Learning by doing oder *doing by learning?*

Die Wechselwirkung zwischen Online-Privatheitskompetenz und Datenschutzverhalten

Johanna Schäwel / Regine Frener / Philipp K. Masur / Sabine Trepte*

Die Nutzung von und die Kommunikation mit sozialen Medien basiert auf dem Austausch persönlicher Daten. Dabei können Privatheitsrisiken entstehen, vor denen man sich oft nur schwer schützen kann. Damit Menschen Online-Angebote selbstbestimmt nutzen können, ist ein gewisser Schutz ihrer Daten erforderlich. Immer häufiger wird die Online-Privatheitskompetenz als Voraussetzung dafür angesehen. Kritisch hinterfragt wird jedoch, ob Wissen über Online-Privatheit tatsächlich zu aktivem Datenschutz führt. Die Kausalität zwischen Online-Privatheitskompetenz und Datenschutz blieb bislang unerforscht: Schützen Menschen mit hoher Online-Privatheitskompetenz ihre Daten besser? Oder ist es umgekehrt, und Datenschutzverhalten macht Internetnutzende kompetenter? Mit einer Längsschnittstudie haben wir die Wechselwirkung zwischen Online-Privatheitskompetenz und der Umsetzung von Datenschutz von N = 898 Internetnutzenden untersucht. Die Ergebnisse zeigen, dass Menschen mit höherer Online-Privatheitskompetenz über die Zeit ihre Daten etwas aktiver schützen. Umgekehrt hat Datenschutzverhalten jedoch keinen signifikanten Einfluss auf die Online-Privatheitskompetenz.

Schlüsselbegriffe: Privatheit, Datenschutz, Online-Privatheitskompetenz, Datenschutzverhalten, Längsschnittstudie

Learning by Doing or *Doing by Learning?*

The Interdependency between Online Privacy Literacy and Data Protection Behavior

The use of and communication via social media is based on the exchange of personal data. This can lead to privacy risks against which protection is difficult. In order to use online services in a self-determined manner, a certain level of data protection is necessary. Increasingly, online privacy literacy is seen as a prerequisite for data protection. However, it is often questioned whether knowledge of online privacy actually leads to active data protection. The causality between online privacy literacy and data protection has remained underexplored: Do people with high online privacy literacy protect their data more? Or is it the other way around, and privacy protection behaviors make Internet users more competent? Based on a sample of N = 898 Internet users that participated in a longitudinal panel study, we investigated the reciprocal effects between online privacy literacy and

* Dr. Johanna Schäwel, Universität Hohenheim, Institut für Kommunikationswissenschaft, Fachgebiet Medienpsychologie. 540 F. 70593 Stuttgart, Deutschland, johanna.schaewel@uni-hohenheim.de, ORCID: https://orcid.org/0000-0002-2038-2443.
Regine Frener, M.Sc., Universität Hohenheim, Institut für Kommunikationswissenschaft, Fachgebiet Medienpsychologie. 540 F. 70593 Stuttgart, Deutschland, Regine.Frener@uni-hohenheim.de, ORCID: https://orcid.org/0000-0002-3212-6893.
Dr. Philipp K. Masur, Vrije Universiteit Amsterdam, Faculty of Social Sciences, Communication Science, De Boelelaan 1105, 1081 HV Amsterdam, Netherlands, p.k.masur@vu.nl, ORCID: https://orcid.org/0000-0003-3065-7305.
Prof. Dr. Sabine Trepte, Universität Hohenheim, Institut für Kommunikationswissenschaft, Fachgebiet Medienpsychologie. 540 F. 70593 Stuttgart, Deutschland, sabine.trepte@uni-hohenheim.de, ORCID: https://orcid.org/0000-0002-6882-8707.

DOI: 10.5771/1615-634X-2021-2-221

data protection. The results show that people who tend to be more literate with regard to online privacy, protect their data somewhat more actively. Conversely, however, privacy protection behaviors do not significantly influence online privacy literacy.

Keywords: privacy, data protection, online privacy literacy, data protection behavior, longitudinal study

1. Einleitung

Wer das Internet nutzt, produziert Daten. Ob bewusst durch das Teilen von personenbezogenen Informationen in sozialen Medien oder unbewusst durch die Nutzung unterschiedlicher Online-Dienste, z. B. zur computervermittelten Kommunikation oder zum Online-Shopping, Internetnutzende hinterlassen stets eine Datenspur. Laut Eurobarometer nutzen in Europa 73 Prozent der Menschen täglich das Internet (European Commission, 2019). Bei den 15- bis 24-Jährigen sind es sogar fast 100 Prozent. Viele der deutschen Internetnutzenden machen dabei von sozialen Netzwerkseiten (52 %) und Online-Shopping-Portalen (67 %) Gebrauch und geben dort eine Vielzahl an personenbezogenen Informationen, wie zum Beispiel Name, Adresse, Kontoverbindung oder persönliche Interessen an (European Commission, 2019).

Dabei entsteht eine Reihe von Risiken für die eigene Privatheit (Gapski, 2020; Livingstone et al., 2013; Livingstone et al., 2019). Neben dem Missbrauch oder der ungewollten Rekontextualisierung von persönlichen Informationen durch andere Nutzende (Vitak, 2012; Vitak et al., 2015) stehen Individuen vor der Herausforderung, mit potenziell privatheitsinvasiven Praktiken von Online-Diensteanbietenden umzugehen. Viele Europäer:innen (68 %) sind besorgt um ihre Daten und befürchten, dass diese von den Webseiten nicht sicher aufbewahrt werden (European Commission, 2019). In Deutschland sind 74 Prozent besorgt oder sehr besorgt darüber, wie Organisationen und Webseitenanbietende ihre Daten behandeln und verarbeiten; dabei wissen 55 Prozent der Deutschen nicht, dass sie das Recht haben, die von ihnen gespeicherten Daten einzusehen (Trepte & Masur, 2017). Weitere 24 Prozent wissen ebenfalls nicht, dass sogar solche Daten von ihnen gesammelt werden, die nicht öffentlich einsehbar sind (z. B. von der NSA; Trepte & Masur, 2017). Nur 47 Prozent der Deutschen fühlen sich „zumindest manchmal" über Risiken von Online-Kriminalität informiert, und fast die Hälfte der Deutschen hat das Gefühl, keine Kontrolle über ihre Daten zu haben, worüber sie sehr besorgt sind (European Commission, 2015; 2019).

Ungewissheit über den Umgang mit Risiken und ein wahrgenommener Kontrollverlust persönlicher Daten können sich als Privatheitsbedenken manifestieren. Dies kann einerseits ein Antrieb für Kompetenzerwerb sein, denn Sorgen und Bedenken führen zu einem emotionalen Ungleichgewicht, welches z. B. durch Informationssuche oder Verhaltensänderungen adressiert wird (Li, 2011). Andererseits kann jedoch ebenso ein Zustand von Resignation resultieren, bei dem Menschen davon ausgehen, dass sie keine Möglichkeit haben, ihre Privatheit zu regulieren, und sie bestehende Risiken somit ausblenden oder akzeptieren (Hoffmann et al., 2016; Lutz et al., 2020).

Das Regulieren der eigenen Privatheit, d. h. des Ausmaßes der Zugänglichkeit zur eigenen Person (Altman, 1974; Westin, 1967), geschieht in vielen alltäglichen Situationen intuitiv. So sind beispielsweise viele Prozesse der physischen Privatheitsregulation seit früher Kindheit sozialisiert. Menschen haben ein gefestigtes und geteiltes Verständnis von Territorialität (Altman, 1975), z. B. in Bezug auf ihren eigenen Körper, ihren Sitznachbarn oder ihr Haus. Durch zwischenmenschliche Kommunikation und das Regulieren der physischen oder psychischen Zugänglichkeit kann ein Zustand gewollter Zu-

rückgezogenheit oder gemeinsamer Privatheit hergestellt werden (Trepte, 2016b; Westin, 1967). Diese Option, Privatheit in verschiedenen Lebensbereichen kommunikativ zu regulieren und immer wieder herstellen zu können, ist für das menschliche Wohlbefinden relevant, da sie wichtige Grundbedürfnisse wie Autonomie, Intimität und Selbstevaluation erfüllt (Pedersen, 1999; Westin, 1967).

In Online-Umgebungen (z. B. auf sozialen Netzwerkseiten) stellt die Privatheitsregulation einen relevanten Teil der Nutzung dar und betrifft ebenfalls Aspekte der zwischenmenschlichen (computervermittelten) Kommunikation und Selbstoffenbarung der Nutzenden. Hier stellt sich die individuelle Privatheitsregulation teilweise als herausfordernd dar (Dienlin & Metzger, 2016; Krämer & Schäwel, 2020; Millham & Atkin, 2018; Tsay-Vogel et al., 2018). Aktive Nutzungspraktiken der Privatheitsregulation sind nach Trepte (2020a) interpersonale Kommunikation (z. B. Absprache mit Familie, welche Bilder auf Facebook geteilt werden dürfen), Deliberation (z. B. aktive öffentliche Debatte zu legitimen Formen des Austausches von Daten mit Unternehmen), Kontrolle (z. B. die gezielte Auswahl geeigneter Online-Dienste und -Plattformen; das Zurückziehen offenbarter personenbezogener Informationen) oder Selbstoffenbarung (z. B. das Teilen persönlicher Informationen auf Facebook) in sozialen Medien.

Über individuellen Privatheitsschutz hinaus beinhaltet aktiver Privatheitsschutz weiterhin die kritische Betrachtung bestehender sozialer Verhaltensnormen, die die Privatheit des Individuums als Teil einer Gruppe oder Gesellschaft tangieren und formen können (Masur, 2020). Diese kritische Auseinandersetzung mit geltenden Normen kann das Bewusstsein für einen demokratischen Umgang mit Online-Privatheitsschutz schärfen und sollte, neben individuellen Schutzmaßnahmen, im besten Fall interdependente (zwischen und in Gruppen abgestimmte) und darauf basierend demokratisch entwickelte, strukturell-systemische Schutzmaßnahmen hervorbringen (Masur, 2020). Um den Privatheitsbedürfnissen auch im Internet und speziell in sozialen Medien nachkommen zu können, bedarf es somit mehr Aufwand als im privaten physischen Raum und es setzt spezifisches Wissen über technische Voraussetzungen (z. B. App-Berechtigungen) und bestimmte Portale oder Kanäle (z. B. Online-Shopping-Seiten oder Messenger-Dienste) sowie konkrete Fähigkeiten voraus.

Zusammenfassend beinhaltet die Idealvorstellung einer allgemeinen Medien- bzw. einer spezifischen Online-Privatheitskompetenz, dass Menschen das Internet *selbstbestimmt* nutzen und dabei das Ausmaß an Privatheitsrisiken minimieren. Während Medienkompetenz die Fähigkeit beschreibt, reflektiert auf mediale Inhalte zugreifen, diese für eine selbstbestimmte Nutzung analysieren, vor dem Hintergrund verschiedener Kontexte evaluieren, sowie eigene Inhalte generieren zu können (Livingstone, 2004; Trepte, 2016a), spezifiziert Privatheitskompetenz diesen Anspruch und umfasst kognitive Fähigkeiten und Fertigkeiten, die ein Individuum in unterschiedlichen Situationen während der Nutzung digitaler Medien dazu befähigen, eine problemorientierte Privatheitsregulation vorzunehmen (Masur, 2018; Trepte et al., 2015).

Sowohl die allgemeine Medienkompetenz als auch die spezifische Online-Privatheitskompetenz zeichnet sich somit durch umfassendes deklaratives und prozedurales Wissen sowie eine ausgeprägte Kritikfähigkeit aus. Forschung zu Medienkritikfähigkeit beschreibt diese als die „Kompetenz, rezipierte Medienangebote kritisch hinsichtlich ihrer Aussagen, Qualität, anzunehmenden Produktionsumstände und/oder gesellschaftlicher oder normativer Implikationen zu bewerten“ (Sowka et al., 2015, S. 65). Die Privatheitsforschung beschreibt entsprechend kritische Privatheitskompetenz als die Fähigkeit, existierende soziale, ökonomische und institutionelle Praktiken und Strukturen,

die die Privatheit beeinflussen, kritisieren, hinterfragen und herauszufordern zu können (Masur, 2020, S. 262).

Die Online-Privatheitskompetenz von Nutzenden digitaler und sozialer Medien wird bereits mithilfe umfassender Programme (z. B. von Landesmedienanstalten oder der Bundeszentrale für digitale Aufklärung; siehe Abschnitt 4) unterstützt. Dies wird insbesondere dann verstärkt gefordert, wenn scheinbar medieninduzierte Gefahren, zum Beispiel durch neue Plattformen, Applikationen oder Technologien, beobachtet oder öffentlich kommuniziert werden und sich Nutzende in ihrer Online-Privatheit bedroht fühlen.

Die bisherige Forschung hat sich vor allem auf die Konzeptualisierung der Online-Privatheitskompetenz und ihren (ungerichteten) Zusammenhang mit Datenschutzverhalten bzw. der allgemeinen Informationspreisgabe konzentriert (vgl. Überblick in Trepte et al., 2015). Offen ist jedoch, ob eine höhere Online-Privatheitskompetenz tatsächlich zu einer Anpassung des Datenschutzverhaltens, oder umgekehrt, ob Datenschutzverhalten langfristig zu einer höheren Online-Privatheitskompetenz führt. In diesem Beitrag analysieren wir entsprechend den längsschnittlichen Einfluss der Kompetenzen auf das aktiv praktizierte Schutzverhalten sowie den Einfluss des Schutzverhaltens auf die Online-Privatheitskompetenz. Damit verfolgen wir das Ziel, die Relevanz von Maßnahmen zur Erweiterung und Aufrechterhaltung von Online-Privatheitskompetenz und damit einhergehend zur Steigerung des Datenschutzverhaltens von Nutzenden digitaler sozialer Medien zu unterstreichen. Zu diesem Zweck wurden die Daten einer Längsschnittstudie herangezogen und die Wechselwirkung zwischen Online-Privatheitskompetenz und Datenschutzverhalten über die Zeit untersucht.

Im Nachfolgenden stellen wir zunächst das Konzept der Online-Privatheitskompetenz im Detail vor und diskutieren bisherige Ergebnisse zum Zusammenhang zwischen Online-Privatheitskompetenz und Datenschutzverhalten. Im Anschluss daran stellen wir die Analyse der Längsschnittstudie vor. Die Ergebnisse werden abschließend in Bezug auf die gesamtgesellschaftliche Schutzverantwortung und die Relevanz für das Individuum reflektiert und eingeordnet.

2. Online-Privatheitskompetenz

Online-Privatheitskompetenz wurde schon früh als Kombination aus verschiedenen Wissensdimensionen operationalisiert (Hoofnagle et al., 2010; Park, 2013; Turow, 2003) und bereits in zahlreichen Werken untersucht (Baruh et al., 2017; Epstein & Quinn, 2020; Kumar et al., 2020; Park, 2013; Park & Jang, 2014; Rosenthal et al., 2019). Zusammenfassend definieren Trepte et al. (2015) Privatheitskompetenz zunächst als Kombination aus deklarativem und prozeduralem Wissen über Online-Privatheit. Das deklarative Wissen bezieht sich auf Faktenwissen (Wissen „was“, z. B. was ein Cookie ist) und das prozedurale auf Handlungswissen (Wissen „wie“, z. B. wie Cookies gelöscht werden; Ackerman et al., 2002; Mandl & Spada, 1988).

Zur weiteren Definition unterteilten Trepte et al. (2015) das deklarative und faktische Wissen über Privatheit basierend auf den Ergebnissen einer Inhaltsanalyse bisheriger Arbeiten zu den Themen Datenschutz und Online-Privatheitskompetenz in fünf Dimensionen. Das deklarative Wissen umfasst (1) das Ausmaß der Informiertheit über potenziell privatheitsinvasive Praktiken (z. B. Sammlung, Speicherung, Weitergabe von personenbezogenen Daten) von Institutionen und Online-Diensteanbietenden, (2) das Wissen über technische Aspekte des Datenschutzes in digitalen Anwendungsbereichen, (3) das Wissen über Datenschutzgesetze und -Richtlinien sowie (4) das Wissen über Strategien für die Regulierung der individuellen Privatheit. Das prozedurale Wissen be-

schreiben sie (5) als die Fähigkeit, Strategien zur Regulation und zum Schutz der Privatheit zu entwickeln und das faktische Wissen für den aktiven Schutz der Privatheit anwenden zu können.

Faktisches und prozedurales Wissen über Privatheitsschutz können sich sowohl auf die *horizontale* (z. B. Schutz vor Privatheitseingriffen durch andere Nutzende) als auch die *vertikale* (z. B. Schutz vor Privatheitseingriffen durch Institutionen oder Dienste-anbietende) Privatheit beziehen (Bazarova & Masur, 2020; Masur et al., 2018; Raynes-Goldie, 2010; Trepte, 2015). In diesem Beitrag fokussieren wir uns primär auf den vertikalen Privatheitsschutz, d. h. auf den Schutz der Privatheit mit Maßnahmen, welche die vertikale Privatheit betreffen (z. B. Nutzung von Anti-Tracking-Diensten oder Verschlüsselungsprogrammen). Diese Schutzmaßnahmen beziehen sich jedoch nicht ausschließlich auf den Schutz der Daten, die beispielsweise mit Facebook oder Google ausgetauscht werden. Vielmehr steht jegliche Form der vertikalen Privatheit in Zusammenhang mit der horizontalen Privatheit, denn geschützt wird die Kommunikation zwischen Individuen, die über Portale, Plattformen und Werkzeuge der Diensteanbietenden stattfindet. Nur wenn Nutzende den computervermittelten Datenaustauch über Dienste wie Gmail oder soziale Medien wie Facebook, Twitter oder Instagram als sicher erleben, werden sie auch ihre Kommunikation auf horizontaler Ebene über diese Dienste als geschützt wahrnehmen.

Masur (2018) erweiterte das fünfdimensionale Konzept der Online-Privatheitskompetenz, indem er die Kritikfähigkeit aus klassischen Konzepten der Medienkompetenz integriert (Baacke, 1996; Groeben, 2004). Er schlägt insgesamt vier Dimensionen vor: (1) faktisches Wissen, (2) privatheitsbezogene Reflexionsfähigkeit, (3) privatheits- und datenschutzbezogene Fertigkeiten (beinhalten prozedurales Wissen) und (4) privatheitsbezogene Kritikfähigkeit. Damit werden bisherige Konzeptualisierungsansätze der Online-Privatheitskompetenz (Masur et al., 2017; Park, 2013; Trepte et al., 2015) und der Medienkompetenz (Baacke, 1996; Groeben, 2002; Sowka et al., 2015) vereint und vertieft. Die Reflexions- und Kritikfähigkeit verhelfen zu einer realistischen und situationsspezifischen Einschätzung potenzieller Gefahren für die Online-Privatheit, welche auf theoretischer Online-Privatheitskompetenz (deklarativem Wissen) basieren und als Voraussetzung für den Einsatz von praktischer Online-Privatheitskompetenz (prozeduralem Wissen) gelten können. Nach Masur (2018) ist die weitere Erforschung der Online-Privatheitskompetenz wichtig, „um letztlich das Individuum in die Lage zu versetzen, sich in der heutigen und zukünftigen Informationsgesellschaft selbstbestimmt und in Einklang mit den eigenen, rational reflektierten Privatheitsbedürfnissen zu bewegen“ (S. 461).

Das bedeutet, dass eine selbstbestimmte Nutzung digitaler Medien und computervermittelte Kommunikation sicherer stattfinden können sollte, wenn die Nutzenden über ein gewisses Ausmaß an Online-Privatheitskompetenz verfügen und somit ihre Online-Privatheit regulieren können. Das bedeutet nicht, dass jederzeit ein hohes Ausmaß an Privatheit gegeben sein muss. Trepte (2020a) definiert mit dem Social Media Privacy Model zwei Ausgangsbedingungen: Zunächst prüfen Individuen in einer initialen Einschätzung (a) das Ausmaß der Zugänglichkeit zu persönlichen Informationen und (b) ihr individuelles Kommunikationsziel, um beides dann vor dem Hintergrund medialer Affordanzen abzuwägen, um einen kontextadäquaten angemessenen Informationsfluss auf der einen Seite und einen ausreichenden Schutz auf der anderen Seite zu gewährleisten.

Online-Privatheitskompetenz ist damit auch eine wichtige Voraussetzung für eine bewusste und bedürfnisorientierte Form der computervermittelten Kommunikation

(Park, 2013). Dies ist von Bedeutung, da computervermittelte Kommunikation durch soziale Medien als *eine* Form der Auseinandersetzung in und mit den sozialen Medien zur Befriedigung verschiedenster Bedürfnisse herangezogen werden kann, beispielsweise für die Aufrechterhaltung von Freundschaften, den Erhalt von sozialer Unterstützung und den Aufbau von Sozialkapital, die Versorgung mit Informationen und auch zur Unterhaltung (Huang, 2016; Liu et al., 2016; Trepte & Scharkow, 2016). Aus diesem Grund ist es wichtig, die Voraussetzungen und Wechselwirkungen für die selbstbestimmte Nutzung von Internet- und Kommunikationsdiensten zu analysieren, um eine Grundlage für die Generierung von Handlungsempfehlungen zu bieten.

3. Datenschutzverhalten als Teil der Online-Kommunikation

Der Austausch von Informationen, Gedanken, Gefühlen und Bewertungen ist zentraler Bestandteil zwischenmenschlicher Kommunikation. Damit diese oftmals sensible zwischenmenschliche Kommunikation auch online, also computervermittelt, stattfinden kann, ist der aktive Schutz persönlicher Informationen und spezifischer Kommunikationsinhalte von zentraler Bedeutung. Ohne einen solchen Schutz können beispielsweise vertrauliche Informationen von nicht-intendiert adressierten Publika rezipiert werden (Vitak et al., 2015). Somit ist Datenschutz die Grundlage dafür, dass Kommunikation zwischen Nutzenden digitaler sozialer Medien situationsadäquat und gemäß ihrer Kommunikationsziele und -bedürfnisse stattfinden kann.

Datenschutz wird vor allem thematisiert, wenn sich Medienangebote und Nutzungsweisen verändern. Wenn beispielsweise neue Online-Dienste oder soziale Netzwerkseiten aufkommen, stehen Menschen vor der Herausforderung, unmittelbar auf diese neuen Angebote mit Datenschutzverhalten zu reagieren, oft auch dann, wenn sie diese nicht selbst nutzen möchten (Trepte & Dienlin, 2014).

Insofern ist Datenschutz meist ein aktives Verhalten, das je nach Anwendungsbereich (z. B. Kommunikation via Messenger-Dienst oder Rezeption eines YouTube-Videos) und in Bezug auf das Ausmaß (z. B. einfaches Anpassen der Privatheitseinstellungen vs. Internetnutzung über TOR) stark variieren kann. In dieser Arbeit greifen wir soziale Medien heraus (z. B. Facebook, Twitter, Instagram, YouTube) und untersuchen Aspekte konkreter partizipativer Nutzungsmuster der interpersonalen computervermittelten Kommunikation (vgl. Schmidt, 2018). Soziale Medien erweitern die Räume und Möglichkeiten (z. B. durch mediale Affordanzen; Trepte, 2020a) der interpersonalen computervermittelten Kommunikation zwischen Individuen über zeitliche und räumliche Grenzen hinweg (Schmidt, 2018).

Aufgrund der Bandbreite an Datenschutzmaßnahmen und -möglichkeiten systematisieren wir erstens im Hinblick auf das Schutzziel und zweitens im Hinblick auf den Kontext. In Bezug auf das Schutzziel lässt sich Datenschutzverhalten in präventive (z. B. die Entscheidung gegen die Nutzung eines bestimmten Netzwerkes oder einer bestimmten Applikation), erhaltende (z. B. Beibehaltung einer bestimmten technischen Einstellung) und korrektive (z. B. offenbarte Informationen zurücknehmen, Inhalte auf sozialen Netzwerkseiten löschen) Maßnahmen untergliedern (Masur, 2019, S. 120). In Bezug auf den Kontext unterscheiden wir horizontale und vertikale Maßnahmen des Datenschutzes (zur Unterscheidung von horizontal vs. vertikal vgl. Abschnitt 2).

Im Kontext dieser Studie definieren wir Datenschutzverhalten als aktives Verhalten mit dem Ziel des Schutzes der eigenen Daten (u. a. während der computervermittelten Kommunikation auf horizontaler und vertikaler Ebene) durch das Regulieren der eigenen Zugänglichkeit und der selbstbestimmten Kontrolle über die Datenverarbeitung und -speicherung.

4. Einfluss von Online-Privatheitskompetenz auf Datenschutzverhalten

Maßnahmen, die Internetnutzende umsetzen können, um dem Eintreten befürchteter Risiken entgegenzuwirken, sind die Suche nach Informationen und Aneignung von Wissen in Bezug auf Risiken und Schutzmaßnahmen. In Deutschland bieten dabei verschiedene Stakeholder aktive Unterstützung: Medien informieren zum Beispiel intensiv über Gerichtsurteile und stellen ausgeprägte Service-Angebote bereit, um Wissen zu vermitteln und konkrete Handlungsanweisungen zu geben (von Pape et al., 2017). Medienanstalten und EU-geförderte Initiativen (z. B. klicksafe.de) bieten eine große Bandbreite an Schulungen und Informationen für Eltern, Lehrkräfte, Kinder und Jugendliche zum sicheren Umgang mit Daten im Internet an (z. B. bei der Verwendung von Smartphone-Applikationen). Zudem werden Themen wie Cyber-Mobbing und der verantwortungsvolle Umgang mit persönlichen Informationen in sozialen Medien behandelt (vgl. den Überblick in Trepte & Dienlin, 2014). Das vom Bundesministerium für Bildung und Forschung geförderte Projekt „Forum Privatheit" bietet Veranstaltungen, Forschungsberichte und Medienberichterstattung in Bezug auf die Themen Datenschutz, Datensicherheit und digitale Privatheit (forum-privatheit.de) und die Forschungsgruppe Global Kids Online widmet sich den Rechten und der informationellen Selbstbestimmung von Kindern und Jugendlichen (globalkidsonline.de).

Zu den Maßnahmen dieser weltweiten Initiativen möchten wir beitragen, indem wir fragen, in welchem Ausmaß das Wissen über Privatheit den aktiven Datenschutz von Nutzenden forcieren und unterstützen kann und ob bzw. unter welchen Umständen faktisches und prozedurales Wissen in aktivem Datenschutzverhalten resultiert.

Das Prozessmodell der Online-Privatheitskompetenz sieht fünf konkrete Schritte des Erwerbs von Online-Privatheitskompetenz vor (Masur et al., 2017): (1) *Bewusstsein* (z. B. über Privatheitsrisiken), (2) *Reflexion* (z. B. Abgleich mit sozialen Normen, Erwerb von faktischem Wissen), (3) *Vorbereitung* (z. B. Erwerb von faktischem und prozeduralem Wissen), (4) *Verhaltensänderung* (z. B. Umsetzung von Datenschutzmaßnahmen) und (5) *Aufrechterhaltung* (z. B. langfristige Umsetzung von Gegenkonditionierungsmaßnahmen). Gemäß dem Modell bauen alle Schritte aufeinander auf und wirken positiv auf den Erwerb und die Umsetzung selbstkritischer Privatheitsverhaltensweisen und fördern somit langfristig die Online-Privatheitskompetenz von Nutzenden digitaler und sozialer Medien.

Bisherige Studien scheinen diese These zunächst zu unterstützen. Vorrangig Querschnittsstudien weisen auf einen moderaten Zusammenhang zwischen Online-Privatheitskompetenz und Datenschutzverhalten hin. Park (2013) konnte beispielsweise zeigen, dass technische Vertrautheit, das Bewusstsein für Überwachung sowie das Verständnis von Richtlinien zum Datenschutz mit kontrollierenden Verhaltensweisen in Bezug auf persönliche Informationen einhergehen. Kraus et al. (2014) zeigten in ihrer Studie mit 154 Teilnehmenden, dass das Wissen über Online-Privatheit und Sicherheit – operationalisiert durch das Wissen über Phishing, Verschlüsselungssoftware und Datenschutzrichtlinien – mit Schutzverhaltensweisen, nämlich der Nutzung von Instant Messengern mit Verschlüsselungstechnologie oder der Deinstallation von invasiven Applikationen, einhergeht. Bartsch und Dienlin (2016) konnten weiterhin in einer Studie mit 630 Facebook-Nutzenden zeigen, dass der Teilbereich der *sozialen* Online-Privatheitskompetenz (z. B. Wissen über die Zugriffsbeschränkung des eigenen Profils) in einem positiven Zusammenhang mit sozialem Privatheitsverhalten (z. B. tatsächliche Zugriffsbeschränkung des eigenen Profils) und wahrgenommener Sicherheit steht. Dieser Zusammenhang konnte in einer Studie von Liu et al. (2017) weiter bestärkt werden. In ihrer Studie zum Management der Online-Privatheit auf der Plattform Facebook

fanden sie, dass das Wissen über den Online-Privatheitsschutz in einem negativen Zusammenhang mit dem Grad der Zugänglichkeit (oder „Offenheit") des Facebook-Profils steht. Wissen wurde hierbei anhand des Wissens über die Möglichkeiten der Zugangsbeschränkung des eigenen Profils operationalisiert (Liu et al., 2017). Schließlich fanden Masur et al. (2017) heraus, dass die allgemeine Online-Privatheitskompetenz, operationalisiert als Globalfaktor aus den Dimensionen Wissen über institutionelle Praktiken, technische Aspekte, Datenschutzrecht und Datenschutzstrategien, positiv mit diversen Datenschutzverhaltensweisen korreliert (vgl. auch oplis.de). Dabei prädizierte eine höhere Kompetenz vor allem aktiveres Datenschutzverhalten, wie z. B. die Pseudonymisierung von E-Mails, Nutzung von Anonymisierungssoftware und das Löschen von Cookies und Caches. Weiterhin wurde das Wissen über technischen Privatheitsschutz als entscheidender negativer Prädiktor für die Akzeptanz potenziell privatheitsinvasiver Prozesse identifiziert (Rosenthal et al., 2019).

Die vorhandenen Querschnittsstudien sprechen also für einen moderaten positiven Zusammenhang zwischen Online-Privatheitskompetenz und Schutzverhalten. Dieser wurde in allen Studien als ein Effekt des Wissens auf das Schutzverhalten interpretiert. Ob diese *kausale* Interpretation zulässig ist, wurde jedoch bisher nicht empirisch untersucht. Der querschnittliche positive Zusammenhang zwischen Wissen und Datenschutzverhalten lässt ebenso die reziproke Kausalität zu: Menschen, die sich besonders aktiv um Datenschutz bemühen, könnten aufgrund ihrer Aktivitäten im Bereich Datenschutz ihr Wissen erweitern. Dabei würde die Umsetzung von Datenschutz auch das Wissen über die Möglichkeiten und Grenzen des Datenschutzes sowie die Kompetenz im Umgang mit privaten Daten im Internet erhöhen. Es ist zudem nicht ausgeschlossen, dass beide Prozesse stattfinden und sich gegenseitig bedingen oder verstärken.

Um den Einfluss von Online-Privatheitskompetenz auf das Datenschutzverhalten analysieren zu können, muss also eine dynamische Wechselwirkung zwischen der Online-Privatheitskompetenz und dem Datenschutzverhalten über die Zeit hinweg angenommen und untersucht werden. Aufgrund der bisher ausschließlich korrelativen Ergebnisse können kausale Effekte in beide Richtungen angenommen werden. Zum einen ist es denkbar, dass Online-Privatheitskompetenz zu (mehr) Datenschutzverhalten führt. Zum anderen kann aber ebenso angenommen werden, dass sich Personen durch das Umsetzen von Datenschutzpraktiken weiteres Wissen aneignen und lernen, dieses umzusetzen, was sich langfristig positiv auf die Online-Privatheitskompetenz auswirken könnte. Somit lassen sich folgende Hypothesen ableiten:

Hypothese 1 (H1): Personen, die zum Zeitpunkt T1 eine höhere Online-Privatheitskompetenz aufweisen, schützen ihre Daten ein Jahr später (T2) mehr als Personen, die zum Zeitpunkt T1 eine geringere Online-Privatheitskompetenz aufweisen.

Hypothese 2 (H2): Personen, die zum Zeitpunkt T1 ihre Daten mehr schützen, weisen ein Jahr später (T2) eine höhere Online-Privatheitskompetenz auf als Personen, die zum Zeitpunkt T1 ihre Daten weniger schützen.

5. Methode

5.1. Design und Stichprobe

Die Hypothesen wurden anhand eines Datensatzes untersucht, der im Rahmen des Projektes „Privatheit im Wandel" in fünf Wellen zwischen Mai 2014 und Mai 2017 erhoben wurde (Trepte, 2020b). In diesem Projekt wurden, neben den hier vorgestellten Varia-

blen, noch weitere Konstrukte erhoben. Ein vollständiger Überblick aller Variablen und assoziierter Studien ist hier zusammengefasst: https://osf.io/4w65z/. Der Datensatz ist hier abrufbar: https://doi.org/10.7802/2117. Der Code für die aktuellen Analysen ist im OSF-Projekt „Interdependency between privacy literacy and data protection behavior" verfügbar: https://osf.io/43ukv/. Alle Analysen sind vollständig reproduzierbar.

Zu Beginn des Projektes wurden 14.714 Personen aus einem Referenzsystem für bevölkerungsrepräsentative Studien in Deutschland (ADM-Master-Sample) in Anlehnung an das Gabler-Häder-Verfahren von einem Marktforschungsunternehmen ausgewählt und telefonisch kontaktiert. Auf diese Weise wurde zum Zeitpunkt der ersten Rekrutierung eine für Deutschland repräsentative Stichprobe gezogen. Aufgrund der eingeschränkten Erreichbarkeit über das Festnetz wurde zusätzlich eine Mobilfunkstichprobe gezogen. So wurden $N = 3.278$ Personen rekrutiert, die an der ersten Untersuchungswelle im Mai 2014 teilnahmen. Zwei weitere Wellen wurden im Abstand von 6 Monaten im November 2014 ($N = 2.484$, Panelmortalität: 24,2 %) und im Mai 2015 ($N = 2.100$, Panelmortalität: 15,6 %) durchgeführt. Die Längsschnittstudie wurde im Anschluss um zwei weitere Wellen mit einem zeitlichen Abstand von jeweils einem Jahr (Mai 2016: $N = 1.429$, Mai 2017: $N = 1.226$; Panelmortalität: 14,2 %) verlängert. Insgesamt nahmen $N = 1.226$ Befragte an allen fünf Erhebungen teil. Die nachfolgenden Analysen beziehen sich auf die Wellen 4 (hier T1) und 5 (hier T2), da zu diesem Zeitpunkt das Datenschutzverhalten der Teilnehmenden erhoben wurde. Für die vorliegende Studie wurden 180 Personen ausgeschlossen, die das Internet zum Befragungszeitpunkt nicht nutzten. Zur Bereinigung des Datensatzes wurden weiterhin fehlende Werte auf systematisches Auftreten untersucht. Um nur die Personen, welche vollständige oder zufällig (anstatt systematisch) fehlende Angaben machten, in die Analyse einzubeziehen, wurden 148 Personen, die weniger als 50 Prozent der Fragen zum Datenschutzverhalten und weniger als 75 Prozent der Online Privacy Literacy Scale (OPLIS; siehe Abschnitt 5.2) ausgefüllt haben, von den Analysen ausgeschlossen. Damit blieben für die nachfolgenden Analysen $n = 898$ Personen.

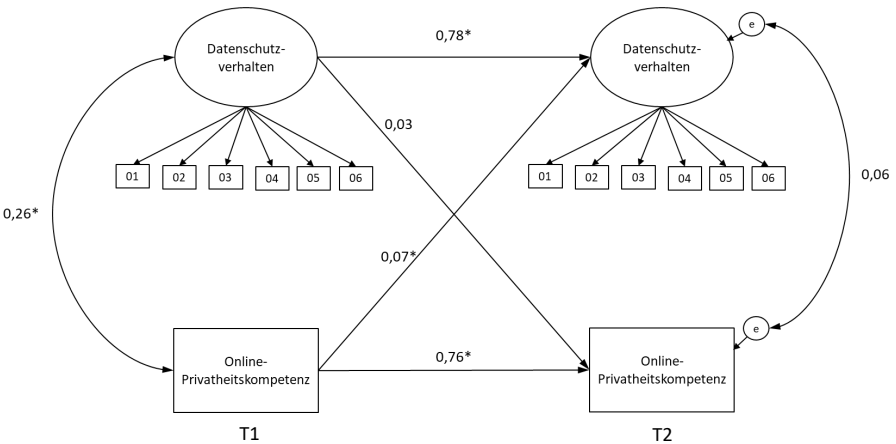
Die Befragten waren zum ersten Befragungszeitpunkt der vorliegenden Studie (hier T1, im Gesamtprojekt Welle 4) zwischen 16 und 86 ($M = 55,64$, $SD = 14,45$) und zum zweiten Befragungszeitpunkt (T2, im Gesamtprojekt Welle 5) ebenfalls zwischen 16 und 86 Jahre alt ($M = 55,61$, $SD = 14,45$). Das vergleichsweise hohe Alter der Befragten beruht auf der Tatsache, dass im Jahr 2014 eine für die deutsche Bevölkerung repräsentative Stichprobe rekrutiert wurde und dass ein Mindestalter von 16 für die Studienteilnahme festgelegt wurde. Das Durchschnittsalter der Deutschen ab 16 Jahren beträgt 49 Jahre (Statistisches Bundesamt, 2019). Der Anteil der männlichen Teilnehmenden betrug 52,2 Prozent. Ein Viertel der Befragten verfügte über einen Realschulabschluss (25,9 %) und 63,4 Prozent über das Abitur. Die Abiturientenquote ist in dieser Stichprobe etwas höher als die Quote der Personen mit Fachhochschulreife oder Hochschulabschluss im bundesweiten Durchschnitt des Jahres 2020 (52 %; Statistisches Bundesamt, 2020).

5.2. Datenanalyse

Alle Analysen wurden in R (Version 3.1.2) mit den Paketen mice (van Buuren & Groothuis-Oudshoorn, 2011) und lavaan (Rosseel, 2012) durchgeführt. Die Passung der Modelle wurde nach den von Hair et al. (2014) beschriebenen Beurteilungskriterien für typische Goodness-of-Fit Indizes (χ^2, RMSEA, CFI, TLI) unter Berücksichtigung der Stichprobengröße (> 250) und der Anzahl der Parameter (< 8) bewertet. Für den Comparative Fit Index (CFI) und Trucker-Lewis-Index (TLI) gelten Werte über 0,90 als akzeptabel. Für den Root Mean Square Error of Approximation (RMSEA) strebten wir

Werte < 0,07 bei einem CFI von mindestens 0,90 an (Hair et al., 2014). Der χ^2-Test sollte in Anlehnung an die Kriterien nicht signifikant sein; in Anbetracht der Stichprobengröße > 250 erwarteten wir jedoch, dass der χ^2-Test unabhängig von der tatsächlichen Modellpassung signifikant wird (Hair et al., 2014). Die kausalen Zusammenhänge zwischen Online-Privatheitskompetenz und Datenschutzverhalten wurden mit Hilfe eines autoregressiven Cross-Lagged-Panel-Models (CLPM) mit latenten und manifesten Variablen analysiert (siehe Abb. 1). Sowohl der Einfluss von Online-Privatheitskompetenz (T1) auf Datenschutzverhalten (T2) als auch der Einfluss von Datenschutzverhalten (T1) auf Online-Privatheitskompetenz (T2) wurde modelliert. Die Autokorrelationen der Variablen zwischen T1 und T2 bilden die Stabilität der Variablen über die Messzeitpunkte hinweg ab. Um zeitliche Invarianz zu gewährleisten, wurden die Faktorladungen zu beiden Messzeitpunkten konstant gehalten. Sowohl für Datenschutzverhalten als auch für Online-Privatheitskompetenz wurden konfirmatorische Faktorenanalysen, welche jeweils auf den Daten beider Messzeitpunkte basieren, durchgeführt.

Abbildung 1: Cross-Lagged-Panel-Modell (CPLM) zur Wechselwirkung zwischen Online-Privatheitskompetenz (Summenscore) und Datenschutzverhalten (latent geschätzt). Die eingetragenen Werte sind standardisierte Pfadkoeffizienten.



* $p < 0,05$

Da wir für die längsschnittlichen Effekte eher kleine bis schwache Effektgrößen erwarteten, wurde zur Minimierung des beta-Fehlers eine ausreichend große Stichprobengröße angestrebt. Deswegen wurden fehlende Werte in der hier verwendeten Stichprobe mithilfe multipler Imputation ergänzt, anstatt weitere Daten auszuschließen. Dabei wurde das Verfahren des semi-parametrischen Predictive Mean Matching verwendet (Meinfelder, 2009; van Buuren, 2012). Bei der semi-parametrischen Predictive-Mean-Matching-Methode wird für jede fehlende Angabe für ein Item zufällig ein Wert aus einer Menge von beobachteten Zielgrößen der betreffenden Person gezogen. Somit werden die imputierten Werte auf den beobachteten Wertebereich der Skala eingegrenzt und simulieren ein realistisches Antwortverhalten dieser Person.

Tabelle 1: Psychometrische Eigenschaften und bivariate Korrelationen zwischen den Variablen

Variables	*M*	*SD*	1	2	3	4	5	6
1. OPLIS (T1)	11,56	3,74						
2. OPLIS (T2)	11,78	3,63	0,77*					
3. Datenschutz (T1)	3,30	0,84	0,28*	0,27*				
4. Datenschutz (T2)	3,29	0,84	0,28*	0,28*	0,76*			
5. Alter	55,63	14,45	-0,17*	-0,26*	0,04	0,04		
6. Geschlecht	0,48	0,50	-0,23*	-0,19*	-0,10*	-0,09*	-0,23*	
7. Bildung	3,52	0,71	0,18*	0,22*	0,00	0,00	-0,07*	-0,01

Anmerkung: M = Mittelwert, *SD* = Standardabweichung, OPLIS = Online-Privatheitskompetenz-Skala als Summenscore von 1 bis 19, Datenschutz = Datenschutzverhalten gemessen auf einer Skala von 1 bis 5. Geschlecht: 1 = weiblich. Bildung gemessen auf einer Skala von 0 bis 4: 0 = „ohne Abschluss", 1 = „noch Schüler/in", 2 = „Hauptschulabschluss", 3 = „Realschulabschluss", 4 =„Abitur, FHS".
* $p < 0{,}05$

5.3. Messinstrumente

Eine Übersicht über die untersuchten Variablen, ihre psychometrischen Eigenschaften, sowie über die bivariaten Korrelationen findet sich in Tabelle 1.

Online-Privatheitskompetenz. Die Online-Privatheitskompetenz wurde mithilfe der Online Privacy Literacy Scale (OPLIS) von Masur et al. (2017) erfasst, welche die Online-Privatheitskompetenz als Kombination aus faktischem und deklarativem Wissen über Online-Privatheit und Datenschutz konzeptualisiert (siehe Abschnitt 2). Die Skala deckt vier Wissensbereiche der Online-Privatheit ab: (1) institutionelle und organisationale Praktiken, (2) technische Aspekte der Online-Privatheit und des Datenschutzes, (3) rechtliche Aspekte des Datenschutzes in Deutschland und (4) Nutzungsstrategien für die individuelle Privatheitsregulierung. Jede Subdimension wird mit fünf Fragen entweder durch ein Multiple-Choice- oder Wahr-Falsch-Antwortformat (für eine Übersicht über die Item-Formulierungen siehe Tabelle A1 im Appendix oder oplis.de) erfasst. Richtige Antworten wurden als 1 kodiert, falsche Antworten oder „Weiß nicht" wurden als 0 kodiert.

Masur et al. (2017) schlagen für die Online-Privatheitskompetenz ein Second-Order-Modell vor, bei dem jede Subdimension zusätzlich auf dem Globalfaktor lädt. Eine integrative konfirmatorische Faktorenanalyse über beide Messzeitpunkte, bei der die Faktorladungen der Items konstant gehalten wurden, passte gut zu den Daten, $\chi^2(658) = 1532$; $p < 0{,}001$, CFI = 0,96, TLI = 0,96, RMSEA = 0,04, 90 % CI [0,036; 0,041], SRMR = 0,07. Durch die hohe Validität und Reliabilität der OPLIS kann die latente Kompetenz jedoch ebenso durch den Summenscore abgebildet werden, welcher mit dem latenten Globalfaktor korrelierte ($r_{T1} = 0{,}96$, $r_{T2} = 0{,}96$). Die Online-Privatheitskompetenz kann als Quotient der richtigen Antworten dargestellt werden (T1: $M = 0{,}61$, $SD = 0{,}21$; T2: $M = 0{,}62$, $SD = 0{,}19$). Für die nachfolgenden Analysen nutzen wir entsprechend den Summenscore der 19 gestellten Fragen der OPLIS. Eine Auflistung der gesamten psychometrischen Eigenschaften der Online-Privatheitskompetenz für jedes Item lässt sich der Tabelle A2 im Appendix entnehmen.

Datenschutzverhalten. Das Datenschutzverhalten der Teilnehmenden wurde mit einer für diese Studie entwickelte Skala erfasst. Von ursprünglich acht Items wurden zwei ausgeschlossen. Ein Item wies hohe Redundanz zu einem weiteren Item auf („Im Internet schütze ich meine Daten eigentlich gar nicht"). Ein weiteres stellte sich zur Erfassung des hier definierten und untersuchten Datenschutzverhaltens als nicht spezifisch genug heraus („Ich verschleiere im Internet meine Identität durch die Angabe falscher Daten"). Die finale Skala besteht somit aus sechs Items („Ich schütze aktiv meine Daten, wenn ich das Internet nutze", „Ich tue viele Dinge, um meine Daten im Internet zu schützen", „Ich achte auf den Schutz meiner eigenen Daten im Internet", „Bevor ich ein Online-Angebot nutze, informiere ich mich, ob meine Daten dort sicher sind", „Ich nutze technische Hilfsmittel wie z. B. Anti-Tracking-Dienste, Anonymisierungstools oder Verschlüsselungsprogramme", „Ich wähle datenschutzfreundliche Apps oder Internet-Dienste"; siehe Tabelle A3 im Appendix). Diese wurden auf einer Skala von 1 (*„trifft überhaupt nicht zu"* bzw. *„nie"*) bis 5 (*„trifft voll und ganz zu"* bzw. *„sehr oft"*) beantwortet. Eine konfirmatorische Faktorenanalyse über beide Messzeitpunkte mit konstanten Faktorladungen zeigte einen akzeptablen Fit, $\chi^2(52) = 331{,}91$; $p < 0{,}001$, CFI = 0,94, TLI = 0,92, RMSEA = 0,08, 90 % CI [0,07, 0,09]. Der Mittelwert der Items bildete den Index für das Datenschutzverhalten (T1: $M = 3{,}30$, $SD = 0{,}84$; T2: $M = 3{,}30$, $SD = 0{,}84$). Zu beiden Zeitpunkten wies die Skala eine hohe Reliabilität auf ($\alpha_{T1} = 0{,}83$, $\omega_{T1} = 0{,}81$; $\alpha_{T2} = 0{,}82$, $\omega_{T2} = 0{,}81$). Eine Auflistung der gesamten psychometrischen Eigenschaften des Datenschutzverhaltens für jedes Item lässt sich der Tabelle A4 im Appendix entnehmen.

6. Ergebnisse

Das aufgestellte autoregressive CLPM weist einen guten Fit auf, $\chi^2(72) = 447{,}92$; $p < 0{,}001$, CFI = 0,95, TLI = 0,93, RMSEA = 0,08, 90 % CI [0,07, 0,08], SRMR = 0,08. Tabelle 2 zeigt eine Übersicht aller Pfadkoeffizienten des Modells. Auffällig ist zunächst, dass sowohl die Online-Privatheitskompetenz ($\beta = 0{,}76$) als auch das Datenschutzverhalten ($\beta = 0{,}78$) im Laufe eines Jahres sehr stabil bleiben. Die Teilnehmenden beantworteten zum Messzeitpunkt T1 im Durchschnitt $M = 11{,}56$ ($SD = 3{,}74$) und zum Messzeitpunkt T2 $M = 11{,}78$ ($SD = 3{,}63$) der 19 Fragen richtig. Jüngere Teilnehmende zeigten generell eine höhere Kompetenz (Korrelation Alter und Privatheitskompetenz: $r_{T1} = -0{,}17$, $p < 0{,}001$; $r_{T2} = -0{,}26$, $p < 0{,}001$). Weiterhin ging höhere Bildung mit einer höheren Online-Privatheitskompetenz einher (Korrelation Bildung und Privatheitskompetenz: $r_{T1} = 0{,}19$, $p < 0{,}001$; $r_{T2} = 0{,}22$, $p < 0{,}001$). Frauen beantworteten weniger Fragen richtig ($M = 11{,}08$) als Männer ($M = 12{,}43$; $t(894{,}35) = 5{,}65$, $p < 0{,}001$).

Im Querschnitt zum Zeitpunkt T1 zeigt sich bereits, dass Online-Privatheitskompetenz mit dem Datenschutzverhalten einhergeht ($b = 0{,}82$, 95 % CI [0,59, 0,04], $p < 0{,}001$, $\beta = 0{,}26$). Dies bedeutet, dass Personen, die auf der Online-Privatheitskompetenz-Skala eine Frage mehr richtig beantworteten als andere Personen, grundsätzlich auch 0,82 Punkte höher auf der Datenschutzverhaltensskala liegen. Somit zeigt die querschnittliche Messung zu T1, dass es einen kleinen (nach Cohen, 1992) bis mittelstarken (nach Funder & Ozer, 2019) positiven Zusammenhang zwischen Online-Privatheitskompetenz und Datenschutzverhalten gibt.

Mit Hypothese 1 nahmen wir an, dass die Online-Privatheitskompetenz zum Zeitpunkt T1 einen positiven Einfluss auf das Datenschutzverhalten zum Zeitpunkt T2 hat. Diese Annahme kann anhand unserer Daten bestätigt werden. Der Zusammenhang erwies sich als schwach positiv ($b = 0{,}02$, 95 % CI [0,01, 0,03], $p = 0{,}003$, $\beta = 0{,}07$). Personen,

Tabelle 2: Ergebnisse des Cross-Lagged Panel Models

Pfad	*b*	se	lower	upper	*p*	beta
Autoregressive Pfade						
OPLIS T1 → OPLIS T2	0,74	0,02	0,69	0,89	< 0,001	0,76
Datenschutz T1 → Datenschutz T2	0,79	0,03	0,74	0,84	< 0,001	0,78
Cross-Lagged Paths						
OPLIS T1 → Datenschutz T2	0,02	0,01	0,01	0,03	< 0,001	0,07
Datenschutz T1 → OPLIS T2	0,14	0,10	-0,06	0,34	0,170	0,03
Korrelationen						
OPLIS T1 ↔ Datenschutz T1	0,82	0,12	0,59	1,04	< 0,001	0,26
OPLIS T2 ↔ Datenschutz T2	0,07	0,05	-0,02	0,16	0,107	0,06

Anmerkung: Maximum Likelihood Schätzung, $\chi^2(72) = 447{,}92$; $p < 0{,}001$, CFI = 0,95, TLI = 0,93, RMSEA = 0,08, 90 % CI [0,07, 0,08], SRMR = 0,08. Basis: $n = 898$.

die zum Zeitpunkt T1 über eine höhere Online-Privatheitskompetenz verfügen, zeigen somit ein etwas höheres Datenschutzverhalten zu T2. Hypothese 1 wurde bestätigt.

In Hypothese 2 postulierten wir einen positiven Einfluss des Datenschutzverhaltens zu T1 auf die Online-Privatheitskompetenz zu T2. Diese Annahme konnte anhand unserer Daten nicht bestätigt werden. Der Zusammenhang war positiv, jedoch sehr klein und nicht signifikant ($b = 0{,}14$, 95 % CI [-0,06, 0,34], $p = 0{,}17$, $\beta = 0{,}03$). Hypothese 2 wurde abgelehnt.[1]

7. Diskussion

„Es wimmelt von gefährlichem Halbwissen! Ministerien informieren oftmals nicht vehement genug", „Eltern und Schulen müssen bei Vermittlung von Medienkompetenz mit anpacken" (digitalcourage.de[2]) oder „Deshalb ist es […] die Aufgabe der Schulen, die jungen Menschen in die Lage zu versetzen, selbstbewusst, selbstbestimmt und selbstkritisch von den Möglichkeiten und Chancen des Internets Gebrauch zu machen" (Landesbeauftragte für Datenschutz und Informationsfreiheit Rheinland-Pfalz[3]). Solche in der Literatur und im öffentlichen Diskurs häufig formulierten Aussagen finden sich in den Diskussionen der Fachartikel, in Feuilletons und wahlweise als Intro oder Abschluss von Policy-Papieren. Sie sind zudem ein finanzkräftiges Argument für die Förderung von Schulungsmaßnahmen und Forschungsanträgen. Selten jedoch wurde der Zusammenhang von Privatheitskompetenz und Datenschutz im Hinblick auf die damit implizierte Kausalität überprüft. Stimmt es also, dass eine Förderung der Privatheitskompetenz und Wissen über Privatheit dazu führen, dass Bürger:innen ihre Daten besser schützen? Ist die Forderung nach einer Förderung von Online-Privatheitskompetenz also gerechtfertigt?

1 Auch wenn bei den Analysen für soziodemografische Daten kontrolliert wird, zeigen sich dieselben Ergebnisse.

2 https://digitalcourage.de/blog/2020/datenschutz-als-medienkompetenz [01.03.2021].

3 https://www.datenschutz.rlp.de/de/themenfelder-themen/schulemedienkompetenz/ [01.03.2021].

Einhergehend mit vorherigen Studien zeigte sich, dass Personen mit einer höheren Online-Privatheitskompetenz grundsätzlich mehr Datenschutzmaßnahmen umsetzen (Querschnittsanalyse). Durch das Längsschnittdesign konnten wir jedoch weiterhin bestätigen, dass Menschen, die über mehr faktisches und prozedurales Wissen über Online-Privatheit verfügen, ihre Daten im Internet langfristig auch etwas mehr schützen. Im Zeitverlauf geht mehr Wissen also auch mit etwas mehr Datenschutz einher. In anderen Worten: Menschen, die heute mehr über Privatheit im Internet wissen, werden in einem Jahr ihre Daten besser schützen als andere. Dieses Ergebnis spricht theoretisch für die Annahmen des Prozessmodells der Online-Privatheitskompetenz (Masur et al., 2017) und praktisch für die Notwendigkeit und die Effektivität von Maßnahmen, die das Ziel einer stärkeren Förderung der Online-Privatheitskompetenz haben.

Weiterhin konnten wir auch untersuchen, inwiefern ein versiertes Datenschutzverhalten (zu T1) zu einem späteren Zeitpunkt (T2) zu einer Veränderung in der Privatheitskompetenz führt. Wir nahmen an, dass dieser Effekt zustande kommen könnte, weil die stärkere Auseinandersetzung mit Maßnahmen des Datenschutzes das Wissen über Privatheit erhöht. Dieser reziproke Effekt, also die Wirkung des Datenschutzverhaltens auf das Wissen, wurde jedoch nicht signifikant.

Zusammenfassend zeigen unsere *analytischen* Ergebnisse, dass das Wissen über Online-Privatheit und Datenschutz als relevanter Teilaspekt des selbstbestimmten und sicheren Umgangs mit sozialen Medien angesehen werden sollte. Unsere *theoretischen* Ausführungen legen nahe, dass der umfassende Wissenserwerb über Online-Privatheit in der heutigen digitalen Gesellschaft von zentraler Bedeutung ist (vgl. Gapski, 2020; Livingstone et al., 2019). Dabei ist es jedoch sehr wahrscheinlich, dass die Umsetzung von Datenschutzverhalten von weiteren Einflussvariablen mitbestimmt wird. Deshalb sollten zukünftig auch persönliche und situative Faktoren in die Analyse der Zusammenhänge von Wissen und Verhalten in Bezug auf Online-Privatheit miteinbezogen werden. Aus diesem Grund ordnen wir unsere Ergebnisse nachfolgend in den Gesamtkontext weiterer Faktoren, die das Datenschutzverhalten beeinflussen können, ein. Dadurch können Denkanstöße für die theoretische Erweiterung des Konzeptes der Online-Privatheitskompetenz gegeben und eine Grundlage für die Gestaltung von Handlungsempfehlungen zu besserem Datenschutzverhalten geschaffen werden.

Da sich nur ein schwach positiver Längsschnitteffekt von Online-Privatheitskompetenz auf Datenschutzverhalten zeigte, ist es denkbar, wie bereits im Prozessmodell ausformuliert (vgl. Abschnitt 4), dass Wissen allein nicht ausreicht, um eine wesentliche Verhaltensveränderung in Bezug auf den Datenschutz in digitalen und sozialen Medien hervorzurufen. Neben deklarativem und prozeduralem Wissen bedarf es der Reflexionsfähigkeit, damit potenzielle Privatheitsrisiken mit den eigenen Privatheitsbedürfnissen abgeglichen und unter Berücksichtigung des deklarativen Wissens als Risiken erkannt werden und langfristig zu einer stabilen Verhaltensveränderung führen können (Masur, 2018). Die Bedeutsamkeit der Kritikfähigkeit von Nutzenden wurde bereits in Bezug auf die Medienkompetenz von Sowka et al. (2015) hervorgehoben. Entsprechend wäre eine Erweiterung bisheriger Konzeptualisierungen und Operationalisierungen zur empirischen Messung von Online-Privatheitskompetenz um zusätzliche Dimensionen und Items der Kritikfähigkeit hilfreich.

Weiterhin können aus psychologischer Perspektive personale Faktoren (z. B. Bedürfnisse, Wahrnehmungen, Kommunikationsziele, Persönlichkeitseigenschaften) und Kontextfaktoren (z. B. Charakteristiken und Affordanzen einer Webseite) eine besondere Rolle für die Umsetzung von Datenschutzverhalten von Internetnutzenden darstellen (Masur, 2019; Schäwel, 2019; Trepte, 2020a). Intrinsische Bedürfnisse (z. B. das

Bedürfnis nach Eingebundenheit) oder spezifische Ziele einer computervermittelten Kommunikation (z. B. beim Online-Dating, Sexting) können dem Wunsch nach Privatheit entgegenstehen und somit dazu beitragen, dass trotz Wissens um Risiken und Gefahren kein Datenschutz umgesetzt wird (Krämer & Schäwel, 2020). Persönlichkeitseigenschaften können das Online-Privatheitsverhalten von Internetnutzenden lenken, indem sie bedingen, wie intensiv sich Personen selbst offenbaren – z. B. enthalten die Statusupdates auf Facebook von Personen mit einer eher narzisstisch ausgeprägten Persönlichkeit intimere und persönlichere Informationen als die Updates von Personen mit einer geringeren Narzissmus-Ausprägung (Winter et al., 2014). Weiterhin kann die individuelle Ausprägung des Narzissmus die Intention einer Person verstärken, die eigene Privatheit auf sozialen Netzwerkseiten zu kontrollieren (Ahn et al., 2015). Die persönliche Wahrnehmung der Online-Privatheit kann ebenso einen Einfluss darauf haben, ob und welche privatheitsschützenden Maßnahmen herangezogen werden (Dienlin, 2014; Kruikemeier et al., 2020).

Affordanzen sozialer Medien und verschiedener Online-Dienste können ebenso einen Einfluss auf das Online-Privatheits- und Datenschutzverhalten von Nutzenden ausüben (Treem & Leonardi, 2012; Trepte, 2020a). Affordanzen sozialer Medien, also die Interaktion von Nutzungsweisen und Funktionalitäten, eröffnen den Nutzenden bestimmte Handlungsoptionen und zeichnen sich durch einen konkreten Aufforderungscharakter aus (Evans et al., 2017; Gibson, 1979[2014]). In Abhängigkeit davon, welche Affordanzen präsent sind (z. B. die Affordanz „Assoziation“) und welche Handlungsoptionen in Folge dessen von Nutzenden digitaler Medien verwendet werden (z. B. Verlinkung auf sozialen Netzwerkseiten), kann das Ausmaß der individuellen und interdependenten Privatheit variieren (z. B. verringert sich der Grad der Privatheit durch eine öffentlich einsehbare Verlinkung auf einem Foto auf einer sozialen Netzwerkseite). Interdependent deshalb, weil nicht nur die verlinkende Person, sondern auch Personen, welche (möglicherweise ohne Zustimmung) verlinkt werden, trotz potenziell hoher Online-Privatheitskompetenz einem höheren Risiko einer Verletzung der Privatheit ausgesetzt sind (Trepte, 2020a). Die Überführung von faktischem und prozeduralem Wissen in tatsächliches Verhalten kann also massiv von personenspezifischen und kontextuellen Faktoren beeinflusst werden. Solche psychologischen und verhaltensbeeinflussenden Determinanten, welche den Abruf des Wissens und situative Kritikfähigkeit beeinflussen können, sollten in zukünftiger Forschung berücksichtigt und mit dem hier vorgestellten Konzept der Online-Privatheitskompetenz in Verbindung gebracht werden.

In Bezug auf die gesellschaftliche Schutzverantwortung lassen sich folgende theoretische Grundlagen für praktische Handlungsempfehlungen ableiten. Zunächst kann umfassende Medien- und Online-Privatheitskompetenz durch verschiedene Akteure, zum Beispiel Lehrende, Erziehende, Forschende sowie Politiker:innen, und vor allem deren Kooperation vermittelt werden (Gapski, 2020). Diese kooperative Anstrengung und die Kombination von edukativen und politischen Maßnahmen haben das Potenzial, Reflektionsprozesse anzustoßen und die kritische Reflektion zur Routine werden zu lassen. Während diese Reflektion im ersten Schritt adressiert, welche sozialen Normen im Bereich der Online-Privatheit vorherrschen, so betreffen sie im zweiten Schritt immer auch die Frage, welche Maßnahmen in einer demokratischen Auseinandersetzung mit dem Thema Datenschutz und Online-Privatheitskompetenz erforderlich sind und aktiv eingeleitet werden können, um sowohl individuelle als auch interdependente Strategien der Online-Privatheit hervorzubringen. Damit einhergehend stellt Masur (2020) fest, dass die Bemühungen der Forschung, Individuen zu schützen, zu stärken und zu belehren,

stets nur eine Symptombehandlung eines gesellschaftlichen Problems darstellen. Dementsprechend sind hier noch einmal die legislativen und politischen Erfolge sowie die Maßnahmen der Datenschützer:innen, Verbraucherschützer:innen und Aktivistinnen und Aktivisten zu benennen, die Ursachen der Risiken für Internetnutzende eruieren, um ihnen entgegenzuwirken (z. B. Potthast, 2019; Rebiger, 2018; Reihs, 2019).

7.1. Limitationen und Ausblick

Eine erste Limitation bezieht sich auf die zeitlichen Abstände des Längsschnittdesigns. In dieser Studie wurden die Online-Privatheitskompetenz sowie das selbstberichtete Datenschutzverhalten der Teilnehmenden zu zwei Messzeitpunkten mit einem Abstand von einem Jahr analysiert. Obwohl dieses Design erste vielversprechende Ergebnisse hervorbrachte, ist nach wie vor unklar, über welchen Zeitraum eine umfassende Wirkung der Privatheitskompetenz auf das Datenschutzverhalten zu erwarten ist. Es ist denkbar, dass ein entsprechender Effekt besser über kürzere Abstände zwischen einzelnen Wellen oder über eine noch längere Gesamtuntersuchungszeit beobachtbar wäre.

Weiterhin ist eine eindeutige Trennung von intra- (within) und interindividuellen (between) Prozessen erst mithilfe von mehr als zwei Messzeitpunkten möglich (Hamaker et al., 2015). Zukünftige Studien sollten entsprechend untersuchen, über welchen Zeitraum der Effekt der Kompetenz auf das Verhalten am stärksten ausgeprägt ist und dabei mehr als zwei Wellen erheben um within- und between-person-Varianz klar voneinander zu trennen. Mehr Wellen würden darüber hinaus erlauben, die weiteren Schritte der Verhaltensänderung, wie sie im Prozessmodell der Online-Privatheitskompetenz (Masur et al., 2017) vorgeschlagen sind, umfassend untersuchen zu können. Zusätzliche Messzeitpunkte könnten einen verdichteten Einblick in die einzelnen Prozessschritte erlauben und ein detaillierteres Bild der Wechselwirkungen zwischen Wissen und berichtetem Verhalten nachzeichnen, wodurch umfassendere Strategien zur Förderung von Online-Privatheitskompetenz erarbeitet und umgesetzt werden könnten.

Die Operationalisierung des Datenschutzverhaltens erfolgte anhand von Selbstberichten. Es erfolgte jedoch keine konkrete Beobachtung des tatsächlich umgesetzten Verhaltens. Es ist somit möglich, dass das berichtete Verhalten von dem tatsächlich umgesetzten Verhalten der Teilnehmenden abweicht. Solche Abweichungen können zum Beispiel durch eine verzerrte Wahrnehmung des befragten Individuums entstehen oder das Resultat der sozialen Erwünschtheit in einer Test- oder Umfragesituation sein. Eine Untersuchung des Einflusses des Wissens auf tatsächliche Verhaltensweisen könnte anhand eines experimentellen Settings oder anhand einer Kombination von Umfragedaten, Wissenstests und von Tracking-Daten in zukünftigen Studien analysiert werden (Stier et al., 2019). Eine weitere Kritik an der Operationalisierung ist, dass nur ein Teilbereich des Datenschutzverhaltens abgefragt wurde. Die Items wurden eher allgemein anstatt spezifisch formuliert. Zukünftige Studien könnten das Datenschutzverhalten alternativ spezifisch entlang der Dimensionen der Online-Privatheitskompetenz operationalisieren (z. B. Umsetzung von konkreten Maßnahmen, die durch Datenschutzgesetze und -richtlinien gegeben sind). Die Online-Privatheitskompetenz wurde anhand der OPLIS (Masur et al., 2017) ermittelt. Mit dieser Skala werden die Dimensionen (1) institutionelle und organisationale Praktiken, (2) technische Aspekte der Online-Privatheit und des Datenschutzes, (3) rechtliche Aspekte des Datenschutzes und (4) Nutzungsstrategien für die individuelle Privatheitsregulierung erfasst. Die hier als relevant eruierte Erweiterung der Online-Privatheitskompetenz nach Masur (2018) wurde anhand dieses Messinstrumentes nicht abgedeckt.

Eine weitere Limitation dieser Studie ist, dass keine Drittvariablen in die Analysen miteinbezogen wurden, die die Stärke des Einflusses der Online-Privatheitskompetenz auf das Datenschutzverhalten moderieren könnten (z. B. individuelle und Kontextfaktoren; siehe Abschnitt 7).

7.2. Fazit

In dieser Studie wurde untersucht, ob eine höhere Online-Privatheitskompetenz langfristig zu mehr Datenschutzverhalten, oder ob die Umsetzung von Datenschutzverhalten umgekehrt zu mehr Online-Privatheitskompetenz führt. Die Ergebnisse einer zweiwelligen Längsschnittstudie zeigen, dass höhere Online-Privatheitskompetenz mit Datenschutzverhalten zusammenhängt. Langfristig gibt es einen schwach positiven Effekt der Online-Privatheitskompetenz auf das Datenschutzverhalten, jedoch nicht umgekehrt. Dies spricht dafür, dass Initiativen zur Förderung einer allgemeinen Medienkompetenz und einer spezifischen Online-Privatheitskompetenz in der Tat sinnvoll sind, da sie langfristig zu einem selbstbestimmteren und sichereren Umgang mit privaten Daten im Internet führen können.

Förderhinweis

Diese Forschung wurde vom Deutschen Bundesministerium für Bildung und Forschung (BMBF) gefördert, Grant 16KIS0094, vergeben an Sabine Trepte (PI).

Literaturverzeichnis

Ackerman, P. L., Beier, M. E. & Bowen, K. R. (2002). What we really know about our abilities and our knowledge. *Personality and Individual Differences*, *33*(4), 587–605. https://doi.org/10.1016/S0191-8869(01)00174-X.

Ahn, H., Kwolek, E. A. & Bowman, N. D. (2015). Two faces of narcissism on SNS: The distinct effects of vulnerable and grandiose narcissism on SNS privacy control. *Computers in Human Behavior*, *45*, 375–381. https://doi.org/10.1016/j.chb.2014.12.032.

Altman, I. (1974). Privacy: A conceptual analysis. In S. T. Margulis (Hg.), *Man-environment interactions: Evaluations and applications* (S. 3–28). Dowden, Hutchinson & Ross.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Brooks/Cole Publishing Company.

Baacke, D. (1996). Medienkompetenz: Begrifflichkeit und sozialer Wandel. In A. von Rein (Hg.), *Theorie und Praxis der Erwachsenenbildung: Medienkompetenz als Schlüsselbegriff* (S. 112–124). Klinkhardt.

Bartsch, M. & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022.

Baruh, L., Secinti, E. & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276.

Bazarova, N. N. & Masur, P. K. (2020). Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology. *Current Opinion in Psychology*, *36*, 118–123. https://doi.org/10.1016/j.copsyc.2020.05.004.

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155–159. https://doi.org/10.1037/0033-2909.112.1.155.

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz & J. M. Mönig (Hg.), *Medien und Privatheit [Media and privacy]* (S. 105–122). Karl Stutz.

Dienlin, T. & Metzger, M. J. (2016). An extended privacy calculus model for SNSs – Analyzing self-disclosure and self-withdrawal in a U.S. representative sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163.

Epstein, D. & Quinn, K. (2020). Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media + Society*, *6*(2). https://doi.org/10.1177/2056305120916853.

European Commission (2015). *Europeans' attitudes towards security. Special Eurobarometer 432.* Brüssel, Belgium.

European Commission (2019). *Special Eurobarometer 480: Europeans' attitudes towards Internet security*, 1–278. https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2207 [01.03.2021].

Evans, S. K., Pearce, K. E., Vitak, J. & Treem, J. W. (2017). Explicating affordances: A conceptual framework for understanding affordances in communication research. *Journal of Computer-Mediated Communication*, *22*(1), 35–52. https://doi.org/10.1111/jcc4.12180.

Funder, D. C. & Ozer, D. J. (2019). Evaluating effect size in psychological research: Sense and nonsense. *Advances in Methods and Practices in Psychological Science*, *2*(2), 156–168. https://doi.org/10.1177/2515245919847202.

Gapski, H. (2020). Diskussionsfelder der Medienpädagogik: Datafizierte Lebenswelten und Datenschutz. In K. Hugge, U. Sander & F. von Gross (Hg.), *Handbuch Medienpädagogik* (S. 1–10). Springer. https://doi.org/10.1007/978-3-658-25090-4_82-1.

Gibson, J. J. (1979 [2014]). *The ecological approach to visual perception*. *Psychology Press & Routledge Classic Editions*. Taylor and Francis.

Groeben, N. (2002). Anforderungen an die theoretische Konzeptualisierung von Medienkompetenz. In N. Groeben & B. Hurrelmann (Hg.), *Medienkompetenz. Voraussetzungen, Dimensionen, Funktionen* (S. 11–22). Juventa.

Groeben, N. (2004). Medienkompetenz. In R. Mangold, P. Vorderer & G. Bente (Hg.), *Lehrbuch der Medienpsychologie* (S. 27–50). Hogrefe.

Hair, J. F., Black, W. C., Babin, B. J. & Anderson, R. E. (2014). *Multivariate data analysis* (Seventh edition). Pearson Education Limited.

Hamaker, E. L., Kuiper, R. M. & Grasman, R. P. P. P. (2015). A critique of the cross-lagged panel model. *Psychological Methods*, *20*(1), 102–116. https://doi.org/10.1037/a0038889.

Hoffmann, C. P., Lutz, C. & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4). https://doi.org/10.5817/CP2016-4-7.

Hoofnagle, C., King, J., Li, S. & Turow, J. (2010). *How different are young adults from older adults when it comes to information privacy attitudes and policies*. http://ssrn.com/abstract=1589864.

Huang, H.-Y. (2016). Examining the beneficial effects of individual's self-disclosure on the social network site. *Computers in Human Behavior*, *57*, 122–132. https://doi.org/10.1016/j.chb.2015.12.030.

Krämer, N. C. & Schäwel, J. (2020). Mastering the challenge of balancing self-disclosure and privacy in social media. *Current Opinion in Psychology*, 67–71. https://doi.org/10.1016/j.copsyc.2019.08.003.

Kraus, L., Wechsung, I. & Möller, S. (2014). A comparison of privacy and security knowledge and privacy concern as influencing factors for mobile protection behavior. *Workshop on Privacy Personas and Segmentation (PPS) at the Symposium on Usable Privacy and Security (SOUPS)*. http://cups.cs.cmu.edu/soups/2014/workshops/privacy/s2p4.pdf [01.03.2021].

Kruikemeier, S., Boerman, S. C. & Bol, N. (2020). Breaching the contract? Using social contract theory to explain individuals' online behavior to safeguard privacy. *Media Psychology*, *23*(2), 269–292. https://doi.org/10.1080/15213269.2019.1598434.

Kumar, P. C., Subramaniam, M., Vitak, J., Clegg, T. L. & Chetty, M. (2020). Strengthening children's privacy literacy through contextual integrity. *Media and Communication*, *8*(4), 175–184. https://doi.org/10.17645/mac.v8i4.3236.

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems*, *28*(1), 453–496. http://aisel.aisnet.org/cais/vol28/iss1/28.

Liu, D., Ainsworth, S. E. & Baumeister, R. F. (2016). A meta-analysis of social networking online and social capital. *Review of General Psychology*, *20*(4), 369–391. https://doi.org/10.1037/gpr0000091.

Liu, Q., Yao, M. Z., Yang, M. & Tu, C. (2017). Predicting users' privacy boundary management strategies on Facebook. *Chinese Journal of Communication*, *10*(3), 295–311. https://doi.org/10.1080/17544750.2017.1279675.

Livingstone, S. (2004). The challenge of changing audiences. Or, what is the audience researcher to do in the age of the internet? *European Journal of Communication*, *19*(1), 75–86.

Livingstone, S., Ólafsson, K. & Staksrud, E. (2013). Risky social networking practices among „underage" users: Lessons for evidence-based policy. *Journal of Computer-Mediated Communication*, *18*(3), 303–320. https://doi.org/10.1111/jcc4.12012.

Livingstone, S., Stoilova, M. & Nandagiri, R. (2019). *Children's data and privacy online: growing up in a digital age: an evidence review*. London School of Economics and Political Science, Department of Media and Communications. http://eprints.lse.ac.uk/101283 [01.03.2021].

Lutz, C., Hoffmann, C. P. & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society*, *22*(7), 1168–1187. https://doi.org/10.1177/1461444820912544.

Mandl, H. & Spada, H. (Hg.) (1988). *Wissenspsychologie*. Psychologie Verlags Union.

Masur, P. K. (2018). Mehr als Bewusstsein für Privatheitsrisiken: Eine Rekonzeptualisierung der Online-Privatheitskompetenz als Kombination aus Wissen, Fähig- und Fertigkeiten. *Medien & Kommunikationswissenschaft*, *66*(4), 446–465. https://doi.org/10.5771/1615-634X-2018-4-446.

Masur, P. K. (2019). *Situational privacy and self-disclosure: Communication processes in online environments*. Springer International Publishing.

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, *8*(2), 258–269. https://doi.org/10.17645/mac.v8i2.2855.

Masur, P. K., Teutsch, D. & Dienlin, T. (2018). Privatheit in der Online-Kommunikation. In W. Schweiger & K. Beck (Hg.), *Springer Reference Sozialwissenschaften. Handbuch Online-Kommunikation* (Bd. 3, S. 1–29). Springer. https://doi.org/10.1007/978-3-658-18017-1_16-1.

Masur, P. K., Teutsch, D., Dienlin, T. & Trepte, S. (2017). Online-Privatheitskompetenz und deren Bedeutung für demokratische Gesellschaften. *Forschungsjournal Soziale Bewegungen*, *30*(2), 180–188. https://doi.org/10.1515/fjsb-2017-0039.

Masur, P. K., Teutsch, D. & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). *Diagnostica, 63*, 256–268.. https://doi.org/10.1026/0012-1924/a000179.

Meinfelder, F. (2009). *Analysis of incomplete survey data – Multiple imputation via bayesian bootstrap predictive mean matching*. Bamberg: opus.

Millham, M. H. & Atkin, D. (2018). Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors. *New Media & Society*, *20*(1), 50–67. https://doi.org/10.1177/1461444816654465.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338.

Park, Y. J. & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, *38*, 296–303. https://doi.org/10.1016/j.chb.2014.05.041.

Pedersen, D. M. (1999). Model for types of privacy by privacy functions. *Journal of Environmental Psychology*, *19*, 397–405. https://doi.org/10.1006/jevp.1999.0140.

Potthast, K. C. (2019). *Political Microtargeting – Zwischen Regulierungsbegehren und Ungewissheit*. https://www.juwiss.de/103-2019/.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, *15*(1). https://doi.org/10.5210/fm.v15i1.2775.

Rebiger, S. (2018). Offener Brief: Europäische Parteien sollen auf Microtargeting verzichten. *Netzpolitik.org.* https://netzpolitik.org/2018/offener-brief-eu-parteien-sollen-auf-microtargeting-verzichten/ [01.03.2021].

Reihs, V. (10. April 2019). Politisches Microtargeting in Deutschland: Ich sehe was, was du nicht siehst. *politik-digital*. https://politik-digital.de/news/politisches-microtargeting-in-deutschland-ich-sehe-was-was-du-nicht-siehst-155876/ [01.03.2021].

Rosenthal, S., Wasenden, O.-C., Gronnevet, G.-A. & Ling, R. (2019). A tripartite model of trust in Facebook: Acceptance of information personalization, privacy concern, and privacy literacy. *Media Psychology*, *9182*(2), 1–25. https://doi.org/10.1080/15213269.2019.1648218.

Rosseell, Y. (2012). lavaan: An R package for structural equation modeling. *Journal of Statistical Software*, *48*(2). http://www.jstatsoft.org/v48/i02/paper [01.03.2021].

Schäwel, J. (2019). *How to raise users' awareness of online privacy*. University of Duisburg-Essen.

Schmidt, J.-H. (2018). *Social media* (2. Aufl.). *Medienwissen kompakt*. Springer Fachmedien Wiesbaden.

Sowka, A., Klimmt, C., Hefner, D., Mergel, F. & Possler, D. (2015). Die Messung von Medienkompetenz. Ein Testverfahren für die Dimension „Medienkritikfähigkeit" und die Zielgruppe „Jugendliche". *Medien & Kommunikationswissenschaft*, *63*(1), 62–82. https://doi.org/10.5771/1615-634x-2015-1-62.

Statistisches Bundesamt (2019). *Bevölkerung: Deutschland, Stichtag, Altersjahre*. https://www-genesis.destatis.de/genesis/online?operation=previous&levelindex=1&step=1&titel=Ergebnis&levelid=1611333386018&acceptscookies=false#abreadcrumb[4] [01.03.2021].

Statistisches Bundesamt (2020). *Bildung, Forschung und Kultur*. https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bildung-Forschung-Kultur/Bildungsstand/_inhalt.html [01.03.2021].

Stier, S., Breuer, J., Siegers, P. & Thorson, K. (2019). Integrating survey data and digital trace data: Key issues in developing an emerging field. *Social Science Computer Review*, *11*. https://doi.org/10.1177/0894439319843669.

Treem, J. W. & Leonardi, P. M. (2012). Social media use in organizations. Exploring the affordances of visibility, editability, persistence, and association. *Communication Yearbook*, *36*, 143–189. https://doi.org/10.1080/23808985.2013.11679130.

Trepte, S. (2015). Social media, privacy, and self-disclosure: The turbulence caused by social media's affordances. *Social Media and Society*, *1*(1), 1–2. https://doi.org/10.1177/2056305115578681.

Trepte, S. (2016a). Medienkompetenz. In N. C. Krämer, S. Schwan, D. Unz & M. Suckfüll (Hg.), *Medienpsychologie: Schlüsselbegriffe und Konzepte* (S. 108–114). Kohlhammer.

Trepte, S. (2016b). Die Zukunft der informationellen Selbstbestimmung – Kontrolle oder Kommunikation? In Stiftung Datenschutz (Hg.), *DatenDebatten: Band 1. Zukunft der informationellen Selbstbestimmung* (S. 159–170). Erich Schmidt Verlag.

Trepte, S. (2020a). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory*, *19*(4), 1–22. https://doi.org/10.1093/ct/qtz035.

Trepte, S. (2020b). The Privacy Longitudinal Study [Dataset]. Leibniz-Institut für Sozialwissenschaften (gesis). https://doi.org/10.7802/2117.

Trepte, S. & Dienlin, T. (2014). Privatsphäre im Internet. In T. Porsch & S. Pieschl (Hg.), *Neue Medien und deren Schatten* (S. 53–80). Hogrefe.

Trepte, S. & Masur, P. K. (2017). *Privacy attitudes, perceptions, and behaviors of the German population: Research report of a representative survey study*. University of Hohenheim.

Trepte, S. & Scharkow, M. (2016). Friends and lifesavers: How social capital and social support received in media environments contribute to well-being. In L. Reinecke & M. B. Oliver (Hg.), *Routledge handbook of media use and well-being* (S. 305–316). Routledge.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A. & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the „online privacy literacy scale" (OPLIS). In S. Gutwirth, R. Leenes & P. d. Hert (Hg.), *Law, governance and technology series: volume 20. Reforming European data protection law* (S. 333–365).

Tsay-Vogel, M., Shanahan, J. & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media & Society*, *20*(1), 141–161. https://doi.org/10.1177/1461444816660731.

4 Angegeben ist die Altersverteilung der deutschen Bevölkerung für die unter 1-Jährigen bis über 85-Jährigen im Jahre 2019. In der vorliegenden Stichprobe wurden nur Personen ab 16 Jahren berücksichtigt. Deshalb wurde das Durchschnittsalter der deutschen Bevölkerung nur für die Personen ab 16 Jahren berechnet.

Turow, J. (2003). *Americans and online privacy. The system is broken. Report from the Annenberg Public Policy Center of the University of Pennsylvania*. Philadelphia, PA.
van Buuren, S. (2012). *Flexible Imputation of Missing Data*. Chapman & Hall/CRC.
van Buuren, S. & Groothuis-Oudshoorn, K. (2011). mice: Multivariate imputation by chained equations in R. *Journal of Statistical Software*, *45*(3). https://doi.org/10.18637/jss.v045.i03.
Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, *56*(4), 451–470. https://doi.org/10.1080/08838151.2012.732140.
Vitak, J., Blasiola, S., Patil, S. & Litt, E. (2015). Balancing audience and privacy tensions on social network sites. *International Journal of Communication*, *9*, 1–20. https://doi.org/10.1016/j.chb.2013.10.004.
von Pape, T., Trepte, S. & Mothes, C. (2017). Privacy by disaster? Press coverage of privacy and digital technology. *European Journal of Communication*, *10*(4). https://doi.org/10.1177/0267323117689994.
Westin, A. F. (1967). *Privacy and freedom*. Atheneum.
Winter, S., Neubaum, G., Eimler, S. C., Gordon, V., Theil, J., Herrmann, J., Meinert, J. & Krämer, N. C. (2014). Another brick in the Facebook wall – How personality traits relate to the content of status updates. *Computers in Human Behavior*, *34*, 194–202. https://doi.org/10.1016/j.chb.2014.01.048

Appendix

Tabelle A1: Itemformulierungen und Antwortmöglichkeiten der Online-Privatheitskompetenzskala (OPLIS)

Item-bezeichnung	Itemformulierung	Antwortoptionen
OPL_GES_01	Die Weiterleitung anonymisierter Nutzerdaten zu Marktforschungszwecken ist in der EU gesetzlich erlaubt.	„wahr“, „falsch“
OPL_GES_02	Die EU-Richtlinien zum Datenschutz…	„...existieren bisher noch nicht“, „...gelten als länderübergreifendes EU-Datenschutzgesetz“, „...geben den EU-Ländern lediglich eine unverbindliche Orientierung hinsichtlich ihrer Datenschutzgesetze“, „...müssen von allen EU-Ländern in das nationale Datenschutzgesetz implementiert werden“
OPL_GES_03	Für alle sozialen Netzwerkseiten gelten in Deutschland die gleichen Standard-AGBs. Abweichungen müssen von den Betreibern kenntlich gemacht werden.	„wahr“, „falsch“
OPL_GES_04	Laut dem deutschen Gesetz haben Nutzer von Online-Anwendungen, die personenbezogene Daten erheben und verarbeiten, einen Anspruch darauf, die über sie gespeicherten Daten einzusehen.	„wahr“, „falsch“
OPL_GES_05	Informationelle Selbstbestimmung ist…	„... ein philosophischer Begriff“, „... ein Grundrecht deutscher Bürger“, „... die zentrale Forderung datenverarbeitender

Item-bezeichnung	Itemformulierung	Antwortoptionen
		Stellen“, „... die zentrale Aufgabe des Bundesdatenschutzbeauftragten“
OPL_ PRA_01	Die National Security Agency (NSA) greift nur auf Nutzerdaten zu, die öffentlich und für jedermann zugänglich sind.	„wahr“, „falsch“
OPL_ PRA_02	Betreiber sozialer Netzwerke (z. B. Facebook) sammeln und verarbeiten auch Informationen von Personen, die dieses Netzwerk gar nicht nutzen.	„wahr“, „falsch“
OPL_ PRA_03	Daten, die Betreiber sozialer Netzwerke (z. B. Facebook) über die Nutzer sammeln, werden nach 5 Jahren gelöscht.	„wahr“, „falsch“
OPL_ PRA_04	Unternehmen kombinieren Daten, die auf verschiedenen Websites im Internet hinterlassen werden, und stellen daraus Nutzerprofile zusammen.	„wahr“, „falsch“
OPL_ PRA_05	E-Mails werden häufig über mehrere Rechner weitergeleitet, bevor sie bei ihrem eigentlichen Empfänger ankommen.	„wahr“, „falsch“
OPL_ STR_01	Das Nachverfolgen der eigenen Internetnutzung kann durch das regelmäßige Löschen von Browserinformationen (Cookies, Cache, Browserverlauf) erschwert werden.	„wahr“, „falsch“
OPL_ STR_02	Durch das Surfen im „Private Browsing“-Modus kann die Rekonstruktion des eigenen Surfverhaltens erschwert werden, da keine Browserinformationen gespeichert werden.	„wahr“, „falsch“
OPL_ STR_03	Durch die Nutzung von falschen Namen oder Pseudonymen kann die Identifikation der eigenen Person im Internet zumindest erschwert werden.	„wahr“, „falsch“
OPL_ STR_04	Auch wenn selbst schwere Passwörter von IT-Profis geknackt werden können, ist es sinnvoll, Passwörter zu verwenden, die aus einer Kombination aus Buchstaben, Zahlen und Sonderzeichen bestehen und keine Wörter, Namen oder einfache Zahlenkombinationen enthalten.	„wahr“, „falsch“
OPL_ STR_05	Um den Zugang zu eigenen Daten zu erschweren, sollte man verschiedene Passwörter und Benutzernamen für unterschiedliche Anwendungen nutzen und diese häufig ändern.	„wahr“, „falsch“

Item-bezeichnung	Itemformulierung	Antwortoptionen
OPL_TEC_01	Was verbirgt sich hinter dem Begriff „Browserverlauf"? Im Browserverlauf werden …	„...Cookies von besuchten Websites abgelegt", „...potenziell infizierte Webseiten separat abgelegt", „...die Adressen der besuchten Websites gespeichert", „...je nach Browsertyp unterschiedliche Informationen über den Nutzer gespeichert"
OPL_TEC_04	Was versteht man unter einem „Trojaner"? Das ist ein Computerprogramm, das …	„... als nützliche Anwendung getarnt ist, im Hintergrund aber eine andere Funktion erfüllt", „... den Rechner vor Viren und anderen Schadprogrammen schützt", „... nur zum Spaß entwickelt wurde und keine spezifische Funktion hat", „... als Computervirus in den 90ern Schaden anrichtete, heute aber nicht mehr existiert"
OPL_TEC_02	Was ist ein „Cookie"?	„Ein Programm, mit dem man die Datenspeicherung von Webanbietern unterbinden kann", „Ein Computer-Virus, das man sich beim Besuch einer Website einfangen kann", „Eine Text-Datei, die es Websites ermöglicht, den Nutzer beim erneuten Besuch wiederzuerkennen", „Ein Browser-Plug-In, das sicheres Surfen gewährleistet"
OPL_TEC_05	Was ist eine „Firewall"?	„Ein veraltetes Schutzprogramm gegen Computer-Viren", „Ein Browser-Plugin, welches sicheres Surfen ermöglicht", „Ein Sicherungssystem, das ein Rechennetz oder einen einzelnen Computer vor unerwünschten Netzangriffen schützen soll", „Eine neue technische Entwicklung, die verhindert, dass Daten bei einem Kurzschluss verloren gehen"
OPL_GES_01	Die Weiterleitung anonymisierter Nutzerdaten zu Marktforschungszwecken ist in der EU gesetzlich erlaubt.	„wahr", „falsch"
OPL_GES_02	Die EU-Richtlinien zum Datenschutz…	„...existieren bisher noch nicht", „...gelten als länderübergreifendes EU-Datenschutzgesetz", „...geben den EU-Ländern lediglich eine unverbindliche Orientierung hinsichtlich ihrer Datenschutzgesetze", „...müssen von allen EU-Ländern in das nationale Datenschutzgesetz implementiert werden"
OPL_GES_03	Für alle sozialen Netzwerkseiten gelten in Deutschland die gleichen Standard-AGBs. Abweichungen müssen von den Betreibern kenntlich gemacht werden.	„wahr", „falsch"
OPL_GES_04	Laut dem deutschen Gesetz haben Nutzer von Online-Anwendungen, die personenbezogene Daten erheben und verarbeiten, einen Anspruch da-	„wahr", „falsch"

Item-bezeichnung	Itemformulierung	Antwortoptionen
	rauf, die über sie gespeicherten Daten einzusehen.	
OPL_GES_05	Informationelle Selbstbestimmung ist…	„... ein philosophischer Begriff“, „... ein Grundrecht deutscher Bürger“, „... die zentrale Forderung datenverarbeitender Stellen“, „... die zentrale Aufgabe des Bundesdatenschutzbeauftragten“
OPL_ PRA_01	Die National Security Agency (NSA) greift nur auf Nutzerdaten zu, die öffentlich und für jedermann zugänglich sind.	„wahr“, „falsch“
OPL_ PRA_02	Betreiber sozialer Netzwerke (z. B. Facebook) sammeln und verarbeiten auch Informationen von Personen, die dieses Netzwerk gar nicht nutzen.	„wahr“, „falsch“
OPL_ PRA_03	Daten, die Betreiber sozialer Netzwerke (z. B. Facebook) über die Nutzer sammeln, werden nach 5 Jahren gelöscht.	„wahr“, „falsch“

Tabelle A2: Psychometrische Eigenschaften der Variable Online-Privatheitskompetenz zu T1(T4) und T2 (T5)

	M	*SD*	Min	Max	Schiefe	Kurtosis
Online-Privatheitskompetenz T1 (T4)	0,58	0,19	0	0,95	-0,56	-0,07
OPL_GES_01	0,51	0,50	0	1	-0,04	-2,00
OPL_GES_02	0,22	0,42	0	1	1,32	-0,27
OPL_GES_03	0,32	0,47	0	1	0,78	-1,39
OPL_GES_04	0,47	0,50	0	1	0,12	-2,00
OPL_GES_05	0,43	0,49	0	1	0,30	-1,91
OPL_PRA_01	0,71	0,45	0	1	-0,95	-1,10
OPL_PRA_02	0,38	0,49	0	1	0,48	-1,78
OPL_PRA_03	0,51	0,50	0	1	-0,03	-2,00
OPL_PRA_04	0,85	0,35	0	1	-2,01	2,04
OPL_PRA_05	0,54	0,50	0	1	-0,17	-1,97
OPL_STR_01	0,63	0,48	0	1	-0,54	-1,71
OPL_STR_02	0,29	0,45	0	1	0,94	-1,11
OPL_STR_03	0,70	0,46	0	1	-0,86	-1,27
OPL_STR_04	0,96	0,20	0	1	-4,71	20,21
OPL_STR_05	0,96	0,20	0	1	-4,50	18,28
OPL_TEC_01	0,63	0,48	0	1	-0,54	-1,71
OPL_TEC_02	0,71	0,45	0	1	-0,94	-1,11
OPL_TEC_04	0,86	0,34	0	1	-2,13	2,53
OPL_TEC_05	0,86	0,34	0	1	-2,10	2,41
Online-Privatheitskompetenz T2 (T5)	0,59	0,18	0	0,95	-0,49	-0,06
OPL_GES_01	0,51	0,50	0	1	-0,04	-2,00
OPL_GES_02	0,21	0,41	0	1	1,40	-0,05
OPL_GES_03	0,36	0,48	0	1	0,57	-1.68
OPL_GES_04	0,44	0,50	0	1	0,25	-1,94
OPL_GES_05	0,44	0,50	0	1	0,24	-1,95
OPL_PRA_01	0,64	0,48	0	1	-0,57	-1,68
OPL_PRA_02	0,44	0,50	0	1	0,26	-1,93
OPL_PRA_03	0,52	0,50	0	1	-0,09	-1,99
OPL_PRA_04	0,84	0,36	0	1	-1,89	1,57
OPL_PRA_05	0,64	0,48	0	1	-0,57	-1,68
OPL_STR_01	0,67	0,47	0	1	-0,74	-1,46
OPL_STR_02	0,32	0,47	0	1	0,78	-1,40
OPL_STR_03	0,69	0,46	0	1	-0,85	-1,29
OPL_STR_04	0,97	0,18	0	1	-5,12	24,27
OPL_STR_05	0,98	0,15	0	1	-6,18	36,21
OPL_TEC_01	0,62	0,48	0	1	-0,51	-1,74
OPL_TEC_02	0,77	0,42	0	1	-1,27	-0,38
OPL_TEC_04	0,85	0,35	0	1	-1,98	1,94
OPL_TEC_05	0,85	0,36	0	1	-1,96	1,84

Tabelle A3: Itemformulierungen von Datenschutzverhalten

Itembezeichnung	Itemformulierung
SEI_ODS_01	Ich schütze aktiv meine Daten, wenn ich das Internet nutze.
(SEI_ODS_02	Im Internet schütze ich meine Daten eigentlich gar nicht.*)
SEI_ODS_03	Ich tue viele Dinge, um meine Daten im Internet zu schützen.
SEI_ODS_04	Ich achte auf den Schutz meiner eigenen Daten im Internet.
ODV_01	Bevor ich ein Online-Angebot nutze, informiere ich mich, ob meine Daten dort sicher sind.
(ODV_02	Ich verschleiere im Internet meine Identität durch die Angabe falscher Daten.)
ODV_03	Ich nutze technische Hilfsmittel wie z. B. Anti-Tracking-Dienste, Anonymisierungstools oder Verschlüsselungsprogramme.
ODV_04	Ich wähle datenschutzfreundliche Apps oder Internet-Dienste.

Anmerkung. *Invertiertes Item, Items in Klammern wurden nicht in die Analyse mit einbezogen

Tabelle A4: Psychometrische Eigenschaften der Variable Datenschutzverhalten zu T1(T4) und T2 (T5)

	M	*SD*	Min	Max	Schiefe	Kurtosis
Datenschutzverhalten T1 (T4)	3,9	0,91	1	5	-0,66	-0,08
SEI_ODS_01	3,9	1,02	1	5	-0,68	-0,13
SEI_ODS_02_rev [a]	4,1	1,09	1	5	-1,09	0,29
SEI_ODS_03	3,5	1,13	1	5	-0,39	-0,68
SEI_ODS_04	3,9	0,97	1	5	-0,76	0,11
ODV_01	3,3	1,17	1	5	-0,24	-0,83
ODV_02 [a]	1,7	0,95	1	5	1,26	0,97
ODV_03	2,0	1,27	1	5	0,95	-0,36
ODV_04	3,1	1,29	1	5	-0,29	-1,00
Datenschutzverhalten T2 (T5)	3,9	0,92	1	5	-0,68	-0,09
SEI_ODS_01	3,9	0,99	1	5	-0,69	0,00
SEI_ODS_02_rev [a]	4,2	1,04	1	5	-1,15	0,44
SEI_ODS_03	3,5	1,14	1	5	-0,36	-0,74
SEI_ODS_04	3,9	1,02	1	5	-0,79	0,00
ODV_01	3,3	1,16	1	5	-0,22	-0,79
ODV_02 [a]	1,7	0,94	1	5	1,28	0,89
ODV_03	2,0	1,27	1	5	0,96	-0,36
ODV_04	3,1	1,25	1	5	-0,38	-0,86

Anmerkung. [a]Items wurden nicht in das Modell einbezogen.