Verbraucherorientierter Datenschutz: Identifizierung von Verbraucherarchetypen zur effektiven Kommunikation von Datenschutzpraktiken

Sunyaev, Ali; Dehling, Tobias; Schmidt-Kraepelin, Manuel

Postprint / Postprint
Sammelwerksbeitrag / collection article

Empfohlene Zitierung / Suggested Citation:
Sunyaev, A., Dehling, T., & Schmidt-Kraepelin, M. (2018). Verbraucherorientierter Datenschutz: Identifizierung von Verbraucherarchetypen zur effektiven Kommunikation von Datenschutzpraktiken. In C. Bala, & W. Schuldzinski (Hrsg.), *Jenseits des Otto Normalverbrauchers: Verbraucherpolitik in Zeiten des "unmanageable consumer"* (S. 163-179). Düsseldorf: Kompetenzzentrum Verbraucherforschung NRW. https://doi.org/10.15501/978-3-86336-920-0_8

Verbraucherorientierter Datenschutz

Identifizierung von Verbraucherarchetypen zur effektiven Kommunikation von Datenschutzpraktiken

Ali Sunyaev, Tobias Dehling und Manuel Schmidt-Kraepelin

DOI 10.15501/978-3-86336-920-0_8

Abstract

Datenschutzkommunikation wird nur dann funktionieren, wenn die Informationsbedürfnisse der Verbraucher, die weder statisch noch einheitlich sind, adressiert werden. Ein vielversprechender, praktisch realisierbarer Ansatz ist es, die Kommunikation an Verbraucherarchetypen anzupassen. Diese Studie identifiziert die verschiedenen Archetypen basierend auf einer Webumfrage. Die identifizierten Archetypen liefern eine solide Grundlage für die Verwirklichung funktionierender Datenschutzkommunikation.

---

1 Einleitung

Im Zeitalter der digitalen Informationen hinterlassen Verbraucherinnen und Verbraucher bei jeder Onlineaktivität Informationsspuren, die Dritten Aufschluss über Interessen, Charaktereigenschaften, Überzeugungen und Absichten geben können (Acquisti, Brandimarte und Loewenstein 2015). So verwundert es nicht, dass drei Viertel der europäischen Verbraucherinnen und Verbraucher der Meinung sind, dass es keine Alternative zur Offenlegung persönlicher Daten gibt, um bestimmte Produkte oder Services nutzen zu können (European Commission 2011). Der Datenschutz ist zu einer Kernherausforderung und einem zentralen Thema der heutigen Zeit geworden (Dehling und Sunyaev 2014).

Bestehende Forschung geht grundsätzlich davon aus, dass Datenschutz aus Verbrauchersicht sowohl durch externe Mechanismen (zum Beispiel Gesetzgebung, industrielle Selbstkontrolle), als auch durch interne Mechanismen (etwa Auswahl, Einwilligungserklärungen, Korrekturen) gesteuert wird (Tavani 2007). Da industrielle Selbstkontrolle versagt (Tavani und Moor 2001) und die Gesetzgebung nur in eingeschränktem Maß Einfluss üben kann (Weber 2010), fällt die Wahrung der Informationsprivatheit zumeist auf die Verbraucherinnen und Verbraucher zurück, und interne Mechanismen gewinnen zunehmend an Bedeutung. Bei der Nutzung von IT-Angeboten stehen Verbraucherinnen und Verbraucher häufig vor der Wahl, einen Teil ihrer Informationsprivatheit aufzugeben, um dadurch entsprechende Gegenleistungen zu erhalten, beispielsweise Datenauswertungen oder Zugang zu Webdiensten (Dinev und Hart 2006). Um fundierte Entscheidungen zu treffen, ob potentiell interessante IT-Angebote mit den eigenen Datenschutzpräferenzen vereinbar sind, müssen Verbraucherinnen und Verbraucher zunächst umfänglich über die Datenschutzpraktiken der jeweiligen Anbieter informiert werden (Tavani 2007). Die Nutzung bestehender Informationsangebote (zum Beispiel Datenschutzerklärungen) erfordert allerdings aufgrund ihrer Komplexität und Länge einen hohen zeitlichen Aufwand und Fachkenntnisse (Park 2013; McDonald und Cranor 2008). Daher werden sie faktisch von Verbraucherinnen und Verbrauchern nicht gelesen (Sunyaev et al. 2015). Verschiedene Anbieter versuchen den Datenschutz von Verbrau-

cherinnen und Verbrauchern durch Privacy Enhancing Technologies (PETs) zu verbessern (Brüggemann et al. 2016). Darunter werden sowohl simple Indikatoren für Datenschutzmaßnahmen, wie zum Beispiel die Anzeige eines Schlosses in der Browsernavigationsleiste bei verschlüsselten Verbindungen als auch komplexere Angebote, wie Anonymisierungssoftware, Cookie-Managementsoftware oder Datenschutzerklärungen verstanden (Sunyaev et al. 2015; Xu et al. 2012). Der Mehrwert dieser Angebote für Verbraucherinnen und Verbraucher wird allerdings häufig durch einen mangelnden Fokus auf Verbraucherbedürfnisse erheblich gemindert. Endnutzern von IT-Angeboten ist daher derzeit kaum bewusst, welche persönlichen Daten in welchem Kontext von ihnen gesammelt und ausgewertet werden.

Um PETs zu schaffen, die einen echten Mehrwert für die Verbraucherschaft generieren und Informationsasymmetrien zwischen Anbietern von IT-Angeboten und Verbraucherschaft reduzieren, müssen PETs zukünftig die Informationen abbilden, die für die jeweilige Verbraucherin oder den jeweiligen Verbraucher relevant sind. So wird auf der einen Seite eine Informationsüberflutung verhindert, gleichzeitig aber werden alle relevanten Informationen berücksichtigt. Um derartige, effektive Kommunikation von Datenschutzpraktiken zu realisieren, wäre es eine intuitive Lösung, die Kommunikation von Datenschutzpraktiken individuell auf jede einzelne Verbraucherin und jeden einzelnen Verbraucher anzupassen. In der Praxis ist dieser Ansatz allerdings kaum umsetzbar, da es einen unzumutbaren Aufwand verursachen würde und Informationen über die Informationsbedürfnisse für jede Verbraucherin und jeden Verbraucher in diesem Detailgrad nicht verfügbar sind. Ein vielversprechenderer Ansatz, der darauf abzielt die Beschränkungen eines universellen Ansatzes zu umgehen – und auch praktisch eher umsetzbar ist als die individuelle Berücksichtigung aller Verbraucherinnen und Verbraucher –, ist die maßgeschneiderte Kommunikation für verschiedene Archetypen von Verbraucherinnen und Verbrauchern. Diese Vorgehensweise benötigt allerdings zunächst eine Einteilung der Verbraucherschaft in Archetypen mit ähnlichen Informationsbedürfnissen im Hinblick auf Datenschutzpraktiken. Diese Arbeit zielt darauf ab, Archetypen von Verbraucherinnen und Verbrauchern in Bezug auf deren Datenschutzinformationsbedürfnisse zu identifizieren und so eine Grundlage für die Entwicklung effektiverer PETs zu schaffen.

2 Bestehende Forschung zu Verbraucherarchetypen

Bisherige Forschung bietet eine Reihe verschiedener Einteilungen von Verbraucherinnen und Verbrauchern in Archetypen im Datenschutzkontext. Dabei wurde eine Reihe von verschiedenen Perspektiven eingenommen. Die bekannteste Einteilung stammt von Alan Westin und ordnet Verbraucherinnen und Verbraucher in Fundamentalisten, Pragmatiker und Unbedarfte ein (Kumaraguru und Cranor 2005). Hauptziel dieser Einteilung war es, die Datenschutzeinstellungen der einzelnen Verbrauchergruppen über längere Zeiträume zu analysieren und Veränderungen zu erklären (Kumaraguru und Cranor 2005). Andere Einteilungen von Verbraucherinnen und Verbrauchern wurden entwickelt und genutzt,

- um die Eigenschaften von Datenschutzbedenken zu analysieren (Ackerman, Cranor und Reagle 1999; Cranor, Reagle und Ackerman 1999),
- um Einstellungen bezüglich der Sekundärnutzung von persönlichen Daten zu untersuchen (Culnan 1993),
- um Zusammenhänge zwischen Personalisierungspräferenzen und Datenschutzeinstellungen zu identifizieren (Zhu et al. 2017),
- um angegebene Datenschutzbedenken mit Verhaltensabsichten (Woodruff et al. 2014) und tatsächlichem Onlineverhalten (Berendt, Günther und Spiekermann 2005; Spiekermann, Grossklags und Berendt 2001) zu vergleichen.

Obwohl diese Forschungsarbeiten interessante Einteilungen der Verbraucherschaft in Archetypen vorschlagen, sind sie für die Entwicklung von PETs aus zwei Gründen ungeeignet. Erstens bleiben alle Einteilungen auf einem sehr abstrakten und wenig detaillierten Level und vermeiden es dabei, inhaltliche Schwerpunkte verschiedener Datenschutzaspekte innerhalb ihrer Typisierungen zu setzen. Zweitens werden für die Archetypen vorrangig Datenschutzbedenken und Einstellungen zum Datenschutz als zentrale Konstrukte genutzt. Weitestgehend unbeachtet bleibt, über welche verschiedenen datenschutzrelevanten Aspekte Verbraucherinnen und Verbraucher bei der Nut-

zung von IT-Angeboten informiert werden möchten. Die vorliegende Studie adressiert diese Forschungslücke und stellt die Datenschutzinformationsbedürfnisse von Verbraucherinnen und Verbrauchern in den Mittelpunkt, um Verbraucherarchetypen zu identifizieren.

3 Methodik

3.1 Szenariobasierte Onlineumfrage

Um die Datenschutzinformationsbedürfnisse von Verbraucherinnen und Verbrauchern generell und mit möglichst wenig kontextbedingten Verzerrungen erheben zu können, wurde eine szenariobasierte Onlineumfrage mit vier verschiedenen Szenarien auf unterschiedlichen Sensitivitätsleveln durchgeführt. Als Szenarien wurden gängige Smartphone Applikationen genutzt, da Verbraucherinnen und Verbraucher mit diesen vertraut sind. Somit wurde den Umfrageteilnehmenden die Durchführung erleichtert.

3.2 Szenarioentwicklung

Zur Identifizierung von Szenarien mit verschiedenen Sensitivitätsleveln wurden zunächst 18 Szenarien entwickelt und in einer Vorstudie auf ihre Informationssensitivität und wahrgenommene Privatheit (Dinev et al. 2013) untersucht. Während der Vorstudie wurden jeder Teilnehmerin und jedem Teilnehmer vier Szenarien angezeigt und Fragen zur Informationssensitivität und wahrgenommenen Privatheit auf einer 7-Punkt Likert-Skala gestellt. In einem Pretest mit 18 wissenschaftlichen und studentischen Mitarbeitern aus dem Fachbereich der Wirtschaftsinformatik wurde die Umfrage getestet, um eine hohe Qualität der genutzten Items und Szenariobeschreibungen zu gewährleisten. Auf Grundlage des Pretests wurden sieben Szenarien aus der Auswahl entfernt, da sie zu ähnliche Ergebnisse im Vergleich zu anderen Szenarien zeigten. Die

Vorstudie wurde im April 2016 mit insgesamt 172 Teilnehmerinnen und Teilnehmern durchgeführt. Die Antworten von 27 Personen wurden entfernt, da sie entweder die Umfrage nicht zu Ende ausfüllten, die Umfrage zu schnell und nicht sorgfältig genug durchführten oder eine Kontrollfrage nicht richtig beantworteten. Von den übrigen 145 Teilnehmerinnen und Teilnehmern gaben 88 ihr Geschlecht als weiblich, 56 ihr Geschlecht als männlich und 1 als trans* an. Die Altersgruppen erstreckten sich von unter 18 Jahre bis 65-70 Jahre alt. Cronbachs Alpha für Informationssensitivität und wahrgenommene Privatheit betrugen 0.8685 und 0.9184. Die beiden Konstrukte offenbarten eine starke negative Korrelation (Pearson $r = 0{,}9816$, $p < 0{,}001$). Basierend aus den Antworten der Umfrage wurden vier Szenarien für die Hauptstudie ausgewählt. Dabei wurden ein Szenario mit hoher Sensitivität, zwei Szenarien mit mittlerer Sensitivität und ein Szenario mit niedriger Sensitivität gewählt. Tabelle 1 zeigt die gemessene Informationssensitivität und wahrgenommene Privatheit für die vier ausgewählten Szenarien.

Szenario	Beschreibung	N	Informations-sensitivität M (SD)	Wahrgenommene Privatheit M (SD)
Taschenrechner	Eine App, die den Nutzer dabei unterstützt simple arithmetische Probleme zu lösen.	54	2,40 (1,78)	5,89 (1,40)
Musikstreaming	Eine App, die den Zugriff auf eine große Anzahl verschiedener Musikstücke und dessen Streaming auf das mobile Endgerät ermöglicht.	50	4,05 (1,72)	3,95 (1,60)
Navigation	Eine App, die den Nutzer bei der Navigation während des Autofahrens unterstützt.	44	5,19 (1,79)	3,47 (1,63)
Finanzen	Eine App, die es ermöglicht Zugriff zu einem Bankkonto zu erhalten und Finanztransaktionen abzuschließen.	44	6,09 (1,63)	2,86 (1,96)

Tabelle 1: Ergebnisse der Vorstudie zur Messung von Informationssensitivität und wahrgenommener Privatheit für die vier ausgewählten Szenarien.

3.3 Umfrage zur Messung von Datenschutzinformationsbedürfnissen

In der Umfrage zur Messung der Datenschutzinformationsbedürfnisse wurde den Teilnehmerinnen und Teilnehmern nach einer kurzen Einführung, welche den Zweck und Aufbau der Umfrage erläuterte, jeweils eins der vier Szenarien zufällig zugewiesen. Bezugnehmend auf das jeweilige Szenario wurde den Teilnehmerinnen und Teilnehmern der Umfrage dann folgende Anweisung zur Messung der Informationsbedürfnisse gestellt:

> „Bitte geben Sie für die folgenden Aspekte an, wie wichtig es für Sie ist, über diese informiert zu werden, wenn Sie die beschriebene Smartphone-App nutzen möchten."

Die Aspekte, die unter der Anweisung jeweils gelistet waren, beinhalteten dabei verschiedene Datenschutzpraktiken, welche in vorangegangener Forschung durch ein Literaturreview und die Betrachtung von Datenschutzerklärungen identifiziert worden waren (Dehling et al. 2015; Sunyaev et al. 2015). Die erhobenen Datenschutzpraktiken waren anhand vier verschiedener Kategorien organisiert: Informationssammlung, Handhabung von Informationen, Zweck der Datenschutzpraktiken und bereitgestellte Kontrollmechanismen (Ackerman, Cranor und Reagle 1999; Antón, Earp und Young 2010). Dabei fokussierten sich die Datenschutzpraktiken wie folgt:

- fünf auf Sensoren zur Sammlung von Informationen,
- fünf auf die Art der gesammelten Informationen,
- fünf auf die Handhabung der Informationen,
- neun auf Kontrollmechanismen,
- sieben auf den Zweck der Datenschutzpraktiken.

Die Teilnehmerinnen und Teilnehmer der Umfrage gaben ihre Antworten für jede einzelne Datenschutzpraktik auf einer 101 Punkte Skala (0 = unwichtig, 100 = sehr wichtig).

Die Umfrage wurde im Juni und Juli 2016 mit deutschen Verbraucherinnen und Verbrauchern durchgeführt. Sie wurden über soziale Medien als Teilnehmende rekrutiert. Insgesamt nahmen 160 Personen teil. 26 Teilnehmerinnen und

Teilnehmer beantworteten eine Kontrollfrage nicht korrekt und wurden daher für die Analyse ausgeschlossen. So blieben insgesamt die Antworten von 134 Personen (weiblich = 73, männlich = 60, unbekannt = 1) für die Datenanalyse übrig. Das Alter der Teilnehmerinnen und Teilnehmer betrug zwischen 18 und 70 Jahren. Die meisten von ihnen gaben an, einen Universitätsabschluss als höchsten Bildungsabschluss zu besitzen: Universitätsabschluss (79; 59 Prozent), Studenten (28; 20,9 Prozent); Berufsausbildung (14; 10,4 Prozent); Anderes (13; 9,7 Prozent). Zwei Personen gaben an, nicht regelmäßig ein Smartphone zu nutzen.

3.4 Datenanalyse

Zur Identifizierung von Verbrauchergruppen wurde ein agglomerativer, hierarchischer Clusteralgorithmus verwendet (Ward 1963). Dabei wurden Teilnehmerinnen und Teilnehmer mit den kleinsten Unterschieden in der Varianz ihrer Antworten iterativ gruppiert und eine hierarchische Struktur gebildet. Im Anschluss daran wurde die hierarchische Einteilung inspiziert und Mittelwerte sowie Standardabweichungen der Informationsbedürfnisse für alle Cluster berechnet. Außerdem wurden die entstandenen Cluster von einem Forscher auf besonders charakteristische Informationsbedürfnisse untersucht und anhand dessen ein initialer Name und eine Kurzbeschreibung der Charakteristiken der Cluster verfasst. Zur Sicherstellung, dass die Namensgebung und Beschreibungen intuitiv verständlich und passend zur vorhandenen Datengrundlage sind, wurden diese von drei weiteren Forschern begutachtet und in einer gemeinsamen Diskussion iterativ verfeinert, bis alle Mitglieder des Forschungsteams mit den Namen und Beschreibungen einverstanden waren (Dehling et al. 2016).

4 Identifizierte Verbraucherarchetypen

Über alle Archetypen hinweg sind Verbraucherinnen und Verbraucher am meisten interessiert

- an der Sammlung von Informationen über Nutzer (M = 83,6; SD = 23,5),
- an der Weitergabe von Informationen (M = 83,6; SD = 26,1),
- an Möglichkeiten für das Management von Einwilligungserklärungen (M = 80,5; SD = 24,2),
- an Benachrichtigungen über Datenschutzverstöße (M = 80,3; SD = 24,7)
- und am Zugriff auf gesammelte Informationen (M = 79,3; SD = 22,8).

Verbraucherinnen und Verbraucher waren am wenigsten interessiert an der Änderungshistorie von Datenschutzerklärungen (M = 58,2; SD = 30,4), ob Datenschutzpraktiken aus technischen Gründen (M = 56,0; SD = 31,04) oder zum Allgemeinwohl (M = 51,5; SD = 32,5) ausgeführt werden und an genutzten Datenformaten zur Informationssammlung (M = 49,9; SD = 32,5). Welches Szenario den Teilnehmerinnen und Teilnehmern präsentiert wurde, hatte keinen signifikanten Einfluss auf deren Zuteilung zu einem Archetyp (Spearman ρ = 0,101; p = 0,245). Das Alter (zweiseitiger Fisher-Test p = 0,139), Geschlecht (zweiseitiger Fisher-Test p = 0,742) und Bildungsniveau (Spearman ρ = -0,141; p = 0,106) zeigen ebenfalls keinen Einfluss auf die Zuteilung zu Archetypen. Die Absicht, Smartphones zukünftig zu nutzen (Spearman ρ = -0,251; p = 0,003) und die angegebene Häufigkeit der Smartphonebenutzung (Spearman ρ = -0,233; p = 0,007) weisen eine schwache negative Korrelation mit den mittleren Informationsbedürfnissen der Archetypen auf. Hingegen zeigen vorangegangene negative Datenschutzerfahrungen (Spearman ρ= 0,267; p = 0,002) und Datenschutzbedenken (Spearman ρ = 0,314; p < 0,001) schwache positive Korrelationen mit den Mittelwerten der Archetypen.

Insgesamt wurden 13 Verbraucherarchetypen auf zwei hierarchischen Ebenen identifiziert. Drei Gruppen bilden das erste Level der Hierarchie:

- Zurückhaltende Informationssuchende,
- Pragmatische Informationssuchende,
- Interessierte Informationssuchende.

Abbildung 1 (siehe Seite 172) zeigt die hierarchische Struktur der identifizierten Archetypen. Im Folgenden werden die Archetypen auf der unteren hierarchischen Ebene kurz beschrieben.

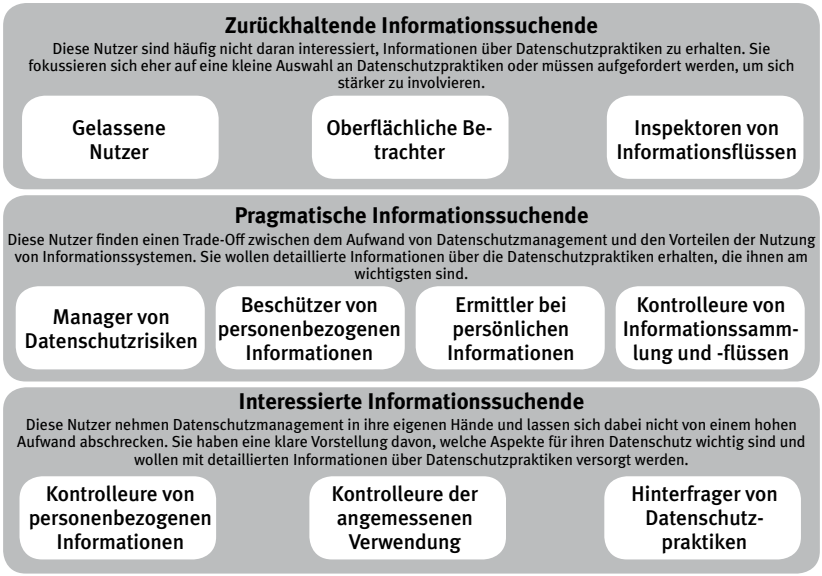

Abbildung 1: Verbraucherarchetypen.

Gelassene Nutzer: Diese Verbraucherinnen und Verbraucher kümmern sich nur wenig um Datenschutz und haben sehr geringe Informationsbedürfnisse. In wenigen Fällen möchten sie über Datenschutzpraktiken informiert werden, aber ihre Informationsbedürfnisse weisen keine eindeutigen Muster auf.

Oberflächliche Betrachter: Diese Verbraucherinnen und Verbraucher sind sich einer weiten Bandbreite an Datenschutzproblematiken bewusst, haben allerdings nur latente Informationsbedürfnisse. Sie wollen Informationen über Datenschutzpraktiken nur in bestimmten Situationen (zum Beispiel Sammlung von offensichtlich irrelevanten Informationen) erhalten.

Inspektoren von Informationsflüssen: Diese Verbraucherinnen und Verbraucher sind vor allem an der Vernetzung von Informationssystemen untereinander interessiert. Sie verlangen einige generelle Informationen über die Sammlung von Informationen, sind aber vor allem an erteilten Einwilligungserklärungen und der Behandlung ihrer Informationen interessiert.

Manager von Datenschutzrisiken: Diese Verbraucherinnen und Verbraucher kennen die Risiken bei der Nutzung von Informationssystemen und wollen mit Informationen versorgt werden, um diese Risiken abschätzen zu können. Sie sind vor allem daran interessiert, welche sensitiven Informationen gesammelt werden und wie mit diesen umgegangen wird.

Beschützer von personenbezogenen Informationen: Diese Verbraucherinnen und Verbraucher möchten es vermeiden, ihre personenbezogenen Informationen an jedes Informationssystem weiterzugeben. Sie müssen informiert werden welche und wie personenbezogenen Informationen gesammelt werden, wie diese behandelt werden und wie Sie über Änderungen informiert werden.

Ermittler bei persönlichen Informationen: Diese Verbraucherinnen und Verbraucher sind nicht sehr stark an Datenschutzpraktiken interessiert, wenn sie der Meinung sind, dass sie nicht identifizierbar sind. Sobald sie allerdings identifizierbar werden, möchten sie mit einer weiten Bandbreite an Informationen versorgt werden.

Kontrolleure von Informationssammlung und -flüssen: Diese Verbraucherinnen und Verbraucher interessieren sich wenig dafür, zu welchem Zweck Datenschutzpraktiken ausgeführt werden. Sie wollen allerdings im Detail informiert werden welche und wie Informationen gesammelt werden, wie diese behandelt werden und wie sie Kontrolle ausüben können.

Kontrolleure von personenbezogenen Daten: Diese Verbraucherinnen und Verbraucher sind nur wenig an Datenschutzpraktiken interessiert, die nicht personenbezogenen Informationen betreffen. Sie müssen darüber informiert werden welche und wie personenbezogenen Informationen gesammelt werden, wie diese behandelt werden, ob diese für die gewünschten Zwecke genutzt werden, und wie sie Kontrolle ausüben können.

Kontrolleure der angemessenen Verwendung: Diese Verbraucherinnen und Verbraucher akzeptieren, dass Datenschutzrisiken zu einem gewissen Grad unausweichlich sind. Allerdings möchten Sie darüber informiert werden was die Gründe von Datenschutzpraktiken sind und wie sie kontrollieren können, dass Informationen nicht weiterführend genutzt werden.

Hinterfrager von Datenschutzpraktiken: Diese Verbraucherinnen und Verbraucher wollen fast alles über Datenschutzpraktiken und den Grund ihrer Ausübung erfahren. Sie müssen daher mit ausführlichen Informationen versorgt werden.

5 Diskussion der Ergebnisse

Die Ergebnisse unserer Studie zeigen, dass sich Datenschutzinformationsbedürfnisse zwischen verschiedenen Gruppen von Verbraucherinnen und Verbrauchern stark unterscheiden. Einige Verbraucherinnen und Verbraucher weisen nur geringe Informationsbedürfnisse auf, andere haben starke Interessen an einer kleinen Auswahl spezieller Datenschutzpraktiken, und wieder andere möchten über fast alles informiert werden, das Datenschutz betrifft. Einige Datenschutzpraktiken sind für fast alle Verbraucherinnen und Verbraucher von Wichtigkeit (zum Beispiel Sammlung und Weitergabe von Nutzerinformationen). Andere Datenschutzpraktiken wiederum sind für fast Niemanden von Interesse (etwa Datenformate der gesammelten Informationen).

Die Projektergebnisse liefern eine Grundlage für die Entwicklung von zukunftsträchtigen PETs, die explizit auf die Bedürfnisse der Verbraucherinnen und Verbraucher ausgerichtet sind und diese in den Mittelpunkt stellen. Welche PETs für Verbraucherinnen und Verbraucher im Kontext welcher Informationssysteme relevant sind, konnte allerdings im Rahmen dieser Studien nicht beantwortet und sollte in Feldstudien ergründet werden. Anbieter können auf die Bedürfnisse verschiedener Verbraucherarchetypen eingehen und ihre Angebote entsprechend gestalten. Verbraucherinnen und Verbraucher profitieren, indem sie genau die Informationen bekommen, die sie benötigen. Auf diese Weise wird sowohl Informationsüberflutung als auch das Fehlen von Informationen, die von Verbraucherinnen und Verbrauchern als wichtig empfunden werden, verhindert. Zukünftige Forschung könnte weitere quantitative Umfragen mit einer größeren und soziodemografisch repräsentativeren Stichprobe durchführen, um so weitere Archetypen auf tieferen hierarchischen Ebenen zu analysieren. Des Weiteren könnten qualitative Untersuchungen dazu beitragen, ein tiefgründiges Verständnis der

identifizierten Archetypen und ihrer Charakteristiken zu entwickeln. Es wäre außerdem von großem Interesse zu erfahren, wie Verbraucherinnen und Verbraucher Informationsbedürfnisse bilden und von welchen Faktoren diese beeinflusst werden. Eine weitere interessante Fragestellung ist, wie Informationen so dargestellt werden können, dass Datenschutzinformationsbedürfnisse von Verbrauchern im Alltag auch bedient werden können. Datenschutzerklärungen sind hier offensichtlich kein vielversprechender Ansatz (McDonald und Cranor 2008). Relevante Fragestellungen sind wann, in welcher Form und über welche Endgeräte Informationen zur Verfügung gestellt werden sowie die Möglichkeiten, die Verbrauchern angeboten werden, um Einfluss auf die Datenverarbeitung zu nehmen (Schaub et al. 2015). Adressierung von Verbraucherbedürfnissen ist ein Kernbestandteil von weltweiten Datenschutzgesetzen, insbesondere auch der EU Datenschutzgrundverordnung. Alltagstaugliche Ansätze dafür wurden allerdings bisher weder von Regierungen oder dem Markt noch von Verbrauchern selbst entwickelt. Die Erkenntnisse dieser Studie dienen als Grundlage für zukünftige Ansätze mit dem Ziel, diese Lücke zu schließen.

6 Handlungsempfehlungen

Angelehnt an die Forschungsergebnisse lassen sich folgende Handlungsempfehlungen für eine gute Verbraucherpolitik ableiten.

- Bestehende Angebote zur Kommunikation von Datenschutzpraktiken überladen Verbraucherinnen und Verbraucher mit zu vielen Informationen und führen dazu, dass diese nicht genutzt werden. Dieser Umstand muss geändert werden, damit es realistisch wird, dass Verbraucherinnen und Verbraucher wissen, was mit ihren persönlichen Informationen passiert.

- Verbraucherinnen und Verbraucher unterscheiden sich in ihren Datenschutzinformationsbedürfnissen. Um eine effektive Kommunikation von Datenschutzpraktiken zu ermöglichen, müssen PETs Informationsbedürfnisse stärker berücksichtigen und insbesondere solche Informationen

kommunizieren, die für Verbraucherinnen und Verbraucher relevant sind. In der Praxis sollten Organisationen versuchen, ihre Nutzerbasis dahingehend zu untersuchen, welche Verbraucherarchetypen besonders stark vertreten sind und ihre Kommunikation von Datenschutzpraktiken entsprechend ausrichten. Dabei müssen allerdings die geltenden gesetzlichen Informationspflichten basierend auf europäischem und nationalem Recht berücksichtigt werden.

- Informationen über die Sammlung und Weitergabe von Nutzerinformationen, das Management von Einwilligungserklärungen und Benachrichtigungen im Fall von Datenschutzverstößen sind für Verbraucherinnen und Verbraucher besonders relevant, vor allem immer dann, wenn personenbezogene Daten betroffen sind. Daher sollte der Kommunikation dieser Datenschutzpraktiken besondere Aufmerksamkeit geschenkt werden.

- Bisher beschränken sich Anbieter von IT-Angeboten häufig auf die rechtlichen Vorgaben zur Kommunikation von Datenschutzpraktiken. Hinsichtlich eines steigenden Bewusstseins der Bedeutung von Datenschutz und Privatheit in der Verbraucherschaft, ist zu erwarten, dass Anbieter zukünftig versuchen werden, durch explizite Bewerbung von transparenten Datenschutzpraktiken Verbraucherinnen und Verbraucher auf ihre Angebote aufmerksam zu machen und so die eigene Marktposition zu stärken.

Literatur

Ackerman, Mark S., Lorrie Faith Cranor und Joseph Reagle. 1999. Privacy in e-commerce. In: *Proceedings of the ACM Conference on Electronic Commerce: Denver, Colorado, November 3-5, 1999,* hg. von Conference on Electronic Commerce und Association for Computing Machinery, 1-8. New York: ACM Press.

Acquisti, Alessandro, Laura Brandimarte und George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, Nr. 6221: 509-514. doi: 10.1126/science.aaa1465.

Antón, Annie I., Julia B. Earp und Jessica D. Young. 2010. How internet users' privacy concerns have evolved since 2002. *IEEE Security & Privacy* 8, Nr. 1: 21-27. doi: 10.1109/MSP.2010.38.

Berendt, Bettina, Oliver Gerendt und Sarah Spiekermann. 2005. Privacy in e-commerce: Stated preferences vs. actual behavoiur. *Communications of the ACM* 48, Nr. 4: 101-106. doi:10.1145/1053291.1053295.

Brüggemann, Thomas, Joel Hansen, Tobias Dehling und Ali Sunyaev. 2016. An information privacy risk index for mHealth apps. In: *Privacy Technologies and Policy*, hg. von Stefan Schiffner, Jetzabel Serna, Demosthenes Ikonomou, und Kai Rannenberg, 190–201. Cham: Springer International Publishing. doi:10.1007/978-3-319-44760-5_12.

Cranor, Lorrie Faith, Joseph Reagle und Mark S. Ackerman. 1999. Beyond concern: Understanding net users' attitudes about online privacy. AT&T Labs-Research Technical Report, TR 99.4.3. https://arxiv.org/html/cs/9904010/report.htm.

Culnan, Mary J. 1993. ‚How did they get my name?': An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly* 17, Nr. 3: 341-363. doi: 10.2307/249775.

Dehling, Tobias, Fangjian Gao, Stephan Schneider und Ali Sunyaev. 2015. Exploring the far side of mobile health: Information security and privacy of mobile health apps on iOS and android. *JMIR mHealth uHealth* 3, Nr. 1: e8. doi: 10.2196/mhealth.3672.

Dehling, Tobias, Manuel Schmidt-Kraepelin, Muhammed Demircan, Jakub Szefer und Ali Sunyaev. 2016. User archetypes for effective information privacy communication. Pre-ICIS workshop on information security and privacy, Dublin, Ireland.

Dehling, Tobias und Ali Sunyaev. 2014. Secure provision of patient-centered health information technology services in public networks – leveraging security and privacy features provided by the German nationwide health information technology infrastructure. Electronic Markets 24, Nr. 2: 89–99. doi:10.1007/s12525-013-0150-6.

Dinev, Tamara und Paul Hart. 2006. Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce* 10, Nr. 2: 7-29. doi: 10.2753/JEC1086-4415100201.

Dinev, Tamara, Heng Xu, Jeff H. Smith und Paul Hart. 2013. Information privacy and correlates. An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems* 22, Nr. 3: 295-316. doi: 10.1057/ejis.2012.23.

European Commission. 2011. *Attitudes on data protection and electronic identity in the European Union.* Special Eurobarometer 359. Brüssel: TNS

Opinion & Social. http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf.

Kumaraguru, Ponnurangam and Cranor, Lorrie Faith . 2005. Privacy Indexes: A survey of Westin's studies. (CMU-ISRI-5-138). Institute for Software Research International, School of Computer Science, Carnegie Mellon University , Pittsburgh, PA. http://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf.

McDonald, Aleecia M. und Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4, Nr. 3: 540-565.

Park, Yong Jin. 2013. Digital literacy and privacy behavior online. *Communication Research* 40, Nr. 2: 215-236. doi: 10.1177/0093650211418338.

Schaub, Florian, Rebecca Balebako, Adam L. Durity und Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In: *Eleventh symposium on usable privacy and security (SOUPS 2015)*, 1–17. Ottawa: USENIX Association. https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub.

Spiekermann, Sarah, Jens Grossklags und Bettina Berendt. 2001. E-privacy in 2nd generation e-commerce. Privacy preferences versus actual behaviour. In: *Proceedings of the 3rd ACM Conference on Electronic Commerce: Tampa, Florida, USA, October 14-17, 2001,* hg. von Conference on Electronic Commerce und Association for Computing Machinery, 38-47. New York: ACM Press.

Sunyaev, Ali, Tobias Dehling, Patrick L. Taylor und Kenneth D. Mandl. 2015. Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association* 22: e28–e33. doi: 10.1136/amiajnl-2013-002605.

Tavani, Herman T. 2007. Philosophical theories of privacy. *Metaphilosophy* 38, Nr. 1: 1-22. doi: 10.1111/j.1467-9973.2006.00474.x.

Tavani, Herman T. und James H. Moor. 2001. Privacy protection, control of information, and privacy-enhancing technologies. *ACM SIGCAS Computers and Society* 31, Nr. 1: 6-11. doi: 10.1145/572277.572278.

Ward, Joe H. 1963. Hierarchical grouping to optimize an objective function. *Journal of the American Statistical Association* 58, Nr. 301: 236-244. doi: 10.1080/01621459.1963.10500845.

Weber, Rolf H. 2010. Internet of things – new security and privacy challenges. *Computer Law & Security Review* 26, Nr. 1: 23-30. doi: 10.1016/j.clsr.2009.11.008.

Woodruff, Allison, Vasyl Pihur, Sunny Consolvo, Lauren Schmidt, Laura Brandimarte und Alessandro Acquisti. 2014. Would a privacy fundamentalist sell their DNA for $1000...if nothing bad happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences. In: *Proceedings of the Symposium On Usable Privacy and Security: SOUPS '14*.

Xu, Heng, Sumeet Gupta, Mary Beth Rosson und John M. Carroll. 2012. Measuring mobile users' concerns for information privacy. In: *Proceedings of the Thirty Third International Conference on Information Systems* (ICIS 2012).

Zhu, Hui, Carol X. J. Ou, W. J. A. M. van den Heuvel und Hongwei Liu. 2017. Privacy calculus and its utility for personalization services in e-commerce. *Information & Management* 54, Nr. 4: 427-437. doi: 10.1016/j.im.2016.10.001.

Über die Autoren

Prof. Dr. Ali Sunyaev ist Professor für Angewandte Informatik am Karlsruher Institut für Technologie (KIT) und leitete an der Universität zu Köln das im Rahmen des KVF NRW geförderte Projekt „Verbraucherorientierter Datenschutz". Webseite: http://www.aifb.kit.edu/web/Ali_Sunyaev.

Dr. Tobias Dehling ist wissenschaftlicher Mitarbeiter am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie (KIT) und war Mitarbeiter im Rahmen des KVF NRW geförderten Projekts „Verbraucherorientierter Datenschutz" an der Universität zu Köln. Webseite: http://www.aifb.kit.edu/web/dehling.

M.Sc. Manuel Schmidt-Kraepelin ist Doktorand am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie (KIT) und war Mitarbeiter im Rahmen des KVF NRW geförderten Projekt „Verbraucherorientierter Datenschutz" an der Universität zu Köln. Webseite: http://www.aifb.kit.edu/web/Manuel_Schmidt-Kraepelin.