehmung entstehen, nämlich das Gefühl der Resignation. Konsument*innen fühlen sich in dem Fall hilflos und machtlos und sind überzeugt, dass sie ihre Daten ohnehin nicht schützen können oder dass sie als aktive Bürger*innen in einer modernen Welt nicht ohne digitale Teilhabe bestehen können (Acquisti et al. 2020; Barassi 2019; Draper und Turow 2019). Ironischerweise können sowohl die Wahrnehmung von Kontrolle als auch Resignation dieselbe Konsequenz haben: Konsument*innen gehen nachlässig mit ihren persönlichen Daten um. Des Weiteren ist in diesem Zusammenhang das „Nichts-zu-verbergen-Argument“ zu beobachten, das besagt, dass staatliche Maßnahmen zur

Überwachung illegaler Aktivitäten dienen und daher keine Personen beeinträchtigt werden, die sich regelkonform verhalten (Solove 2011). Hier kann das Gefühl vermeintlicher Kontrolle schlicht durch die Einhaltung von Gesetzen entstehen, obwohl Maßnahmen zur Überwachung in vielen Fällen unabhängig von Verdachtsfällen geschehen.

Soziale Umwelt. Die soziale Umwelt spielt in zweierlei Hinsicht eine bedeutende Rolle für den Umgang von Konsument*innen mit ihren persönlichen Daten. Einerseits dient die soziale Umwelt oftmals als Referenz für das „richtige" Verhalten in bestimmten Situationen und unterstützt Konsument*innen dabei, die ihre Einstellungen zu einem bestimmten Thema zu ermitteln. Tatsächlich konnten Studien bestätigen, dass Konsument*innen bei der Nutzung einer bestimmten Technologie eher ihre persönlichen Daten preisgeben, wenn sie dieses Verhalten bereits bei anderen beobachtet haben (Acquisti et al. 2012). Darüber hinaus können Konsument*innen in ihren datenschutzrelevanten Entscheidungen durch soziale Normen, Herdenverhalten sowie dem Vertrauen in andere Nutzer*innen von Plattformen und Reziprozitätsgedanken beeinflusst werden (Acquisti et al. 2012; Chellappa und Sin 2005; Schumann et al. 2014; White 2004). Schließlich kann auch das Bedürfnis nach dem Teilen persönlicher Informationen mit anderen Menschen maßgeblich beeinflussen, wie stark Konsument*innen auf Datenschutzaspekte achten (Carbone und Loewenstein 2020).

Habituation. Der Umgang von Konsument*innen mit ihren persönlichen Daten hängt nicht zuletzt davon ab, wie sehr sie sich an bestimmte Gegebenheiten und Situationen gewöhnen. So können datenschutzrelevante Probleme zwar in einer bestimmten Situation oder für einen bestimmten Zeitraum im Fokus der Aufmerksamkeit stehen (z. B. wenn ein Datenschutzskandal in den Medien aufbereitet wird), allerdings treten im Zeitverlauf andere Themen in den Vordergrund, während die datenschutzrelevanten Probleme ungelöst bleiben oder sich sogar unbemerkt weiterhin nachteilig für die Konsument*innen entwickeln (z. B. durch Agenda Setting). Dies führt u. a. dazu, dass sich Konsument*innen selbst an Umstände gewöhnen, die ihnen eigentlich schaden könnten (Adjerid et al. 2018). Darüber hinaus kann auch die genutzte technologische Plattform zu Gewöhnungseffekten führen und den Umgang mit den persönlichen Daten beeinflussen. So zeigen Melumad und Meyer (2020), dass Konsument*innen eher Persönliches auf sozialen Netzwerken teilen, wenn sie ein Smartphone statt eines PCs nutzen.

Wahrgenommene Vulnerabilität. Das Konzept der wahrgenommenen Vulnerabilität bzw. Verwundbarkeit beschreibt das von Konsument*innen wahrgenommene potenzielle Risiko, das mit der Offenlegung persönlicher Daten einhergeht (Aguirre et al. 2015; Awad und Krishnan 2006; Raab und Bennet 1998). Die wahrgenommene Verwundbarkeit entspringt der individuellen Befürchtung, dass andere (z. B. Unternehmen, Staaten, Betrüger) die Absicht hegen könnten, die persönlichen Daten von Konsument*innen zu deren Nachteil zu nutzen. Die jüngste Literatur, die sich der wahrgenommenen Verwundbarkeit intensiv gewidmet hat (Aguirre et al. 2015; Awad und Krishnan 2006; Martin und Murphy 2017), konnte nachweisen, dass diese einen beträchtlichen Einfluss darauf hat, wie Konsument*innen ihre eigene Privatsphäre erleben und beurteilen (Petronio 2002). Schließlich beeinflusst die wahrgenommene Verwundbarkeit subjektive Datenschutzbedenken (Dinev und Hart 2004).

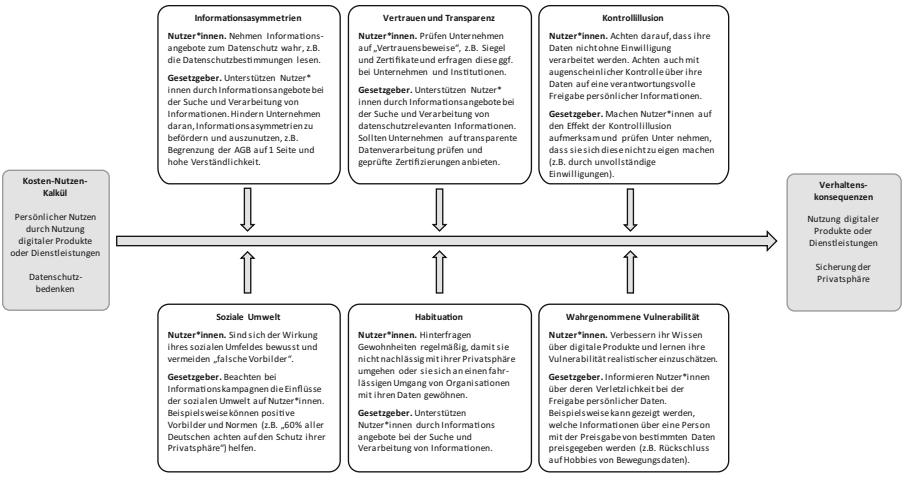

Abb. 1 Handlungsempfehlungen für Nutzer*innen und Gesetzgeber

4 Handlungsempfehlungen für Nutzer*innen und Gesetzgeber

Aus dem vorliegenden Beitrag wird klar, dass wichtige Dimensionen der digitalen Datenschutzkompetenz das Verständnis der Nutzer*innen für die tatsächliche Kontrolle über deren persönliche Daten, soziale Einflüsse, Habituationen und Vulnerabilität und Informationen sind. Auf Seiten des Gesetzgebers könnte man übergeordnet davon sprechen, dass neben rechtlichen Rahmenbedingungen und Standards sowie Kontrolle der Anbieter auch Maßnahmen zur Steigerung der digitalen Datenschutzkompetenz wichtig sind (Informations- und Bildungsangebote). Basierend auf diesen Überlegungen gestalten sich zahlreiche Möglichkeiten, um einen sicheren und verantwortungsvollen Umgang der Nutzer*innen mit den eigenen Daten zu fördern. Gesetzgeber, Verbraucherschutzorganisationen und öffentliche Institutionen können bspw. Unternehmen gesetzlich verpflichten oder dazu motivieren, ihre Kund*innen zu einem verantwortungsvollen Umgang mit persönlichen Daten zu unterstützen. Eine Darstellung von Handlungsoptionen für Konsument*innen und Gesetzgeber werden in Abb. 1 dargestellt.

5 Die Untersuchung der drei Privatsphäre-Gaps als Forschungsagenda

Der Literaturüberblick verdeutlicht, dass bereits zahlreiche Studien datenschutzrelevante Aspekte im Konsumentenverhalten untersuchten. Es wurde deutlich, dass die konsumentenpsychologische Forschung nützliche konzeptionelle Vorarbeit geleistet hat, die in zukünftigen empirischen Studien vertieft werden sollte. Bislang existiert allerdings noch kein Modell, das zeigt, wie verschiedene datenschutzrelevante Konsumentenreaktionen zueinander stehen und wie sich die aufgeführten Prozesse gegenseitig beeinflussen und die Reaktionen auslösen. Darüber hinaus wurden die verschiedenen Arten von Konsumentenreaktionen in datenschutzrelevanten Si-

tuationen nicht systematisch untersucht, obwohl diese Reaktionen paradoxerweise gegenläufige Effekte annehmen können: So kann beispielsweise das Gefühl von Kontrolle über die eigenen Daten einen positiven Effekt auf das Vertrauen gegenüber Unternehmen ausüben und sich in einer positiven Kaufabsicht und der bereitwilligen Preisgabe sensibler Daten widerspiegeln. Allerdings kann dieses Vertrauen auch zu einer Nachlässigkeit im Umgang mit den eigenen Daten führen. So kann ironischerweise das Gefühl von Kontrolle zu einem Kontrollverlust über die Daten führen.

Für eine spezifischere Untersuchung datenschutzrelevanter Aspekte im Konsumverhalten erscheint eine Abgrenzung der erstrebenswerten, erstrebten und erreichbaren Privatsphäre besonders fruchtbar (vgl. Abb. 2). Die *subjektiv erstrebenswerte Privatsphäre* kennzeichnet das Maß an Privatsphäre, das aus individuellen, politischen oder sozialen Norm- und Zielvorstellungen resultiert. Besonders die individuellen Normvorstellungen sind hierbei aus unserer Perspektive wichtig, da sich diese einerseits aus tiefergehenden Einstellungen speisen, andererseits auch aus dem Verhalten in anderen datenschutzrelevanten Bereichen. Unter der *erstrebten Privatsphäre* verstehen wir den Grad an Privatsphäre, den Konsument*innen allgemein oder in bestimmten Situationen anstreben. Er kann von verschiedenen Faktoren beeinflusst werden, die schon empirisch untersucht wurden und in diesem Artikel diskutiert wurden. Schließlich beschreibt die *subjektiv erreichbare Privatsphäre* das individuell wahrgenommene Maß an Privatsphäre, das allgemein oder in einer bestimmten Situation erreicht werden kann. Es ist stark abhängig vom Informationsstand der Konsument*innen.

Auf Basis der berichteten Literatur und diesen drei zu unterscheidenden Formen der Privatsphäre ergibt sich folgende übergeordnete Fragestellung, die in zukünftiger Forschung untersucht werden sollte: Welche situativen und kognitiven Verzerrungen erklären die Abweichungen zwischen erstrebenswerter, erstrebter und erreichbarer Privatsphäre von Konsument*innen sowie ihr datenschutzrelevantes Verhalten in konkreten Situationen? Für staatliche Institutionen ergibt sich die praktische Fragestellung, durch welche individuellen verhaltenswissenschaftlichen Interventionen und Bildungsmaßnahmen diese Lücken geschlossen werden können. Konkret ergibt sich Forschungsbedarf zu den folgenden drei Gaps der Privatsphäre bei digitalen Dienstleistungen.

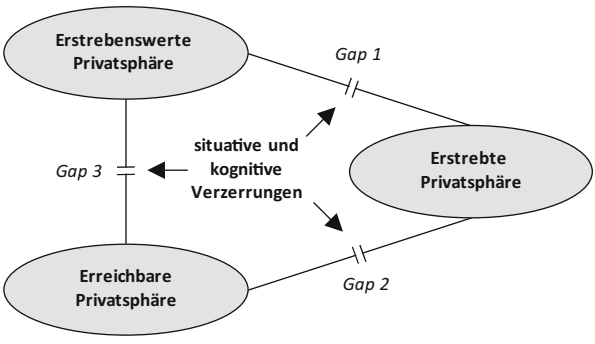

Abb. 2 Drei Privatsphären-Gaps als Rahmen für zukünftige Forschung

5.1 Gap 1: Diskrepanz zwischen erstrebenswerter und erstrebter Privatsphäre

Zunächst sollte untersucht werden, wieso Konsument*innen für verschiedene Anwendungen sowie in verschiedenen Kontexten und Situationen unterschiedliche Maßstäbe an den Datenschutz anlegen. Ein geeignetes Beispiel ist der Unterschied im Umgang mit Datenschutzbedenken einiger Konsument*innen zwischen der Corona Warn-App und sozialen Netzwerken (Lasarov 2020). So lehnten im Zuge der Einführung der Corona Warn-App in Deutschland zahlreiche Konsument*innen eine Nutzung aus Gründen des Datenschutzes ab, teilten diese Meinung aber auf sozialen Netzwerken (z. B. Facebook, WhatsApp) (Lasarov 2020). Paradox an dieser Situation ist, dass Konsument*innen das erstrebte Maß an Privatsphäre für unterschiedliche Anwendungen inkonsistent beurteilten: für die sinnvolle Teilhabe an sozialen Netzwerken wird die Offenlegung zahlreicher privater Daten in Kauf genommen, während die Anforderungen an die Warn-App sehr hoch waren. Es kommt hinzu, dass der gesellschaftliche Nutzen der Corona Warn-App von zahlreichen Expert*innen und in den Medien als sehr hoch beurteilt wurde. Eine potenzielle Erklärung ergibt sich aus dem Ethical Intuitionism Model, wonach ein moralisches Urteil der rationalen Begründung vorgelagert ist. Eine höhere Bewertung des Datenschutzes kann also auch die nachgelagerte Rationalisierung dafür sein, wieso man das dafür genutzte Produkt ablehnt. Ferner ist auf normativer Ebene zu klären, welches Maß an Privatsphäre überhaupt „gut“ ist. Die Forschung zum Datenschutz konnte bisher bestätigen, dass ein hohes Maß an Privatsphäre mit einer Erhöhung der gesellschaftlichen Wohlfahrt verbunden ist (Acquisti et al. 2016; 2020; Varian 1996). Jedoch fehlen bislang Studien, die diese Lücke empirisch schließen.

5.2 Gap 2: Diskrepanz zwischen erstrebter und erreichbarer Privatsphäre

Die erstrebte Privatsphäre kann auch von der erreichbaren Privatsphäre abweichen. Diese Lücke wurde in der bisherigen Forschung besonders aus der Perspektive des Privatsphäre-Paradoxon untersucht, da Konsument*innen nicht in allen Situationen das höchstmögliche Maß an Privatsphäre suchen, sondern sich mit einem Maß an Privatsphäre zufriedengeben, das ihnen das gewünschte Maß an gesellschaftlicher Teilhabe ermöglicht (sog. Privatsphäre-Externalität) und auch der Verfolgung anderer persönlicher Interessen nicht im Wege steht (sog. Privacy-Personalization-Paradox). Auch hier ist weitere Forschung notwendig, die sich mit der spezifischen Entschlüsselung der Verzerrungen befasst.

5.3 Gap 3: Diskrepanz zwischen erstrebenswerter und erreichbarer Privatsphäre

In einigen Situationen können auch die erreichbare und die erstrebenswerte Privatsphäre divergieren. Sollte die erreichbare Privatsphäre deutlich hinter der erstrebenswerten Privatsphäre zurückfallen, entstehen mentale Konflikte. Gewährleistet beispielsweise ein Unternehmen wenig Datenschutz für ein bestimmtes Produkt (niedrige erreichbare Privatsphäre) in einem Bereich, bei dem Privatsphäre als sehr erstrebenswert gilt (hohe erstrebenswerte Privatsphäre, z. B. Gesundheit), entstehen

bei Konsument*innen derartige Dissonanzen. Äußere Faktoren beeinflussen die Strategien, mit deren Hilfe Konsument*innen diese kognitiven Dissonanzen reduzieren können. Konsument*innen könnten bspw. das erstrebenswerte Maß an Privatsphäre (oder die Bedeutung von Privatsphäre insgesamt) für sich verringern, wenn sie das angebotene Produkt unbedingt möchten. Sie können allerdings auch das Produkt durch ein Substitut ersetzen oder zu einem anderen Anbieter wechseln, das bzw. der ihnen ein höheres Maß an erreichbarer Privatsphäre bietet. Außerdem können sie in bestimmten Fällen auch die erreichbare Privatsphäre im selben Unternehmen erhöhen, z. B. kurzfristig durch Extra-Zahlungen.

6 Fazit

Der vorliegende Artikel diskutiert verschiedene situative und kognitive Verzerrungen, die zur Erklärung der Diskrepanz zwischen den persönlichen Datenschutzbedenken und dem tatsächlichen, oft sorglosen Verhalten bei digitalen Dienstleistungen beitragen. Es wird allerdings deutlich, dass bisher kein übergeordnetes Modell existiert, das die Wechselwirkungen zwischen diesen Verzerrungen sowie den datenschutzrelevanten Konsequenzen untersucht und dabei eine in unseren Augen wichtige Differenzierung zwischen erstrebenswerter, erstrebter und erreichbarer Privatsphäre einbezieht. Dieser Beitrag soll daher zukünftige Forschung auf diesem Gebiet stimulieren.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Acquisti A, John LK, Loewenstein G (2012) The impact of relative standards on the propensity to disclose. J Mark Res 49(2):160–174. https://doi.org/10.1509/jmr.09.0215

Acquisti A, John LK, Loewenstein G (2013) What Is Privacy Worth? The Journal of Legal Studies 42(2):249–274

Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and human behavior in the age of information. Science 347(6221):509–514. https://doi.org/10.1126/science.aaa1465

Acquisti A, Taylor C, Wagman L (2016) The economics of privacy. J Econ Lit 54(2):442–492. https://doi.org/10.1257/jel.54.2.442

Acquisti A, Adjerid I, Balebako R, Brandimarte L, Cranor LF, Komanduri S, Wang Y (2017) Nudges for privacy and security: understanding and assisting users' choices online. ACM Comput Surv 50(3):1–41. https://doi.org/10.1145/3054926
Acquisti A, Brandimarte L, Loewenstein G (2020) Secrets and likes: the drive for privacy and the difficulty of achieving it in the digital age. J Consum Psychol 30(4):736–758. https://doi.org/10.1002/jcpy.1191
Adjerid I, Pe'er E, Acquisti A (2018) Beyond the privacy paradox: objective versus relative risk in privacy decision making. MIS Q 42(2):465–488. https://doi.org/10.25300/MISQ/2018/14316
Aguirre E, Mahr D, Grewel D, Ruyter KD, Wetzels M (2015) Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. J Retail 91(1):34–59. https://doi.org/10.1016/j.jretai.2014.09.005
Awad NF, Krishnan MS (2006) The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Q 30(1):13–28. https://doi.org/10.2307/25148715
Barassi V (2019) Datafied citizens in the age of coerced digital participation. Soc Res Online 24(3):414–429. https://doi.org/10.1177/1360780419857734
Bleier A, Eisenbeiss M (2015a) The importance of trust for personalized online advertising. J Retail 91(3):390–409. https://doi.org/10.1016/j.jretai.2015.04.001
Bleier A, Eisenbeiss M (2015b) Personalized online advertising effectiveness: the interplay of what, when, and where. Mark Sci 34(5):669–688. https://doi.org/10.1287/mksc.2015.0930
Brandimarte L, Acquisti A, Loewenstein G (2012) Misplaced Confidences. Social Psychological and Personality Science 4(3):340–347
Brandimarte L, Acquisti A, Loewenstein G (2013) Misplaced confidences: privacy and the control paradox. Soc Psychol Personal Sci 4(3):340–347. https://doi.org/10.1177/1948550612455931
Bundesministerium der Justiz und für Verbraucherschutz (2020) Corporate digital responsibility initiative. https://www.bmjv.de/DE/Themen/FokusThemen/ CDR_Initiative/CDR_Initiative_node.html. Zugegriffen: 29. Okt. 2020
Carbone E, Loewenstein G (2020) Dying to divulge: the determinants of, and relationship between, desired and actual disclosure. PsyArXiv. https://doi.org/10.31234/osf.io/wfdhx
Chellappa RK, Sin RG (2005) Personalization versus privacy: an empirical examination of the online consumer's dilemma. Inf Technol Manag 6(2–3):181–202. https://doi.org/10.1007/s10799-005-5879-y
Dehmel S, Kenning P, Wagner GG, Liedtke C, Micklitz HW, Riemenschneider L (2020) Die Wirksamkeit der Corona-Warn-App wird sich nur im Praxistest zeigen. Der Datenschutz ist nur eine von vielen Herausforderungen. Sachverständigenrat für Verbraucherfragen, Berlin, S 1–37
Dinev T, Hart P (2004) Internet privacy concerns and their antecedents-measurement validity and a regression model. Behav Inf Technol 23(6):413–422. https://doi.org/10.1080/01449290410001715723
Dowling K, Guhl D, Klapper D, Spann M, Stich L, Yegoryan N (2020) Behavioral biases in marketing. J of the Acad Mark Sci 48(1):1–29. https://doi.org/10.1007/s11747-019-00699-x
Draper NA, Turow J (2019) The corporate cultivation of digital resignation. New Media Soc 21(8):1824–1839. https://doi.org/10.1177/1461444819833331
Feng E (2019) How China is using facial recognition technology. NPR. https://www.npr.org/2019/12/16/788597818/how-china-is-using-facial-recognition-technology?t=1604482231208. Zugegriffen: 4. Nov. 2020
Gabisch JA, Milne GR (2014) The impact of compensation on information ownership and privacy control. J Consumer Mark 31(1):13–26. https://doi.org/10.1108/JCM-10-2013-0737
Goldfarb A, Tucker C (2011a) Online display advertising: targeting and obtrusiveness. Mark Sci 30(3):389–404. https://doi.org/10.1287/mksc.1100.0583
Goldfarb A, Tucker CE (2011b) Privacy regulation and online advertising. Manage Sci 57(1):57–71. https://doi.org/10.1287/mnsc.1100.1246
Goldfarb A, Tucker C (2012) Shifts in privacy concerns. Am Econ Rev 102(3):349–353. https://doi.org/10.1257/aer.102.3.349
Gray CM, Kou Y, Battles B, Hoggatt J, Toombs AL (2018) The dark (patterns) side of UX design. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, S 1–14 https://doi.org/10.1145/3173574.3174108
Habib H, Colnago J, Gopalakrishnan V, Pearman S, Thomas J, Acquisti A, Cranor LF (2018) Away from prying eyes: analyzing usage and understanding of private browsing. Fourteenth Symposium on Usable Privacy and Security, S 159–175
Hoofnagle CJ, Urban JM (2014) Alan Westin's privacy homo economicus. Wake For L Rev 49:261
John L, Acquisti A, Loewenstein G (2011) Strangers on a plane: context-dependent willingness to divulge sensitive information. J Consumer Res 37(5):858–873. https://doi.org/10.1086/656423

Kahneman D (2003) A perspective on judgement and choice: mapping bounded rationality. Am Psychol 58(9):697–720. https://doi.org/10.1037/0003-066X.58.9.697
Kannan PK (2017) Digital marketing: a framework, review and research agenda. Int J Res Mark 34(1):22–45. https://doi.org/10.1016/j.ijresmar.2016.11.006
Kumar V (2018) Transformative marketing: the next 20 years. J Mark 82(4):1–12. https://doi.org/10.1509/jm.82.41
Lasarov W (2020) Im Spannungsfeld zwischen Sicherheit und Freiheit. HMD. https://doi.org/10.1365/s40702-020-00646-3
Lobschat L, Mueller B, Eggers F, Brandimarte L, Diefenbach S, Kroschke M, Wirtz J (2020) Corporate digital responsibility. J Bus. https://doi.org/10.1016/j.jbusres.2019.10.006
Lockamy M, Mothersbaugh E (2020) PSYC 384 the effect of Instagram on appearance, self-esteem, and social approval. Longwood University, Longwood
Malhotra A, Malhotra CK (2011) Evaluating customer information breaches as service failures: an event study approach. J Serv Res 14(1):44–59. https://doi.org/10.1177/1094670510383409
Malhotra NK, Kim SS, Agarwal J (2004) Internet users' infor-mation privacy concerns: the construct, the scale, and a causal model. Inf Syst Res 15(4):336–355. https://doi.org/10.1287/isre.1040.0032
Martin K (2015) Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. J Public Policy &marketing 34(2):210–227. https://doi.org/10.1509/jppm.14.139
Martin K (2020) Breaking the privacy paradox: the value of privacy and associated duty of firms. Bus Ethics Q 30(1):65–96. https://doi.org/10.1017/beq.2019.24
Martin K, Nissenbaum H (2016) Measuring privacy: an empirical test using context to expose confounding variables. Columbia Sci Technol Law Rev 18:176
Martin KD, Murphy PE (2017) The role of data privacy in marketing. J of the Acad Mark Sci 45(2):135–155. https://doi.org/10.1007/s11747-016-0495-4
Martin KD, Borah A, Palmatier RW (2016) Data privacy: Effects on customer and firm performance. J Mark 81(1):36–58. https://doi.org/10.1509/jm.15.0497
Melumad S, Meyer R (2020) Full disclosure: how Smartphones enhance consumer self-disclosure. J Mark 84(3):28–45. https://doi.org/10.1177/0022242920912732
Miyazaki AD (2008) Online privacy and the disclosure of cookie use: effects on consumer trust and anticipated patronage. J Public Policy Mark 27(1):19–33. https://doi.org/10.1509/jppm.27.1.19
Mothersbaugh DL, Foxx WK II, Beatty SE, Wang S (2012) Disclosure antecedents in an online service context: the role of sensitivity of information. J Serv Res 15(1):76–98. https://doi.org/10.1177/1094670511424924
Neuman RW, Guggenheim L, Jang MS, Bae SY (2014) The dynamics of public attention: agenda-setting theory meets big data. J Commun 64(2):193–214. https://doi.org/10.1111/jcom.12088
Norberg PA, Horne DR (2007) Privacy attitudes and privacy-related behavior. Psychology & Marketing 24(10):829–847
Norberg PA, Horne DR (2014) Coping with information requests in marketing exchanges: an examination of pre-post affective and behavioral coping. J of the Acad Mark Sci 42(4):415–429. https://doi.org/10.1007/s11747-013-0361-6
Norberg PA, Horne DR, Horne DA (2007) The privacy paradox: personal information disclosure intentions versus behaviors. J Consumer Aff 41(1):100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x
Petronio S (2002) Boundaries of privacy: dialectics of disclosure. State University of New York Press, New York
PricewaterhouseCoopers (2020) How consumers see cybersecurity and privacy risk and what to do about it. https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html. Zugegriffen: 29. Okt. 2020
Raab CD, Bennet CJ (1998) The distribution of privacy risks: who needs protection? Inf Soc 14(4):253–262. https://doi.org/10.1080/019722498128719
Romanosky S, Hoffman D, Acquisti A (2014) Empirical analysis of data breach litigation. J Empir Leg Stud 11(1):74–104. https://doi.org/10.1111/jels.12035
Rust RT (2020) The future of marketing. Int J Res Mark 37(1):15–26. https://doi.org/10.1016/j.ijresmar.2019.08.002
Sachverständigenrat für Verbraucherfragen (2017) Digitale Souveränität: Gutachten des Sachverständigenrats für Verbraucherfragen. https://www.svr-verbraucherfragen.de/dokumente/digitale-souveraenitaet/. Zugegriffen: 29. Okt. 2020

Satariano A (2019) Real-time surveillance will test the British tolerance for cameras. New York Times. https://www.nytimes.com/2019/09/15/technology/britain-surveillance-privacy.html. Zugegriffen: 4. Nov. 2020

Schouten B, Tistarelli M, Garcia-Mateo C, Deravi F, Meints M (2008) Nineteen urgent research topics in biometrics and identity management. In: European workshop on biometrics and identity management. Springer, Berlin, Heidelberg, S 228–235

Schumann JH, Wangenheim FV, Groene N (2014) Targeted online advertising reciprocity appeals to increase acceptance among users of free web services. J Mark 78(1):59–75. https://doi.org/10.1509/jm.11.0316

Sheehan KB, Hoy MG (2000) Dimensions of privacy concern among online consumers. J Public Policy Mark 19(1):62–73. https://doi.org/10.1509/jppm.19.1.62.16949

Smith JH, Milberg SJ, Burke JB (1996) Information privacy: measuring individuals' concerns about organizational practices. MIS Q 20(2):167–196. https://doi.org/10.2307/249477

Solove DJ (2011) Nothing to hide: the false tradeoff between privacy and security. Yale University Press, New Haven

Solove DJ, Schwartz PM (2020) ALI data privacy: overview and black letter text. UCLA Law Rev 68(1):1–46. https://doi.org/10.2139/ssrn.3457563

Trabandt M, Lasarov W (2020) Consumer Digital Responsibility – eine Einführung. In: Heidbrink L, Müller S (Hrsg) Consumer Social Responsibility. Zur gesellschaftlichen Verantwortung von Konsumenten. Metropolis, Marburg

Tsai JY, Egelman S, Cranor L, Acquisti A (2011) The effect of online privacy information on purchasing behavior: an experimental study. Inf Syst Res 22(2):254–268. https://doi.org/10.1287/isre.1090.0260

Tucker CE (2014) Social networks, personalized advertising and privacy controls. J Mark Res 51(5):1547–7193. https://doi.org/10.1509/jmr.10.0355

Vail MW, Earp JB, Antón AI (2008) An empirical study of consumer perceptions and comprehension of web site privacy policies. IEEE Trans Eng Manag 55(3):442–454. https://doi.org/10.1109/TEM.2008.922634

Varian HR (1996) Economic aspects of personal privacy, privacy and self-regulation in the information age. National Telecommunications and Information Administration Report, Washington DC

Webb TL, Sheeran P (2006) Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence. Psychol Bull 132(2):249–268

White TB (2004) Consumer disclosure and disclosure avoidance: a motivational framework. J Consum Psychol 14(1):41–51. https://doi.org/10.1207/s15327663jcp1401&2_6

White K, Habib R, Hardisty DJ (2019) How to SHIFT consumer behaviors to be more sustainable: a literature review and guiding framework. J Mark 83(3):22–49. https://doi.org/10.1177/0022242919825649

White TB, Zahay DL, Thorbjørnsen H, Shavitt S (2008) Getting too personal: Reactance to highly personalized email solicitations. Market Lett 19(1):39–50. https://doi.org/10.1007/s11002-007-9027-9

Wirtz J, Lwin MO (2009) Regulatory focus theory, trust, and privacy concern. J Serv Res 12(2):190–207. https://doi.org/10.1177/1094670509335772

Xu H, Teo HH, Tan BCY, Agarwal R (2012) Effects of individual self-protection industry self-regulation, and government regulation on privacy concerns: A study of location-based services. Inf Syst Res 23(4):1342–1363. https://doi.org/10.1287/isre.1120.0416