

Das Privacy Paradox aus psychologischer Perspektive

Preprint

Tobias Dienlin

Diesen Preprint bitte wie folgt zitieren:

Dienlin, T. (2019). Das Privacy Paradox aus psychologischer Perspektive. In L. Specht, S. Werry, & N. Werry (Eds.), *Handbuch Datenrecht und Digitalisierung* (pp. 305–323). Erich Schmidt Verlag.

Weitere Informationen zum Handbuch sind hier erhältlich:

<https://www.esv.info/lp/datenrecht/>

Einleitung

Das Privacy Paradox besagt, dass Menschen beim Nutzen von Online-Diensten bereit sind, große Mengen personenbezogener Daten zu teilen – selbst dann, wenn ihnen Privatsphäre wichtig ist und sie um diese besorgt sind (Treppe & Teutsch, 2016).

Dies führt an mancher Stelle zu Verwunderung, Bedenken oder gar Zynismus, und es lassen sich verschiedene kritische Fragen stellen. Beispielsweise: Warum sind viele Menschen bereit, im Internet Informationen zu offenbaren, die doch eigentlich privat sind (Pew Research Center, 2013)?¹ Ist es nicht paradox, dass sich einige um ihre Privatheit sorgen (European Commission, 2015), aber dennoch viele aktives Mitglied auf sozialen Netzwerkseiten (SNS) wie Facebook, Instagram oder Snapchat sind?² Warum gingen bei der Volkszählung im Jahre 1987 noch tausende Menschen auf die Straße, um gegen die Sammlung vermeintlich harmloser Daten wie Wohnsituation und Erwerbstätigkeit zu protestieren (Reymann, 2011), sind aber jetzt bereit, intimere Daten wie Fotos, Hobbies und sexuelle Orientierung mit privatwirtschaftlichen Unternehmen zu teilen? Ist die Fülle der produzierten Daten nicht bedenklich – zumal diese meist auch noch auf Servern im Ausland liegen, für welche nicht das vergleichsweise strenge Datenschutzgesetz der Bundesrepublik Deutschland gilt?³ Sind die Parallelen zu Orwells 1984, Benthams Panoptikum oder den Praktiken ehemaliger Nachrichtendienste wie der ‚Stasi‘ nicht offenkundig (Seele & Zapf, 2017)? Zusammengefasst: Ist das nicht paradox?

Der vorliegende Beitrag greift diese Fragen, Beobachtungen sowie Bedenken auf und versucht, in verständlicher Sprache und Form, Antworten aus einer psychologischen Perspektive anzubieten. Das Privacy Paradox stellt aktuell eine wichtige gesellschaftliche Frage dar, die in Medien und an Stammtischen entsprechend rege diskutiert wird. Es gibt viele journalistische Artikel zu dem Thema (Seemann, 2013), einen eigenen darauf verweisenden Wikipedia-Eintrag (Wikipedia, 2018) und sogar spezifische Websites, die sich ausschließlich damit beschäftigen, das Privacy Paradox näher zu erklären (New York Public Radio, 2018). Ein interessanter Aspekt des Privacy Paradox ist dabei die Tatsache, dass es zum einen ein Alltagsphänomen darstellt, das intuitiv zugänglich ist und umgangssprachlich diskutiert werden kann. Zum anderen ist es aber auch ein akademisches Problem, das methodisch dezidiert untersucht wird und eine eigene Forschungsgeschichte sowie -dynamik aufweist. Im Beitrag möchte ich sowohl den intuitiven Zugang bedienen, indem ich zuerst allgemeine und le-

¹Beispielsweise posten 62% aller amerikanischer Teenager ihren Beziehungsstatus auf SNSs; 82% posten ihr Geburtsdatum.

²In Deutschland nutzten im Mai 2017 30 Millionen Menschen Facebook, 15 Millionen Instagram (Statista, 2017).

³Vgl. Ablehnung des Safe-Harbour Abkommens (bspw. Holland, Datenschutz bei Facebook & Co.: EuGH erklärt Safe Harbor für ungültig - <https://www.heise.de/newsticker/meldung/Datenschutz-bei-Facebook-Co-EuGH-erklaert-Safe-Harbor-fuer-ungueltig-2838025.html> (25.01.2018)).

icht zugängliche Betrachtungen zu Privatheit, Verhalten und dem Internet voranstelle, als auch den akademischen, indem ich aktuelle Forschungsergebnisse analysiere.

In den zwei einführenden Abschnitten dieses Beitrages lege ich somit zunächst dar, was Privatheit aus psychologischer Perspektive bedeutet und anschließend, wie sich menschliches Verhalten – ganz allgemein betrachtet – erklären lässt. Denn, um das Privacy Paradox bestmöglich verstehen zu können, ist es hilfreich, zuerst ein grundlegendes Verständnis von menschlichem Verhalten zu gewinnen. Dies hilft, die später berichteten Forschungsarbeiten und Ergebnisse zum Privacy Paradox besser einordnen zu können. Anschließend übertrage ich diese allgemeinen Aspekte auf den Kontext des Internets. Hierbei stelle ich zuerst *personenbezogene* Faktoren vor, die Online-Verhalten erklären können, gefolgt von *umgebungsbezogenen*. Im anschließenden Teil widme ich mich dem Privacy Paradox aus einer spezifischen, primär akademischen Perspektive, indem die bisherige Forschungshistorie zusammengefasst und aktuelle Studienergebnisse analysiert werden. Abschließend folgt eine Diskussion des Privacy Paradox: Hier finden eine individuelle Bewertung, gesellschaftliche Implikationen mit Handlungsempfehlungen sowie ein eigenständiges Fazit statt.

Was ist Privatheit?

Klassischerweise starten Ausführungen zur Definition von Privatheit mit der Beobachtung, dass Privatheit ein komplexes und schwer zu fassendes theoretisches Phänomen darstellt (Nissenbaum, 2010) – eine Einschätzung, der ich mich anschließe. Die Tatsache, dass Privatsphäre ein geläufiges Wort mit intuitivem Zugang ist, suggeriert eine bisweilen trügerische Gewissheit, das dahinterliegende Konstrukt auch tatsächlich inhaltlich zu verstehen. Über die Definition und den Umfang von Privatheit gibt es in akademischen Diskursen verschiedene Auffassungen. Es lassen sich zwei Perspektiven unterscheiden: Zum einen die Auffassung von Privatheit als Maß der *Abgeschiedenheit*, der Trennung vom sozialen Umfeld. Als Beispiel: Sobald ein Nutzer auf Facebook anstatt seines vollständigen korrekten Namens einen Alias verwendet, ist er weniger und schlechter erreichbar, somit abgeschiedener und privater. Als prominenter Vertreter wird hier häufiger Alan Westin genannt (Westin, 1967). In diesem Verständnis lässt sich im Übrigen auch die juristische Sphärentheorie der Privatheit verorten, welche zwischen Sozialsphäre, Privatsphäre und Intimsphäre unterscheidet (Geminn & Roßnagel, 2015). Die Privatsphäre ist somit eine spezifische Ausprägung auf der allgemeinen Skala der Privatheit. (Entsprechend verwende ich in diesem Kapitel, wenn es um das Phänomen an sich geht, anstatt „Privatsphäre“ stets den Begriff „Privatheit“.) Auf der anderen Seite gibt es die Auffassung, dass Privatheit die *Kontrolle* über Abgeschiedenheit darstellt und Menschen nur dann privat sind, wenn sie selbst beeinflussen können, mit wem sie wie interagieren. Als Beispiel: Sobald ein Unternehmen verschiedene Seiten und Kommunikationskanäle für seine Mitarbeiter sperrt, wären diese

zwar abgeschieden, aber nicht in Kontrolle über ihre Abgeschiedenheit, somit auch nicht privat. Prominente Vertreterin ist hier beispielsweise Judee Burgoon (Burgoon, 1982). Neuere Definitionen verbinden beide Ansätze:

„Die Privatheit eines Menschen bemisst in erster Linie, wie stark sich dieser aus der Gesellschaft zurückzieht. Privatheit ist somit ein Maß der individuellen *Abgeschiedenheit*. Eine hohe Privatheit bedeutet also gleichzeitig eine hohe Abgeschiedenheit. Diese Abgeschiedenheit kann dabei sowohl als horizontaler Rückzug von anderen Menschen, oder als vertikaler Schutz vor institutioneller Überwachung betrachtet werden. Eine zusätzliche notwendige Bedingung von Privatheit besteht darin, dass diese Abgeschiedenheit selbstbestimmt erfolgen muss. Privatheit ist somit auch dadurch bedingt, dass die Abgeschiedenheit einer gewissen *Freiwilligkeit* und *Kontrollmöglichkeit* unterliegt“ (Masur et al., 2018).

In der Definition wird zudem eine weitere Unterscheidung vorgenommen: vertikale und horizontale Privatheit. Diese Unterscheidung geht in den Grundzügen auf Barry Schwartz zurück, der als einer der ersten unterschied, gegenüber welcher Entität Menschen Privatheit suchen (Schwartz, 1968). Horizontale Privatheit meint dabei Personen, die auf einem vergleichbaren sozialen Niveau stehen – etwas umfassender betrachtet geht es somit um interpersonale Privatheit. Demgegenüber beschreibt vertikale Privatheit verschiedenrangige Personen, wie etwa Autoritäten und Vorgesetzte oder Kinder und Schutzbefohlene – etwas weiter gefasst ebenso Institutionen, Unternehmen oder Dienstleister. Diese Unterscheidung kann insofern hilfreich sein, als dass die eigene Privatheitsregulation auf der horizontalen Ebene bisweilen besser gelingt als auf der vertikalen (Masur et al., 2018).

Im Vorausgegangenen klingt eine weitere wichtige Prämisse des aktuellen Privatheitsverständnisses an, nämlich die der Privatheitsregulation. Zurückgehend auf den Sozialpsychologen Irwin Altman wird häufig betont, dass Privatheit keinen absoluten, rigiden Zustand darstellt, der grundsätzlich gut oder schlecht, erstrebenswert oder zu vermeiden wäre (Altman, 1976). Im Gegenteil: Ein optimales Privatheitsniveau liegt demgemäß genau dann vor, wenn das gewünschte Maß an Privatheit dem tatsächlichen entspricht. Beide sind wohlgeartet einer ständigen Schwankung unterlegen. Darüber hinaus postuliert Judee Burgoon, dass Privatheit auf mehreren Dimensionen existiert – der informationalen (wie viele identifizierende Daten liegen über Personen vor?), der psychologischen (wie frei sind Menschen darin, zu denken und Ansichten zu äußern?), der sozialen (wie viele Menschen haben Zugang zu persönlichen Informationen?) und der physischen (wie stark abgeschottet und entfernt sind Personen?) (Burgoon, 1982).

Viele der vorangegangenen Auffassungen und Positionen habe ich in dem sogenannten Privacy Process Model (PPM) synthetisiert (Dienlin, 2014). Als zusätzliche Annahme postuliert das PPM, dass sich eine Unterscheidung zwischen objektivem Privatheitskontext und subjektiver Privatheitswahrnehmung lohnt. Bisweilen fühlen sich Menschen – gerade auch im Internet, etwa auf SNS –

privat, obwohl ihr objektiver Kontext wohl vielmehr als öffentlich eingeschätzt werden müsste (Trepte & Reinecke, 2011). Diese Diskrepanz vermag somit unterschiedliches „Fehlverhalten“ von Menschen abzubilden, die im Internet persönliche Dinge offenbaren, obwohl der Kontext hierzu objektiv betrachtet bisweilen wenig geeignet erscheint.

Wie lässt sich Verhalten erklären?

Interessanterweise ist das Privacy Paradox – rein strukturell betrachtet – ein klassisches Problem der Psychologie. Es betrifft sie sogar in ihrem wissenschaftlichen Kern. Denn dem Privacy Paradox liegt die Fragestellung zugrunde: Wie lässt sich menschliches Verhalten erklären? Welche Faktoren beeinflussen dieses und wann wird welcher Faktor relevant? Lässt sich Verhalten beeinflussen, gegebenenfalls korrigieren? Zusammengefasst geht es somit auch beim Privacy Paradox um die Erklärung menschlichen Verhaltens – und hierfür gilt folgende Prämisse:

“As every student of psychology knows, explaining human behavior in all its complexity is a difficult task” (Ajzen, 1991).

Die einfachste Formel, um menschliches Verhalten zu erklären, wurde von Kurt Lewin im Rahmen seiner Feldtheorie entwickelt (Lewin, 1935). Sie lautet:

$$V = f(P, U).$$

Die Formel besagt, dass Verhalten, in erster Instanz, eine nicht näher bestimmte Funktion von Person und Umwelt (oder auch Umgebung, Umfeld, Situation) darstellt. Der gleiche Mensch wird sich in unterschiedlichen Umgebungen verschieden verhalten. Unterschiedliche Menschen in gleicher Umgebung ebenso. Je mehr Informationen über Person und Umwelt vorliegen, umso besser können wir das Verhalten vorhersagen; gleichzeitig ist die Vorhersage von Verhalten nie perfekt, sondern stets fehlerbehaftet und approximativ. Informationen über Person und Umwelt steigern zwar die Erklärungswahrscheinlichkeit, sie genügen allerdings nie, um Verhalten vollständig voraussagen zu können. Zusammengefasst spricht dies für ein sogenanntes *probabilistisches* Verständnis: Spezifisches Verhalten lässt sich stets nur mit einer bestimmten Wahrscheinlichkeit vorhersagen.

Als konkretes Beispiel: Mittels der sogenannten Theory of Planned Behavior lassen sich mindestens 18% und maximal 38% der Varianz von Verhalten erklären (Sutton, 1998); das Technology Acceptance Model erklärt ca. 40% (Venkatesh & Bala, 2008). Es bleiben stets viele Unbekannte – in manchen Bereichen gelingt die Erklärung besser, in anderen schlechter. Wichtig ist allerdings, dass Informationen über Person und Umwelt nicht allein deswegen verworfen werden sollten, weil sie Verhalten nicht komplett erklären können. Selbst geringe Verhaltensänderungen und -erklärungen können wertvoll

sein. Als Veranschaulichung: Psychologische Studien zeigen, dass Warnhinweise bei Werbung mit der erhöhten Wahrscheinlichkeit einhergehen, dass Menschen diese (mit einer sehr geringen Wahrscheinlichkeit) befolgen und sich (marginal) sicherer verhalten. Die durchschnittliche Korrelation beträgt dabei $r = .16$ (oder umgerechnet: ca. 3% des Verhaltens lassen sich durch die Warnhinweise erklären) (Witte & Allen, 2000).

Es stellt sich nun die Frage, was das für die Praxis bedeutet und ob ein solcher Zusammenhang überhaupt relevant ist? Betrachten wir einmal folgendes, konkretes Beispiel aus dem Alltag: Im Jahr 2015 hat die EU Kommission entschieden, dass auf sämtlichen Zigarettenpackungen große Warnhinweise in Form abschreckender Bilder abgedruckt sein müssen. Viele Raucher und Medien verneinen, dass dies einen Effekt auf ihr Verhalten hätte. Gleichzeitig berichtet das statistische Bundesamt, dass im Folgejahr insgesamt 6,3 Milliarden Zigaretten weniger versteuert wurden, was einem Rückgang von 7,7% entspricht – nach vorausgegangener Stabilität über mehrere Jahre hinweg (Statistisches Bundesamt, 2017). Selbstverständlich lässt sich nicht beweisen, dass es sich hierbei um einen kausalen Zusammenhang handelt; allerdings erscheint dieser im Kontext der Forschungsergebnisse und Theorie durchaus plausibel. Die Krux ist: Einflussfaktoren auf Verhalten sind häufig gering, lassen sich subjektiv nicht nachempfinden, finden allerdings objektiv statt, können skalieren und somit beträchtliche Relevanz erlangen. Wenn es beispielsweise um die Verlängerung der Lebenserwartung oder die Senkung von Kosten im Gesundheitssystem geht, können auch kleine Einflüsse in der Summe große Effekte ergeben.

Zu beachten ist: Sowohl Personen- als auch Umweltvariablen sind stets multifaktoriell. Auf der Personenebene entscheiden über das Verhalten Faktoren wie Biographie, Lernerfahrung, Persönlichkeit, Einstellung, Motivation oder Physiologie (z.B. Physiognomie, Hormonhaushalt, Stimmung, Wachheit, Hunger, Durst). Auf der Umweltebene sind dies beispielsweise die Präsenz und das Verhalten anderer Personen, Verhaltenskontingenzen (i.e., Verstärkung vs. Bestrafung von Verhalten), Verhaltensoptionen, Affordanzen (i.e., Struktur und Handlungsaufforderungscharakter von Objekten), Normen und Traditionen. Sämtliche diese Faktoren wirken somit zugleich, auf ihre eigene Art und Weise, zu unterschiedlichen Zeitpunkten und unterschiedlich stark.

Wie lässt sich Verhalten im Internet verstehen?

Personenbezogene Faktoren

Menschen offenbaren vor allem deswegen persönliche Informationen im Internet, weil sie daraus verschiedene Vorteile ziehen können. Zu nennen sind hier vor allem das Knüpfen und Aufrechterhalten sozialer Beziehungen, Freundschaften

und Partnerschaften, unmittelbare Informationsgewinnung, Persönlichkeitsentwicklung, Identitäts- und Reputationsmanagement, Aufwandsreduzierung, Angebotserweiterung, Niedrigschwelligkeit oder finanzielle Vergünstigungen (Smock et al., 2011). Menschen erhalten vielfältigen Nutzen durch das Kommunizieren von Informationen – wäre dies nicht der Fall, so hätte das Internet schwerlich so viele Kommunikationsabläufe derart tiefgreifend verändern können. Dies führt sogar soweit, dass Einige die verschiedenen Nutzungsvorteile, ähnlich einer Droge, als das eigentliche Problem betrachten. Sinngemäß: Das Internet ist nicht gefährlich, weil es so schlecht ist – im Gegenteil, das Internet ist gefährlich, weil es so gut ist (in Anlehnung an Miller, 2014).

Neben diesen Positivfaktoren, welche die Selbstoffenbarung erhöhen, gibt es auch Negativfaktoren, welche die Selbstoffenbarung reduzieren. So zeigen verschiedene Studien, dass Menschen, die sich vermehrt Sorgen um ihre Privatheit machen, im Durchschnitt auch etwas weniger personenbezogene Informationen kommunizieren (Baruh et al., 2017). Diese Negativfaktoren sind dabei allerdings meist weniger wichtig als die Anzahl der Vorteile, die Menschen mit der Nutzung assoziieren (Dienlin & Metzger, 2016). Wie im Abschnitt „Das Privacy Paradox“ noch näher ausgeführt werden wird, berichten sowohl aktuelle Forschungsergebnisse als auch eine Meta-Analyse vergangener Studien, dass Privatheitssorgen mit Selbstoffenbarung signifikant korrelieren. Gleichzeitig zeigen die Ergebnisse aber auch, dass die Korrelation nicht besonders stark ist. In anderen Worten: Das Privacy Paradox trifft in seiner Extremform – nämlich, dass sich Privatheitssorgen gar nicht im Verhalten widerspiegeln – aller Wahrscheinlichkeit nach nicht zu. Nichtsdestoweniger kann postuliert werden, dass sich die Sorgen und Ängste noch stärker im Verhalten zeigen sollten.

Umweltbezogene Faktoren

Hinsichtlich umweltbezogener Faktoren ist der vermutlich wichtigste Einfluss die wahrgenommene subjektive Norm (Fishbein & Ajzen, 2010). Viele Theorien der Psychologie stehen somit in der Tradition des Konstruktivismus: Es entscheidet weniger das tatsächliche Verhalten des Umfelds, sondern vielmehr die individuelle psychologische Wahrnehmung dessen. Sobald eine kritische Anzahl an Personen in der sozialen Umgebung Online-Dienste nutzen, erhöht dies die eigene Nutzungswahrscheinlichkeit signifikant. Beispielsweise steht die wahrgenommene subjektive Norm, dass man das soziale Netzwerk Facebook nutzen sollte, in direktem Zusammenhang mit der Wahrscheinlichkeit, selbst Facebook zu nutzen (Niemann & Schenk, 2014). In einer Studie mit 1042 Jugendlichen aus Flandern stieg die Wahrscheinlichkeit, personenbezogene Daten bei Online-Käufen anzugeben, sobald eher geglaubt wurde, dass dies eine gängige soziale Norm darstellt (Heirman et al., 2013). Subjektive Normen wirken dabei primär auf zwei Arten und Weisen: injunktiv und deskriptiv.

Injunktive Normen bedeuten, dass das soziale Umfeld eine konkrete Erwartung stellt: Eltern erwarten von ihren Kindern, dass diese höflich sind, Vorgeset-

zte von ihren Mitarbeitern, dass diese pünktlich am Arbeitsplatz erscheinen, Partner von einander, dass sie aufmerksam zugehören. Injunktive Normen sind aktiv, sie werden konkret geäußert und eingefordert. Übertragen auf die Informationsweitergabe im Internet wäre eine injunktive Norm, dass beim Posten von persönlichen Informationen Vorsicht walten sollte. In einer Informationsbroschüre von „Schau hin“ (ein Beratungsangebot des Bundesministeriums für Familie, Senioren, Frauen und Jugend und verschiedenen öffentlichen Medien) wird darauf hingewiesen, dass „sensible Daten wie Name, Telefonnummer und Adresse nicht an Fremde weitergegeben werden sollten und im Netz nichts zu suchen haben“ (Schau hin, 2017). Grundsätzlich berichten Medien in Deutschland meist kritisch gegenüber SNS (Teutsch & Niemann, 2016).

Demgegenüber wirken deskriptive Normen passiv. Sie besagen, dass das soziale Umfeld allein durch gezeigtes Verhalten eine Norm erzeugen kann. Sobald Eltern sich selbst höflich und freundlich verhalten, der Vorgesetzte selbst pünktlich erscheint und der eine Partner aufmerksam zuhört, wird solches Verhalten eher zur sozialen Norm. Übertragen auf den hiesigen Anwendungskontext: Das allgemein gezeigte Verhalten im Internet prägt ebenso stets das individuell umgesetzte. Sobald Eltern selbst soziale Medien aktiv nutzen, hat dies einen anteiligen Einfluss auf ihre Kinder. Wichtig zu beachten ist, dass sämtliche Normen vorrangig für solche Bezugsgruppen der Umgebung gelten, welche als relevant erachtet werden. Die Bedeutsamkeit verändert sich dabei im Laufe der persönlichen Entwicklung: In der Kindheit ist die Familie meist die erste Instanz, in der Adoleszenz die Peer-Group, später der professionelle Kontext, gefolgt von erneut der Familie (Lang et al., 2006).

Zusammengefasst: Die Sorge um die Privatheit ist, wie vorab ausgeführt, ein Faktor unter vielen, welcher signifikant mit Selbstopffenbarung korreliert, diese womöglich determiniert. Die grundsätzliche Erwartungshaltung an die prädiktive und kausale Kapazität von Privatheitssorgen sollte entsprechend konservativ ausfallen. Trotz Privatheitssorgen offenbaren Menschen situativ persönliche Information; selbst Edward Snowden – ein Mensch, der sich von allen wohl mit am meisten um seine Privatheit sorgt – hat mittlerweile ein eigenes Twitter Profil,⁴ das er rege nutzt und damit Rückschlüsse ermöglicht, welche seine Privatheit reduzieren.

Das Privacy Paradox

Historie

Im Folgenden widme ich mich nun der spezifischen und expliziten Forschung zum Privacy Paradox. Das Privacy Paradox weist eine wissenschaftliche Historie auf, die mindestens bis in das Jahr 2004 zurückreicht. Die Forschergruppe

⁴<https://twitter.com/Snowden> (25.01.2018).

rund um Alessandro Acquisti war die erste, welche empirische Studien durchführte, die aufzeigten, dass Diskrepanzen zwischen Privatheitseinstellungen und Privatheitsverhalten vorliegen (Acquisti et al., 2015). Susan Barnes war gemäß meinen Recherchen dann die erste, welche explizit den Begriff „Privacy Paradox“ prägte (Barnes, 2006). In ihrem vielzitierten Essay bewerte Barnes das Verhalten von jungen Menschen auf SNS als grundsätzlich paradox. Sie listete hierbei verschiedene Beobachtungen auf: Beispielsweise, dass junge Menschen nicht erkennen würden, dass SNS öffentliche Räume darstellen, dass die Informationsweitergabe insgesamt betrachtet zu hoch sei und dass selbst solche Personen, die sich über die Öffentlichkeit der Netzwerke bewusst wären, dennoch viele Informationen kommunizierten. Anschließend befassten sich verschiedene Forscher auch empirisch explizit mit der Thematik des Privacy Paradox. Auf der einen Seite gab es Studien, welche das Privacy Paradox unterstützten: Zu den einflussreichsten zählen hierzu die Studien von Monika Taddicken und Zeynep Tufekci. Taddicken zeigte in einer Studie mit 2739 Befragten in Deutschland, dass Privatheitssorgen nicht signifikant mit Privatheitsverhalten zusammenhängen (Taddicken, 2014). Tufekci berichtete, dass es in ihrer Stichprobe nahezu keinen Zusammenhang zwischen Privatheitssorgen und dem Preisgeben von Informationen in SNS gab (Tufekci, 2008). Auf der anderen Seite entstanden auch Studien, welche dem Privacy Paradox widersprachen. Beispielsweise fanden Utz und Krämer in einer Befragung von 217 Personen, dass Privatheitssorgen und -verhalten signifikant korrelierten (Utz & Krämer, 2009). Ebenso berichteten Wannes und Heirman, dass Privatheitssorgen einen indirekten Zusammenhang mit Selbstoffenbarung vorwiesen (Heirman et al., 2013). (Eine mögliche Erklärung der Unterschiedlichkeit der Ergebnisse folgt im Abschnitt Analyse des Privacy Paradox.)

Interessanterweise entstand neben der Forschung zum Privacy Paradox ebenso der Forschungsstrang zum sogenannten *Privacy Calculus*. Beide Stränge existierten parallel, ohne größere Verbindung der jeweiligen Ergebnisse. Dies könnte daran liegen, dass das Privacy Paradox – meiner Wahrnehmung nach – vorrangig in der Disziplin der Kommunikationswissenschaft und Medienpsychologie angesiedelt war, wohingegen der Privacy Calculus eher aus dem Bereich der Informationssysteme stammt. Im Gegensatz zum Privacy Paradox besagt der Privacy Calculus das genaue Gegenteil: Wohingegen das Paradox postuliert, dass sich Sorgen und Ängste nicht im Verhalten zeigen, argumentiert der Calculus, dass sowohl Sorgen und Ängste als auch Vorteile und Gratifikationen das Verhalten beeinflussen. Gemäß dem Privacy Calculus wägen Menschen Vor- und Nachteile gegeneinander ab und entscheiden sich zur Informationsweitergabe, sobald Vorteile die Nachteile überwiegen. Der Privacy Calculus geht auf die Arbeiten von Laufer und Wolfe zurück, welche den Privacy Calculus bereits in regulären, analogen – nicht nur in digitalen – Lebensverhältnissen vermuteten (Laufer & Wolfe, 1977). Culnan und Armstrong übertrugen ihn auf Informationsweitergabe im Kontext von Online-Shopping (Culnan & Armstrong, 1999), Krasnova und Kollegen auf SNS (Krasnova et al., 2010). Studien zum Calculus zeigten, dass beide Faktoren mit Online-Verhalten statistisch signifikant zusam-

menhängen: Wenn Menschen Vorteile in der Weitergabe sehen, offenbaren sie mehr Informationen. Wenn Sie Risiken wahrnehmen und/oder Angst um ihre Privatheit haben, offenbaren sie weniger Informationen (Krasnova et al., 2010). Der Privacy Calculus Ansatz unterscheidet sich somit stark vom Privacy Paradox, er trägt in den Grundzügen das Bild des homo oeconomicus, steht in der Tradition des Rational Choice Paradigmas (Simon, 1955). Gleichzeitig gilt auch hier das probabilistische Prinzip: Vor- und Nachteile erklären Verhalten anteilig, aber nie ganzheitlich. Als konkretes Beispiel: In einer US-repräsentativen Studie fanden wir, dass ca. 33% der Selbstoffenbarung durch antizipierte Vorteile erklärt werden konnte und 5% durch empfundene Privatheitssorgen (Dienlin & Metzger, 2016).

Eine grundsätzliche Perspektive sozialwissenschaftlicher empirischer Forschung ist diejenige, dass Einzelstudien inhaltliche Fragestellungen selten abschließend beantworten können. Einzelstudien können zum einen Schwachstellen haben und zum anderen – rein statistisch bedingt – falsche Positiv-Befunde sein. Entsprechend bedarf es der Aggregation mehrerer (hochwertiger) Studien, um mögliche Inferenzen besser gegen den Zufall abzusichern. Wie berichtet, liegen bezüglich des Privacy Paradox bisweilen unterschiedliche Ergebnisse von Einzelstudien vor. Mittlerweile gibt es allerdings auch eine erste Meta-Studie, welche die Ergebnisse von 37 verschiedenen Einzelstudien aggregierte (Baruh et al., 2017). Die Autoren kamen zu dem Schluss, dass Privatheitsängste und das Teilen von Informationen auf SNS schwach negativ korrelieren ($r = -.13$): Menschen, die sich mehr um ihre Privatheit sorgten, waren entsprechend etwas weniger bereit, persönliche Informationen über sich zu verbreiten. Es lässt sich an dieser Stelle konstatieren, dass sich Privatheitsängste mit großer Wahrscheinlichkeit – und entgegen der Annahme des Privacy Paradox – im Verhalten zeigen, aber dass dieser Einfluss nicht besonders stark und im Einzelfall nur schwer konstatierbar ist. Über mehrere Personen hinweg lässt er sich allerdings statistisch nachweisen und könnte somit – ähnlich der Warnhinweisen auf Zigarettenspackungen – gesellschaftlich relevant und von allgemeiner Bedeutung sein.

Analyse

Wie lassen sich die teils unterschiedlichen Ergebnisse der Studien erklären, warum fanden manche Studien keinen Zusammenhang zwischen den Variablen? Zum einen liegt dies an den bereits ausgeführten Punkten: Es sollte grundsätzlich nicht davon ausgegangen werden, dass Privatheitssorgen einen Großteil des Online-Verhaltens beeinflussen können, sondern lediglich einen kleinen bis mittleren Anteil. Wichtig dabei: Man sollte grundsätzlich von der Existenz dieses kleinen bis mittleren Einflusses ausgehen – die spezifischen personen- und umweltbezogenen Faktoren sowie Studienergebnisse wurden hierzu bereits genannt. Nichtsdestoweniger gibt es durchaus Faktoren, welche den Zusammenhang abschwächen können, beziehungsweise zu erklären vermögen, warum der Zusammenhang eben nicht groß ist. Im Folgenden führe ich nun zuerst

verschiedene *inhaltliche* Gründe auf, welche den Einfluss von Privatheitssorgen abschwächen. Anschließend diskutiere ich mögliche *methodische* Aspekte, weshalb manche Studien keine signifikanten Effekte zeigen konnten.

Als eine der ersten analysierten Alessandro Acquisti und Jens Grossklags das Phänomen aus psychologischer Perspektive. Sie nannten unter anderem drei überzeugende Gründe, warum es womöglich doch keinen Zusammenhang gibt: (1) psychological distortions, (2) hyperbolic discounting, (3) bounded rationality. Psychological distortions beinhalten unter anderem, dass sich Menschen zwar um ihre Privatheit sorgen, sie aber nicht über ausreichend Selbstkontrolle verfügen, um ihre Daten für sich zu behalten. So zeigte sich beispielsweise, dass Personen, die eine höhere Selbstwirksamkeitserwartung bezüglich des Schutzes von Privatheit aufweisen, diesen ebenso mit größerer Wahrscheinlichkeit umsetzen (Dienlin & Metzger, 2016). Hyperbolic discounting meint, dass sich Menschen zwar um ihre Privatheit sorgen, aber, dass diese langfristigen Sorgen aufgrund der kurzfristigen Vorteile in den Hintergrund treten. Kurzfristige Konsequenzen, seien sie positiv oder negativ, bestimmen das Verhalten stärker als langfristige; im Fall von Selbstoffenbarung und Privatheitsverletzungen sind die Vorteile unmittelbarer als die Nachteile. Dies lässt sich beispielsweise auch daran festmachen, dass viele Menschen bereit sind, sogar für einen einfachen Keks, den sie direkt geschenkt bekommen können, personengebundene Daten wie Name, Adresse oder sogar Führerscheinnummer zu offenbaren (Beckett, 2014; Jentzsch et al., 2012). Bounded rationality besagt, dass Menschen häufig nicht über die Kapazität verfügen, sich logisch und sinnvoll zu verhalten; sie können nicht Vor- und Nachteile korrekt einschätzen, überakzentuieren oder vernachlässigen bestimmte Aspekte, weswegen Verhalten nicht logisch vorhersehbar ist. Zuletzt würde ich noch als vierten Punkt ergänzen, dass nicht nur das Kommunizieren von personenbezogenen Daten Vorteilen bringt, sondern ebenso, dass die Zurückhaltung Kosten birgt. Zur Veranschaulichung: Es bedeutet mehr Aufwand, sich zu informieren, welcher Messenger auf dem Smartphone die Privatheit eigentlich am besten schützt; ebenso kann es sein, dass der privatsphärefreundliche Messenger nur von wenigen Menschen genutzt wird. Oder ganz wortwörtlich: Während Messenger wie WhatsApp sich darüber finanzieren, dass sie Daten verkaufen, weswegen sie ihre Dienstleistung kostenlos anbieten können, müssen privatsphärefreundlichere Apps wie Threema käuflich erworben werden. Die Protection Motivation Theory besagt, dass sobald Kosten für das adaptive Verhalten (also das schützende und vorsichtige Verhalten) steigen, sinkt selbstverständlich auch dessen Wahrscheinlichkeit (Rogers, 1975).

Neben diesen inhaltlichen Punkten, welche für die tatsächliche Existenz des Privacy Paradox argumentieren, gibt es auch methodische Erklärungen, warum sich das Paradox zwar bisweilen in Studien zeigt, aber womöglich in Wirklichkeit nicht existiert. Als erstes Argument ist hier ein wissenschaftsphilosophisches zu nennen, das sogenannte Duhem-Quine Problem (Dienes, 2008). Dieses besagt, dass sämtliche Hypothesen weitere Nebenhypothesen mit sich führen. Als Veranschaulichung: Ein psychologischer Fragebogen, der die Hypothese analysiert, ob Privatheitssorgen mit Selbstoffenbarung korrelieren, hat ebenso die Neben-

hypothese, dass beide Konstrukte korrekt gemessen werden. Sollte die Analyse des Fragebogens keine signifikanten Ergebnisse produzieren, kann dies daran liegen, dass es tatsächlich keinen Zusammenhang gibt, oder aber, dass beide Konstrukte schlecht oder falsch gemessen wurden. Beim Privacy Paradox handelt es sich, wie bereits ausgeführt, wahrscheinlich um kleine bis moderate Effekte. Im Gegensatz zu großen Effekten ist es schwieriger und herausfordernder, kleine überzufällig nachweisen zu können. Es bedarf großer Stichproben (zur Erzielung ausreichender statistischer Power), genauer Messinstrumente und adäquater Auswertungsstrategien – Voraussetzungen, die schwer zu erfüllen sind und in der Vergangenheit auch nicht immer erfüllt waren. Zum Beispiel: Um tatsächliches Verhalten anhand psychologischer Fragebögen vorhersagen zu können, ist es wichtig, dass diese dem sogenannten Kompatibilitätsprinzip folgen (Fishbein & Ajzen, 2010): Soll spezifisches Verhalten erklärt werden (bspw. „Kommunikation von Baby-Fotos auf Facebook“), müssen spezifische Kognitionen abgefragt werden (bspw. „Sorgen bzgl. der Kommunikation von Baby-Fotos auf Facebook“); soll allgemeines Verhalten analysiert werden (bspw. „Hochladen von Bildern ins Internet“), müssen ebenso generische Kognitionen erfasst werden (bspw. „Sorge bzgl. des Hochladens von Bildern ins Internet“). In einer Umfrage mit 595 Menschen im deutschsprachigen Raum fanden wir etwa heraus, dass 28% aller Nutzer nicht ihren richtigen Namen auf Facebook angaben (Dienlin & Trepte, 2015) – ein spezifischer Schutz der Privatheit. Dieser lässt sich allerdings besser mit ebenso spezifischen Fragen erklären.

Zuletzt gibt es noch eine Erklärung, welche beide Perspektiven verbindet. Es könnte sein, dass die Privatheitssorgen womöglich doch nicht besonders ausgeprägt sind, sondern in Wahrheit eher klein ausfallen (Trepte et al., 2014). Als Konsequenz: Wären sie groß, würden sie das Verhalten beeinflussen; eventuell sind sie aber zu klein, um dies zu tun. Dies stellt erstens ein methodisches Problem dar. Es impliziert, dass die Sorgen bisher falsch gemessen wurden, beziehungsweise, dass Angaben wie „2/3 aller Europäer sind besorgt, dass sie keine komplette Kontrolle über die online kommunizierten Daten haben“ (European Commission, 2015) in die Irre führen. Dies könnte zum einen an einem Mangel an Information liegen: Nutzer von SNS wissen nicht, dass ihre Daten weiterverkauft werden, sie sehen nicht die latenten Profile, welche über sie vorliegen und tiefe Einblicke in Persönlichkeit erlauben (Kosinski et al., 2013). (Mittlerweile scheint es sogar möglich zu sein, auf Fotos die sexuelle Orientierung eines Menschen mit Algorithmen automatisch ablesen zu können; Wang & Kosinski, 2018.) Sobald Menschen allerdings ein Einblick in solche latenten Profile ermöglicht wird, erhöht dies hingegen ihre Privatheitssorgen (Padyab et al., 2016). Zweitens könnte es auch daran liegen, dass Menschen selten tatsächlich negative Erfahrungen sammeln: Zum Beispiel gaben 2011 nur 2% aller Europäer an, dass schon einmal ihre Identität geklaut worden wäre (European Commission, 2011). Die Gefahren vor dem Verlust der Privatheit sind häufig abstrakt, ethisch, politisch, philosophisch oder akademisch – für manche somit schwer nachzuvollziehen. Es zeigt sich allerdings, dass eigene persönliche Erfahrungen die Wahrscheinlichkeit erhöhen, dass sich Einstellungen auch tatsächlich im

Verhalten niederschlagen (Fazio & Roskos-Ewoldsen, 1994). Eventuell könnte es auch der Tatsache geschuldet sein, dass Menschen in der Beantwortungssituation der sozialen Norm entsprechen wollen, sozial erwünscht antworten (Trepte et al., 2014). Doris Teutsch und Julia Niemann zeigten, dass Medien in Deutschland eher kritisch über Informationsweitergabe auf SNS berichten (Teutsch & Niemann, 2016), weswegen Befragte eine solche Haltung eventuell emulieren, obwohl sie in dieser Form, beziehungsweise Intensität, nicht zutrifft.

Diskussion

In der Diskussion stelle ich nun eine abschließende Einschätzung zum Privacy Paradox dar. Die Diskussion beinhaltet eine Bewertung des Forschungsstandes, Gedanken bezüglich möglicher gesellschaftlicher Implikationen und ein eigenständiges Fazit.

Bewertung

Obwohl es durchaus einzelne Studien und Argumente gibt, die für das Privacy Paradox sprechen, legen sowohl eine Meta-Analyse empirischer Arbeiten als auch die theoretische Gesamtperspektive nahe, dass sich die Sorgen der Menschen bezüglich ihrer Privatheit tatsächlich im Verhalten niederschlagen. Wohl gemerkt: Sie tun dies nicht in starkem Maße, lediglich gering und anteilig. Dies erscheint allerdings angesichts der allgemein moderaten Bedeutung von Ängsten und Sorgen durchaus plausibel – beispielsweise hält die Angst vor dem frühzeitigen Tode Viele nicht davon ab zu rauchen, mehr Sport zu betreiben oder gesünder zu essen. Diese anteilige Diskrepanz zwischen Einstellungen und Verhalten ist in der sozialpsychologischen Forschung seit Längerem bekannt und recht gut erklärbar; ich würde einen neuen Anwendungsfall (i.e., Selbstoffenbarung im Internet) somit nicht als paradox bezeichnen. Nichtsdestoweniger lässt sich argumentieren, dass der Einfluss größer sein könnte, müsste oder vielleicht sogar sein sollte.

Der Forschungsprozess zum Privacy Paradox ist allerdings noch nicht abgeschlossen. Zum einen wurde die allgemeine Güte sozialwissenschaftlicher Ergebnisse in der vergangenen Zeit (berechtigterweise) kritisiert (Munafò et al., 2017). Folgendes Beispiel zur Illustration: Aktuell herrschen in der Wissenschaft ungünstige Anreizsysteme. Wissenschaftler werden in erster Linie für erfolgreiche Publikationen in renommierten Fachzeitschriften belohnt, nicht aber für allgemeinen Erkenntnisgewinn. Beide können einander diametral gegenüberstehen; beispielsweise, da das Finden von überraschenden oder signifikanten Ergebnissen die Publikationswahrscheinlichkeit erhöht (Simonsohn et al., 2014). Damit Studienergebnisse objektiv und aufschlussreich sein können, müssen Hypothesen vorab registriert und Studien unabhängig von den Ergebnissen publiziert werden können. Dieses Modell wird als sogenannte

Registered Reports bezeichnet (Nosek & Lakens, 2014). Ebenso gibt es keine Anreize für Wissenschaftler, bereits publizierte Forschung zu replizieren oder hinsichtlich möglicher Fehler zu überprüfen und zu kritisieren; entsprechend kursieren in der Literatur einige Ergebnisse, die voraussichtlich zufallsbedingt oder zumindest methodisch verbesserungswürdig sein können. Aktuell befindet sich die Forschungslandschaft zwar bereits im Umbruch – es wird allerdings noch einige Jahre dauern, bis sich diese und andere gute wissenschaftliche Praktiken nachhaltig durchsetzen und zur sozialen Norm werden; mit der erhofften Folge, dass Studienergebnisse, entsprechend auch solche zum Privacy Paradox, zunehmend vertrauenswürdiger und verlässlicher werden.

Zum anderen wissen wir aktuell noch recht wenig über die kausale Wirkung von Privatheitssorgen auf das Verhalten. In einer ersten längsschnittlichen Studie mit 1384 Befragten konnten wir feststellen, dass sobald Privatheitssorgen wuchsen, ebenso die Wahrscheinlichkeit zur Datenweitergabe sank (Dienlin et al., 2019). Darüber hinaus haben allgemeine Privatheitssorgen wahrscheinlich einen Langzeiteffekt auf spezifische Privatheitseinstellungen: Wenn Sorgen zunahmen, reduzierte dies die positive Einstellung gegenüber Datenweitergabe sechs Monate später. Weitere Forschung ist vonnöten, um diese Effekte replizieren und besser verstehen zu können. Ebenso ist es das erklärte Ziel, anstelle von Selbst-Berichten in Form von Fragebögen, welche Verhalten lediglich approximieren können, in Zukunft noch mehr tatsächliches Verhalten zu beobachten (und somit reliabler zu erfassen). Erste Studien zeigen, dass sich der Privacy Calculus auch anhand von Verhaltensdaten replizieren lässt (Dienlin et al., 2017) – weitere Forschung ist allerdings auch hier erstrebenswert.

Aktuell wird dem Privacy Paradox der Privacy Calculus gegenübergestellt. Gemäß dem Privacy Calculus ist das Verhalten nicht paradox, sondern zumindest anteilig rational und kalkuliert. Menschen offenbaren Information, da sie Vorteile für wichtiger einschätzen als mögliche Risiken. Der Calculus impliziert somit eine gewisse Selbstbestimmtheit und Mündigkeit. Allerdings ist dies nicht zwangsläufig der Fall: Die Tatsache, dass sich Vorteile im Verhalten zeigen, muss nicht notwendigerweise das Ergebnis eines dezidierten Abwägungsprozesses sein – vielmehr kann es auch ein Produkt unbewusster (oder unterbewusster) Konditionierung darstellen. Aktuelle Forschung zeigt vor allem, dass sich sowohl positive als auch negative Kognitionen im Verhalten widerspiegeln; es erfordert aber nicht, dass beide aktiv abgewogen werden müssen. Es könnte auch sein, dass Menschen dies zwar situativ durchaus tun, es somit vereinzelte Meilensteine der rationalen Abwägung gibt (bspw., wenn eine neue App auf den Markt kommt und sich Nutzer überlegen, ob sie diese installieren möchten), das meiste Verhalten an sich aber eher allgemeinen niederschweligen Heuristiken entspricht (Sundar et al., 2013). Im Sinne von: Fühlt es sich für die Nutzer gut an, vertraut und vertrauenswürdig? Falls ja, könnte dies bereits zur aktiven Kommunikation genügen.

Gesellschaftliche Implikationen

Welche Bedeutung hat das Vorangestellte für die Gesellschaft? In erster Instanz denke ich, dass die Ergebnisse aufzeigen, dass Online-Verhalten an und für sich nicht paradox, irrational oder absurd ist. Die Online-Welt hat wahrscheinlich mehr Gemeinsamkeiten mit der Offline-Welt als Unterschiede. Die Prämisse, dass Offline-Verhalten logisch und sinnhaft ist, stimmt vermutlich ebenso wenig wie diejenige, dass es online unlogisch und sinnfrei wäre. Dies hat folgende Konsequenz: Online-Verhalten lässt sich ebenso wie Offline-Verhalten schulen, beeinflussen und verbessern. Genau wie offline wird dies aber ebenso auch online nicht unmittelbar erfolgen, sondern eine konzertierte gesellschaftliche Umsetzung erfordern. In anderen Lebensbereichen mit ambivalentem Kosten-Nutzen-Verhältnis ist uns dies bereits bewusst (bspw. Ernährung, Alkoholkonsum, Transport, Sport). Berechtigte Risiken müssen minimiert, mögliche Vorteile maximiert und beides miteinander abgewogen werden. Der Ratschlag zum vollständigen Verzicht auf Social Media zur Wahrung der Privatheit richtet bei einem Jugendlichen heutzutage womöglich mehr Schaden an, als dass er Nutzen bringt, da Social Media mittlerweile für Viele einen wichtigen Anker sozialer Zugehörigkeit darstellen. Man könnte dergestalt auch argumentieren, dass es eher paradox wäre, würden sich Jugendliche diesen Diensten komplett entziehen.

Eine weitere interessante Frage ist übrigens Folgende: Könnte es sich beim Privacy Paradox nicht auch anteilig um einen Generationenkonflikt handeln? Ist es vielleicht so, dass sich die Sorgen der einen Generation lediglich nicht ausreichend im Verhalten der anderen wiederfinden? In jedem Fall bedarf es als Reaktion verschiedener gesellschaftlicher Anpassungsprozesse: Horizontal betrachtet könnte dies bedeuten, mehr Rücksicht darauf zu nehmen, dass heutzutage eher kompromittierendes Material über Person vorliegt und dieses leichter eingesehen werden kann, was mehr gegenseitiges Verständnis für Fehlritte wünschenswert erscheinen lässt. Vertikal betrachtet könnte es möglicherweise bedeuten, der Praxis Einhalt zu gebieten, dass Unternehmen anwendungsübergreifende Nutzerprofile erstellen und diese an Dritte weiterverkaufen. Um Privatheit effektiv zu gestalten, bedarf es der Möglichkeit, sowohl horizontal als auch vertikal Anpassungen vornehmen zu können. Wohingegen Nutzer bereits jetzt schon relativ effektiv ihre Privatheit horizontal gegenüber anderen Personen schützen können, ist dies vertikal in Bezug auf Unternehmen und Institutionen noch nicht ausreichend der Fall. Gäbe es hier weitere Stellschrauben, könnte sich die Lücke zwischen Einstellungen und Verhalten voraussichtlich weiter schließen. Dies beinhaltet dabei ebenso die Gesetzgebung: „Während also analoge Privatheit deren Herstellung, Wahrung und Durchsetzung prinzipiell bei deren Trägern selbst sieht, ist es im Netz genau umgekehrt: Sie bedarf vielmehr der Anerkennung, Sicherung und Durchsetzung durch die Rechtsordnung selbst“ (Gusy, 2018). Entsprechend gibt es aus politischer Perspektive durchaus Sinn, das Privacy Paradox nicht komplett ad acta zu legen – gerade auch angesichts der großen Bedeutung von Privatheit für Demokratien (Eichenhofer, 2017). Ja, Sorgen zeigen sich bereits im Verhalten, aber nein, noch nicht

ausreichend, weswegen es sich lohnt, weiter für mehr Gestaltungs- und somit Selbstbestimmungsmöglichkeit zu streiten.

Zurück zu den eingangs des Kapitels gestellten Fragen: „Warum sind viele Menschen bereit, im Internet Informationen zu offenbaren, die vermeintlich privat sind?“ Antwort: Weil sie hieraus vielfältige Nutzen ziehen können und sich gesellschaftliche Normen hinsichtlich typischen Verhaltens stetig ändern (siehe bspw. Sexualethik, Rauchverhalten oder Kindeserziehung). Während 2006 noch lediglich 29% aller amerikanischen Jugendlichen ihre E-Mail-Adresse online posteten, waren dies 2012 bereits 53% (Tsay-Vogel et al., 2018). Dies bedeutet nicht, dass der Wert des Privaten zwangsläufig sinkt. Eine Trendstudie aus den Vereinigten Staaten zeigt beispielsweise, dass die allgemeine Sorge um die Privatheit bei 2789 Studierenden zwischen den Jahren 2010 und 2015 signifikant anstieg. „Ist es nicht paradox, dass sich einige um ihre Privatheit sorgen, aber dennoch viele aktives Mitglied auf SNS wie Facebook, Instagram oder Snapchat sind?“ Antwort: Nein. Auch auf SNS spiegeln sich Privatheitssorgen im Verhalten wider; besorgtere Menschen würden etwa mit einer geringeren Wahrscheinlichkeit Bilder von ihren Kindern posten. Folgendes stimmt allerdings: Aufgrund der mannigfaltigen Vorteile von SNS reichen die Sorgen für viele nicht aus, sich komplett fernzuhalten. „Warum gingen bei der Volkszählung im Jahre 1987 noch tausende Menschen auf die Straße, um gegen die Sammlung vermeintlich harmloser Daten wie Wohnsituation und Erwerbstätigkeit zu protestieren, sind aber jetzt bereit, intimere Daten wie Fotos, Hobbies und sexuelle Orientierung mit privatwirtschaftlichen Unternehmen zu teilen?“ Antwort: Vermutlich deswegen, da die Menschen früher keinen Nutzen von der Sammlung hatten, sie diese vorrangig als Kontrollverlust und Eingriff des Staates wahrnehmen mussten. Der Nutzen war damals womöglich genauso abstrakt wie heute die Sorge vor den möglichen Gefahren. „Ist die Fülle der produzierten Daten nicht bedenklich – zumal diese meist auch noch auf Servern im Ausland liegen, für welche nicht das vergleichsweise strenge Datenschutzgesetz der Bundesrepublik Deutschland gilt?“ Antwort: Ja, dies ist bedenklich; umso wichtiger ist es, dass multinationalen Einzelunternehmen supranationale Staatenbünde wie die Europäische Union gegenüberstehen, welche die berechtigten Interessen der Bürgerinnen und Bürger besser schützen können (und müssen). „Sind die Parallelen zu Orwells 1984, Bentham's Panoptikum oder den Praktiken ehemaliger Nachrichtendienste wie der ‚Stasi‘ nicht offenkundig?“ Antwort: Ja, es gibt einige Parallelen, aber zeitgleich auch manche Unterschiede. Wohingegen die skizzierten Beispiele die Probleme veranschaulichen, wenn Einzelvertreter staatlicher Institutionen Einzelbürgern konkret gegenüberstehen und diese einander ausspielen, somit eine interpersonale Ebene vorliegt, sind die aktuellen Probleme eher vertikaler und probabilistischer Natur: Menschen bekommen schlechtere Kredite, unterschiedliche Werbung und mehr Fragen an der Grenzkontrolle gestellt. Umso wichtiger es, dass Rechtsstaat und Justiz als notwendige Korrektive für den Einzelfall ordnungsgemäß funktionieren. „Ist das nicht paradox?“ Antwort: Ich denke nicht, nein.

Fazit

Das Privacy Paradox besagt, dass Menschen trotz ausgeprägter Privatheitssorgen viele persönliche Informationen im Internet teilen. Das Privacy Paradox lässt sich anteilig auflösen: Es liegt recht sicher eine Fehleinschätzung vor; die Annahme, dass sich Sorgen nicht im Verhalten zeigen würden, stimmt so wahrscheinlich nicht. Es lässt sich zeigen, dass Menschen, die sich mehr Sorgen um ihre Privatheit machen, auch tatsächlich etwas weniger personengebundene Daten kommunizieren. Es stimmt allerdings, dass diese Sorgen nicht allein ausschlaggebender Faktor sind oder an und für sich ausreichen würden, sorgsamer mit Daten umzugehen. Vielmehr sind Privatheitssorgen nur ein Faktor unter vielen, welche das Selbstoffenbarungsverhalten beeinflussen können. Neben den Privatheitssorgen gibt es vor allem noch zwei weitere Aspekte, welche das Kommunizieren von Daten besser erklären können: Erstens, die zu erwartenden Vorteile; zweitens, die wahrgenommenen subjektiven Normen (Ajzen, 1991).

Vertiefende/weiterführende Literatur

- Acquisti, Alessandro/Brandimarte, Laura/Loewenstein, George, Privacy and human behavior in the age of information, *Science* 347 (2015), 509–514.
- Dienlin, The psychology of privacy: Analyzing processes of media use and interpersonal communication, Dissertation, 2017 - <http://opus.uni-hohenheim.de/volltexte/2017/1315/> (30.11.2018)
- Masur, Philipp K./Teutsch, Doris/Dienlin, Tobias, Privatheit in der Online-Kommunikation, in: Schweiger, Wolfgang/Beck, Klaus (Hrsg.), *Handbuch Online-Kommunikation*. 2. Aufl., Wiesbaden, Germany in press.
- Trepte, Sabine/Teutsch, Doris, Privacy paradox, in: Krämer, Nicole C./Schwan, Stephan/Unz, Dagmar u. a. (Hrsg.), *Medienpsychologie, Schlüsselbegriffe und Konzepte*. 2. Aufl., Stuttgart, Germany 2016, S. 372–377.

Dieser Beitrag wurde gefördert von der VolkswagenStiftung.

Literatur

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>

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)

- Altman, I. (1976). Privacy: A conceptual analysis. *Environment and Behavior*, 8(1), 7–29. <https://doi.org/10.1177/001391657600800102>
- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9). <https://doi.org/https://doi.org/10.5210/fm.v11i9.1394>
- Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67(1), 26–53. <https://doi.org/10.1111/jcom.12276>
- Beckett, L. (2014). *People are willing to give away their personal data for a cinnamon cookie* [InternetDocument]. <http://mashable.com/2014/10/01/data-for-cookies/#a.PHIEiXW8qw>
- Burgoon, J. K. (1982). Privacy and communication. *Annals of the International Communication Association*, 1, 206–249.
- Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104–115. <https://doi.org/10.1287/orsc.10.1.104>
- Dienes, Z. (2008). *Understanding psychology as a science: An introduction to scientific and statistical inference*. Palgrave Macmillan.
- Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J. M. Mönig (Eds.), *Medien und Privatheit* (pp. 105–122). Karl Stutz.
- Dienlin, T., Masur, P. K., & Trepte, S. (2019). *A longitudinal analysis of the privacy paradox* [Preprint]. SocArXiv. <https://doi.org/10.31235/osf.io/fm4h7>
- Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs—Analyzing self-disclosure and self-withdrawal in a representative U.S. Sample. *Journal of Computer-Mediated Communication*, 21(5), 368–383. <https://doi.org/10.1111/jcc4.12163>
- Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, 45(3), 285–297. <https://doi.org/10.1002/ejsp.2049>
- Dienlin, T., Trepte, S., & Scharnow, M. (2017). *Self-disclosure and the affordances of SNSs: Testing the privacy calculus within an experimental framework* [Lecture].
- Eichenhofer, J. (2017). Privatheit und Transparenz in der Demokratie. *Forschungsjournal Soziale Bewegungen*, 30(2), 1. <https://doi.org/10.1515/fjsb-2017-0034>
- European Commission. (2011). *Attitudes on data protection and electronic identity in the European Union*. www.ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
- European Commission. (2015). *Data protection: Special Eurobarometer 431* [UnpublishedWork]. www.ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

Fazio, R. H., & Roskos-Ewoldsen, D. R. (1994). Acting as we feel: When and how attitudes guide behavior. In S. Havitt & T. C. Brock (Eds.), *Persuasion* (pp. 71–93). Allyn & Bacon.

Fishbein, M., & Ajzen, I. (2010). *Predicting and changing behavior: The reasoned action approach*. Psychology Press.

Geminn, C., & Roßnagel, A. (2015). „Privatheit“ und „Privatsphäre“ aus der Perspektive des Rechts – ein Überblick. *Juristenzeitung*, *70*(14), 703–708. <https://doi.org/10.1628/002268815X14346427046980>

Gusy, C. (2018). Datenschutz als Privatheitsschutz oder Datenschutz statt Privatheitsschutz? *Europäische Grundrechte*, *45*(9), 244–254.

Heirman, W., Walrave, M., & Ponnet, K. (2013). Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking*, *16*(2), 81–87. <https://doi.org/10.1089/cyber.2012.0041>

Jentzsch, N., Preibusch, S., & Harasser, A. (2012). *Study on monetising privacy* [UnpublishedWork]. <https://www.enisa.europa.eu/publications/monetising-privacy>

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, *110*(15), 5802–5805. <https://doi.org/10.1073/pnas.1218772110>

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125. <https://doi.org/10.1057/jit.2010.6>

Lang, F. R., Reschke, F. S., & Neyer, F. J. (2006). Social relationships, transitions, and personality development across the life span. In D. K. Mroczek & T. D. Little (Eds.), *Handbook of personality development* (pp. 445–466). Lawrence Erlbaum Associates.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42. <https://doi.org/10.1111/j.1540-4560.1977.tb01880.x>

Lewin, K. (1935). *A dynamic theory of personality*. McGraw-Hill.

Masur, P. K., Teutsch, D., & Dienlin, T. (2018). Privatheit in der Online-Kommunikation. In W. Schweiger & K. Beck (Eds.), *Handbuch Online-Kommunikation* (2nd ed.). Springer VS. https://doi.org/10.1007/978-3-658-18017-1_16-1

Miller, C. (2014). *The dangers of the Internet* [InternetDocument]. <https://www.youtube.com/watch?v=uquRzrcwA18&index=5&list=PLMseCXTTEwOi5B72bYTe0EsKWFGWdQjDpt=4s>

- Munafò, M. R., Nosek, B. A., Bishop, D. V. M., Button, K. S., Chambers, C. D., Du Percie Sert, N., Simonsohn, U., Wagenmakers, E.-J., Ware, J. J., & Ioannidis, J. P. A. (2017). A manifesto for reproducible science. *Nature Human Behaviour*, 1(1). <https://doi.org/10.1038/s41562-016-0021>
- New York Public Radio. (2018). *The privacy paradox* [InternetDocument]. <https://project.wnyc.org/privacy-paradox/>
- Niemann, J., & Schenk, M. (2014). Niemann, J. & Schenk, M. (2014). Im Spannungsfeld zwischen Risiko und Nutzen Selbstoffenbarung auf Social-Networking-Sites. In B. Stark, O. Quiring, & N. Jakob (Eds.), *Von der Gutenberg-Galaxis zur Google-Galaxis: Alte und neue Grenzvermessungen nach 50 Jahren DGPK* (Vol. 41, pp. 207–223). UVK.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- Nosek, B. A., & Lakens, D. (2014). Registered reports: A method to increase the credibility of published results. *Social Psychology*, 45(3), 137–141. <https://doi.org/10.1027/1864-9335/a000192>
- Padyab, A., Päivärinta, T., Ståhlbröst, A., & Bergvall-Kåreborn, B. (2016). *Facebook users attitudes towards secondary use of personal information* [Lecture]. <http://aisel.aisnet.org/icis2016/ISSecurity/Presentations/7/>
- Pew Research Center. (2013). *Teens, Social Media, and Privacy* [InternetDocument]. <http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/>
- Reymann, K. (2011). Volkszählung 1987: Bürgerprotest und Boykott-Initiativen. *Frankfurter Allgemeine Zeitung*. <http://www.faz.net/aktuell/politik/zensus-2011/volkszaehlung-1987-buergerprotest-und-boykott-initiativen-1636625.html>
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- Schau hin. (2017). *Persönliche Daten im Internet schützen* [InternetDocument]. <https://www.schau-hin.info/informieren/extrathemen/datenschutz.html>
- Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology*, 73(6), 741–752.
- Seele, P., & Zapf, C. L. (2017). „Privacy is dead“: Wie konnte es so weit kommen? In P. Seele & C. L. Zapf (Eds.), *Die Rückseite der Cloud* (pp. 13–46). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-54758-8_2
- Seemann, M. (2013). Die Privatsphären-Falle. *Die Zeit*. <http://www.zeit.de/digital/datenschutz/2013-10/privatsphaere-ueberwachung-nsa-seemann>
- Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics*, 69(1), 99. <https://doi.org/10.2307/1884852>

- Simonsohn, U., Nelson, L. D., & Simmons, J. P. (2014). P-curve: A key to the file-drawer. *Journal of Experimental Psychology. General*, *143*(2), 534–547. <https://doi.org/10.1037/a0033242>
- Smock, A. D., Ellison, N. B., Lampe, C., & Wohn, D. Y. (2011). Facebook as a toolkit: A uses and gratification approach to unbundling feature use. *Computers in Human Behavior*, *27*(6), 2322–2329. <https://doi.org/10.1016/j.chb.2011.07.011>
- Statista. (2017). *Anzahl der Nutzer von Facebook und Instagram in Deutschland im Jahr 2017 (in Millionen)* [InternetDocument]. <https://de.statista.com/statistik/daten/studie/503046/umfrage/anzahl-der-nutzer-von-facebook-und-instagram-in-deutschland/>
- Statistisches Bundesamt. (2017). *Rückgang bei Zigaretten und Feinschnitt im Jahr 2016* [InternetDocument]. https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2017/01/PD17_014_799.html
- Sundar, S. S., Kang, H., Wu, M., Gu, E., & Zhang, B. (2013). Unlocking the privacy paradox: Do cognitive heuristics hold the key? In *CHI 2013: Changing Perspectives* (pp. 811–816).
- Sutton, S. (1998). Predicting and explaining intentions and behavior: How well are we doing? *Journal of Applied Social Psychology*, *28*(15), 1317–1338. <https://doi.org/10.1111/j.1559-1816.1998.tb01679.x>
- Taddicken, M. (2014). The “privacy paradox” in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. <https://doi.org/10.1111/jcc4.12052>
- Teutsch, D., & Niemann, J. (2016). Social network sites as a threat to users’ self-determination and security: A framing analysis of German newspapers. *The Journal of International Communication*, *22*(1), 22–41. <https://doi.org/10.1080/13216597.2015.1111841>
- Trepte, S., Dienlin, T., & Reinecke, L. (2014). Risky behaviors. How online experiences influence privacy behaviors. In B. Stark, O. Quiring, & N. Jakob (Eds.), *Von der Gutenberg-Galaxis zur Google-Galaxis: Alte und neue Grenzwermessungen nach 50 Jahren DGPuK* (Vol. 41, pp. 225–244). UVK.
- Trepte, S., & Reinecke, L. (2011). The social web as a shelter for privacy and authentic living. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 61–73). Springer. https://doi.org/10.1007/978-3-642-21521-6_6
- Trepte, S., & Teutsch, D. (2016). Privacy paradox. In N. C. Krämer, S. Schwan, D. Unz, & M. Suckfüll (Eds.), *Medienpsychologie: Schlüsselbegriffe und Konzepte* (2nd ed., pp. 372–377). Kohlhammer.
- 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>
- Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1), 20–36. <https://doi.org/10.1177/0270467607311484>
- Utz, S., & Krämer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 3(2). www.cyberpsychology.eu/view.php?cisloclanku=2009111001&article=2
- Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, 39(2), 273–315. <https://doi.org/10.1111/j.1540-5915.2008.00192.x>
- Wang, Y., & Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of Personality and Social Psychology*.
- Westin, A. F. (1967). *Privacy and freedom*. Atheneum.
- Wikipedia. (2018). *Privacy concerns with social networking services* [Internet-Document]. https://en.wikipedia.org/wiki/Privacy_concerns_with_social_networking_services
- Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior*, 27(5), 591–615. <https://doi.org/10.1177/109019810002700506>