4 Der datensouveräne Bürger

„Dann drück ich auf's Mikro, wenn's hier mal um Dinge geht...": Kreative Privatisierung. Der Umgang mit Privatheitsansprüchen in der Smart Speaker-Nutzung

Lukas Schmitz

Zusammenfassung

Der vorliegende Beitrag erörtert den Umgang mit dem Datenkapitalismus im häuslichen Umfeld am Beispiel der Smart Speaker-Nutzung. Menschen nutzen Smart Speaker im Alltag aus Motiven der Erleichterung und produzieren dabei Daten, die von Unternehmen angeeignet werden; dabei bleibt zumeist unklar, wie diese Daten ausgewertet werden und welches Risiko für die Nutzer:innen damit verbunden ist. Mithilfe einer pragmatistischen Theorie des Attachments wird gezeigt, dass Menschen dieses Risiko unter Rückgriff auf Formen des Vertrauens sowie Strategien der Analogisierung bearbeiten. Auf diese Weise wird ein tiefergehendes Verständnis der kreativen Auseinandersetzung von Nutzer:innen mit antizipierten Privatheitsbedrohungen erarbeitet, das ermöglicht, den je spezifischen Umgang nicht als paradox – im Sinne eines Widerspruchs zwischen Sensibilität in Privatheitsfragen und ergriffenen Maßnahmen – , sondern als erfahrungsgeleitete Auseinandersetzung zu beschreiben.

1. Einleitung

Privatheitsfragen gehören zu den drängendsten Herausforderungen in Zeiten der fortschreitenden Digitalisierung jedweder Lebensbereiche. Mit dem steigenden Zugriff privatwirtschaftlicher Akteure auf Datensätze, die Eigenschaften und Verhalten von Nutzer:innen verschiedener Dienstleistungen sammeln und prognostizieren, gewinnen diese Fragen an Brisanz. Sie verlangen nach einer Antwort, die den Ansprüchen eines sich digitalisierenden Gemeinwesens (in staatlicher und wirtschaftlicher Hinsicht) einerseits und einer demokratisch integrierten und selbstbestimmten Bürger:in andererseits Rechnung trägt. Dass die Sammlung von Daten Voraussetzung von Gesellschaft ist und eine Lösung nicht darin bestehen kann, diese *nicht* zu erheben, ist mittlerweile ein Gemeinplatz der Privatheitsforschung gewor-

den. Jedoch ist insbesondere der Umgang mit der Kapitalisierung ebenjener Daten eine besondere Herausforderung – zu unklar ist das Ausmaß der Sammlung sowie die Art der Verwertung, zumal die Möglichkeiten der Bürger:innen, Handlungsmacht in dieser Frage zu gewinnen, beschränkt sind (Lamla 2019). Seien es Unkenntnis über technische Möglichkeiten der Kontrolle der eigenen Daten, der bewusste Verzicht auf Kontrolle zugunsten sozialer Teilhabe oder schlicht Unlust, sich mit den häufig komplizierten Zusammenhängen zu beschäftigen – potenzielle Gefahren des Datenkapitalismus sind offenbar und dennoch scheint im alltäglichen Umgang das stille Einvernehmen, Daten für Bequemlichkeit der Nutzung digitaler Dienstleistungen preiszugeben, etabliert.

Die Diskussion ebendieser Fragen ist währenddessen in verschiedenen Diskursen verortet, sei es in der Medienberichterstattung, der akademischen Sphäre, parlamentarischer Diskussion und Gesetzgebung, Verlautbarungen zivilgesellschaftlicher Akteure oder in den individuellen Reflexionen der Staatsbürger, in denen Auswirkungen der um sich greifenden Datensammlung behandelt werden.

Allerdings hinkt der Diskurs dabei der Wirklichkeit hinterher. Daten werden fortlaufend gesammelt und der Begleitdiskurs erörtert allzu häufig eine Perspektive ex post – als nachträgliche Korrektur von Fehlentwicklungen oder einer verspäteten Einsicht in kritische Potenziale technischer Neuerungen. Ganz unabhängig von bestehenden, möglichen und künftigen Regelungsverfahren, die den Einzelnen vor Übergriffen (gleich welcher Art: sei es in personalisierter Werbung oder im potenziellen Angriff auf Persönlichkeitsrechte) schützen, sehen sich Menschen gegenwärtig der Frage ausgesetzt, wie sie dem Datenkapitalismus im Alltag begegnen. Die Antworten dafür können verschieden ausfallen: Plädieren die einen für eine systemische Lösung, da es schwerfällt, durchgehend Aufmerksamkeit für potenziell bedrohlichen Datenfluss aufzubringen, verorten andere die Kontrollgewalt über den Datenkapitalismus in einem selbstbestimmten Akteur, der – vermeintlich gut informiert und privatheitssensibel – selbst alles Nötige aufbringt, um seine Privatheit (worin auch immer sie besteht) zu schützen.

Dieser Aufsatz erörtert den Umgang von Menschen mit Fragen der Privatheit am Beispiel der Smart Speaker-Nutzung im häuslichen Bereich:[1]

1 Als Smart Speaker werden hier Sprachassistenten wie Amazon Echo, Google Nest oder Apple Home Pod verstanden, also Lautsprecher mit integrierten Mikrophonen, die auf Sprachbefehle hin verschiedene Funktionen ausführen können, so etwa Internet-

Wie begegnen Menschen dem Umstand, dass sie in ihrem häuslichen Bereich potenziell Daten produzieren, die über den Smart Speaker von einer dritten Partei nutzbar gemacht werden können? Nach welchen Kriterien werden in der Smart Speaker-Nutzung Privatheitsansprüche formuliert, wo sind die Grenzen der Umsetzung dieser Privatheitsansprüche und auf welche Art stellen Nutzer:innen ihre persönliche, gefühlte Privatheit wieder her? Insbesondere das Bild des selbstbestimmten, rationalen Akteurs, der eine informierte Entscheidung über seine Privatheit trifft, soll dabei kritisch hinterfragt werden. Es bestehen bereits einige Ansätze dazu, das sogenannte Privacy Paradox (Barnes 2006),[2] also die Beobachtung, dass Personen im Gespräch ihre Privatheit als zentralen Wert adressieren, aber im konkreten Handeln diese Sensibilität missen lassen, zu dekonstruieren (Trepte u. a. 2020; Solove 2021; Agi/Jullien 2018). Daran anknüpfend verfolgt dieser Aufsatz einen Ansatz, der unter Rückgriff auf eine pragmatistische Theorietradition eine Perspektive eröffnet, die das Handeln von Personen nicht als Ergebnis von objektiv gebotenen (und entsprechend subjektiv ausgedeuteten), rationalen Kriterien behandelt, sondern als individuelle Auseinandersetzung und Aushandlung, die vor dem Hintergrund persönlicher Erfahrung vorgenommen wird.

Für die Auseinandersetzung mit diesen Fragestellungen greife ich zurück auf Interviewmaterial aus zehn Besuchen in Haushalten, die mit Smart Speakern ausgestattet sind. Im Ergebnis zeigt sich, dass die Auseinandersetzung mit Privatheitsfragen in der Smart-Speaker-Nutzung als kreative Aushandlung begriffen werden muss, die in spezifischen, scheinbar teils widersprüchlichen oder inkonsistenten, Formen der Privatisierung mündet. Nach einer soziologischen Begriffsbestimmung der Privatheit (2.1) wird ein Überblick über den Forschungsstand zu Smart Speakern und Privatheit bereitgestellt (2.2). Anschließend wird eine pragmatistische Theoriegrundlage erarbeitet (3) sowie das methodische Vorgehen vorgestellt (4); daraus resultieren empirische Ergebnisse zur „Kreativen Privatisierung" (5), die abschließend in einem Fazit zusammengefasst werden (6).

recherche, Koordinierungsleistungen (Terminplanung, Steuerung von IoT-Vernetzungen) oder Unterhaltungsfeatures.

2 Eine frühe Beobachtung dieses Phänomens findet sich auch bei: Acquisti, Grossklags (2005): Privacy and Rationality.

2. Forschungsstand

2.1 Privatheit als soziologischer Begriff

Bevor der Umgang von Personen mit Fragen der Privatheit in Bezug auf Smart Speaker behandelt wird, wird hier zunächst ein soziologischer Begriff der Privatheit erarbeitet. Zu berücksichtigen ist, dass der Diskurs um den Begriff der Privatheit überaus differenziert ist, sodass keine umfassende Zusammenfassung der vielfältigen Ausprägungen gegeben werden kann, die sich auch nach wissenschaftlicher Disziplin massiv unterscheiden.[3] Auch die Ansprüche an einen Privatheitsbegriff differieren je nach disziplinärer Verortung stark: Während in der Informatik etwa der Schwerpunkt häufig auf technischen Möglichkeiten zu Datenkontrolle liegt, ist die Sozialwissenschaft eher an einer theoretischen Bestimmung und insbesondere im Falle der Sozialphilosophie auch der normativen Dimension des Begriffs interessiert.

Häufig beschreiben theoretische Perspektiven auf Privatheit ein spezifisches Verhältnis des Subjekts zu einer übergeordneten Struktur, zumeist einem bestimmten Begriff der Öffentlichkeit. In klassischen soziologischen Ansätzen steht dabei mal das Private, mal das Öffentliche im Fokus, etwa indem das Private als Vorbereitungsraum für öffentliches, politisches Wirken und also als Grundlage für eine funktionierende Demokratie beschrieben wird (Arendt 2002) oder indem ein Idealbild von Öffentlichkeit gezeichnet wird, in dem Privatleute bar jeden Eigeninteresses einen Diskurs um die objektiv bestmögliche Organisation des Staates führen (Habermas 1990).

Mittlerweile besteht jedoch Konsens darin, dass Öffentlichkeit und Privatheit keinen Gegensatz bilden, sondern ein komplementäres Antithesenpaar im Wandel. Laut Armin Nassehi muss etwa die systematische Datensammlung im 19. Jh., nicht allein als Übergreifen staatlicher Gewalt auf private Lebenswelten verstanden werden, sondern Staatlichkeit – und damit auch eine spezifische Arena der Öffentlichkeit – lässt sich vielmehr nur auf Grundlage systematischer Datensammlung herstellen. Die staatliche Datensammlung wiederum bringt auf diese Art eine Blaupause für Normalität in der individuellen Lebensführung hervor. Bürgerliche Vorstellungen von Privatheit sind entsprechend als Ergebnis von Selbsttechniken zu verstehen,

3 Für eine ausführliche Darstellung des soziologischen Privatheitsdiskurses siehe: Lamla u.a. (2022): Privatheit und Digitalität.

die sich als Reaktion auf äußere Erwartung und Datensammlung herausbilden (Nassehi 2019, S. 307f.). Die vermeintlichen Gegensätze Privatheit und Öffentlichkeit bringen sich also wechselseitig hervor und sind nur in dieser Verwobenheit zu denken.

Privatheit zeichnet sich, um diese Verwobenheit weiterhin zu unterstreichen, zudem auch durch bestimmte Praktiken der Offenbarung aus – wenn man etwa an ein geteiltes Geheimnis in einer privaten Beziehung denkt. Anderseits funktioniert Öffentlichkeit nur über spezifische Praktiken der Privatisierung: Höflichkeit als gesellschaftliche Umgangsform, und damit in der Sphäre des Öffentlichen verortet, beispielsweise ist häufig dadurch gekennzeichnet, dass bestimmte Dinge nicht zur Sprache kommen; auch dass man sich an öffentlichen Orten i. d. R. bemüht, seine Umgebung nicht durch lautes Sprechen zu stören, verdeutlicht die enge Verzahnung der Sphären (Roessler/Mokrosinska 2013).

Neuere Ansätze konzentrieren sich daher auch weniger auf das grundsätzliche Verhältnis von Privatheit und Öffentlichkeit als Gegensatzpaar, sondern erarbeiten differenziertere Kartierungen, indem sie etwa den Begriff der Privatheit theoretisch in verschiedenen Dimensionen bestimmen oder sich den Praktiken der Privatisierung – häufig unter den Vorzeichen der Digitalisierung – widmen. Der Begriff der Privatheit spielt verschiedene Rollen und wird in höchst unterschiedlichen Zusammenhängen in Anschlag gebracht. Die aktuelleren Ausarbeitungen versuchen entsprechend, dieser Vielfalt gerecht zu werden, indem sie den Begriff theoretisch dynamisieren.

So entwirft Beate Roessler einen multidimensionalen Zugang zum Privatheitsbegriff, indem sie drei Ausrichtungen des Privaten beschreibt. Sie differenziert zwischen dezisionaler, informationeller sowie lokaler Privatheit: Während dezisionale Privatheit die Freiheit zur selbstbestimmten Entscheidung beschreibt, umfasst informationelle Privatheit die Art und Weise, selbstbezogene Aufschlüsse in sozialen Beziehungen zu moderieren. Lokale Privatheit schließlich zielt auf eine spezifische Räumlichkeit ab, die dem Menschen als Schutzraum die Möglichkeit zur freien Entfaltung bietet (Roessler 2001).

Helen Nissenbaum dagegen versteht Privatheit nicht als Kontrollbegriff ausgehend vom Individuum, sondern, nicht zuletzt vor dem Hintergrund fortschreitender Digitalisierung, als kontextabhängig. So beschreibe Privatheit nicht das Recht, persönliche Informationen zu kontrollieren, sondern jenes „to live in a world in which our expectations about the flow of personal information are, for the most part, met" (Nissenbaum 2010, S. 231).

Eine Privatheitsverletzung liege nicht vor, wenn eine Person keine absolute Kontrollgewalt über diese Informationen hat, sondern wenn die impliziten Normen der jeweiligen Kontexte verletzt werden. Privatheit besteht so verstanden in *Contextual Integrity*.

Auch für Christina Nippert-Eng (2010) ist Privatheit kein holistischer Begriff, sondern Gegenstand der Aushandlung in Praktiken des Teilens oder Verbergens. Absolute Privatheit als solche gebe es nicht, vielmehr versuchten Menschen, sich gewissermaßen situativ private Inseln zu schaffen, in denen sie Kontrollgewalt über zu teilendes oder nicht zu teilendes besitzen.

Den Praktiken des Teilens und Verbergens wenden sich auch Alice Marwick und danah boyd zu. In ihrer Arbeit zum Verhalten von Teenagern in sozialen Medien zeigen sie, dass diese ihre Privatheit auf kreative Weise in Auseinandersetzung mit der Technik herstellen. Insbesondere soziale Netzwerke arbeiten mit einem solch hohen Maß an Sichtbarkeit, dass eine absolute Kontrolle kaum möglich ist. Entsprechend bilden Teenager kreative Weisen des Umgangs heraus, mit denen sie einerseits ihre Privatheit schützen und andererseits nicht auf soziale Teilhabe verzichten müssen; dabei argumentieren Marwick/boyd, dass soziale Medien grundsätzlich die Art und Weise verändern, wie Privatheit verhandelt wird (Marwick/boyd 2014).

Eine umfassende Bestimmung des Begriffs der Privatheit, der in einem spezifischen Verhältnis der Verwobenheit von Privatheit und Öffentlichkeit besteht, bietet Carsten Ochs. Dafür nähert er sich dem Begriff aus zwei Richtungen. Einerseits beschreibe das Private vom Individuum ausgehend gedacht sogenannte Erfahrungsspielräume: Durch bestimmte Praktiken der Beschränkung oder Öffnung dieser Spielräume mache sich das Individuum bestimmte Erfahrungen zugänglich oder schließe diese aus. Andererseits werde über den Begriff der Privatheit auch markiert, in welchem Maße eine Öffentlichkeit im Sinne von dem Individuum distanten Akteuren wie Staaten oder Unternehmen, an diesem teilhaben können: Das Maß, in dem das Individuum diesen Zugriff zulasse, bestimme Privatheit als Teilhabebeschränkung (Ochs 2022).

Der soziologische Privatheitsbegriff kann also verschiedene Ausprägungen haben – gemein ist insbesondere aktuelleren Arbeiten aber der Fokus auf Aushandlungsprozesse sozialer Teilhabe in Auseinandersetzung mit kontextbestimmenden Faktoren. Insbesondere das konkrete Tun, also die situative, kontextgebundene Herstellung von Sicherheit, steht dabei im Vordergrund.

Hintergründe, die Smart Speaker als problematisch in Privatheitsfragen kennzeichnen, liegen freilich in der engen Verzahnung von Fragen der Privatheit mit Prozessen der Digitalisierung. Der Smart Speaker sammelt und speichert Daten – entsprechend gilt er auch als Projektionsfläche für Diskurse um Privatheit in Zeiten fortschreitender Digitalisierung.

Häufig liegt in diesen ein Fokus darauf, wie sich die soziale Welt mit der digitalen Transformation verändert: Insbesondere Datenerfassungs- und -verwertungspraktiken stehen dabei im Vordergrund (Palen/Dourish 2003; Gstrein/Beaulieu 2022). Problematisiert wird dabei der – von Shoshanna Zuboff benannte – *Überwachungskapitalismus*, indem argumentiert wird, dass gegenwärtig einem System Vorschub geleistet werde, das in der Sammlung und Kapitalisierung personenbezogener Daten totalitäre Züge trage (Zuboff 2018). Überhaupt ist die fortschreitende Digitalisierung bereits länger ein kritisches Thema für die Privatheitsforschung. Rief Reg Whitaker bereits 1999 das Ende der Privatheit aus (Whitaker 1999), kam sie als paradoxes Phänomen einige Jahre später doch wieder zu unverhoffter Prominenz: Susan Barnes' bereits oben erwähntes *Privacy Paradox* ist mittlerweile nachgerade ein geflügeltes Wort geworden und beschreibt die Beobachtung, dass Personen sich i. d. R. selbst als privatheitssensibel beschreiben, jedoch in der Interaktion diese scheinbare Sensibilität nicht an den Tag legten (Barnes 2006). Aus soziologischer Perspektive ist mit der Zuschreibung paradoxen Verhaltens unter Verweis auf eine objektive Rationalität jedoch nicht viel gewonnen. Entsprechend nähern sich viele sozialwissenschaftliche Perspektiven dem Begriff der Privatheit aus praxeologischer Perspektive, die akzeptiert, dass Handlungen von Subjekten nicht als intentional vorauszusetzen sind; vielmehr wirken Habitualisierungen und Routinisierungen handlungsleitend und je nach Medium, Sozialisation und Lebensphase entstehen neue Erfordernisse und Praktiken. (Roessler/Mokrosinska 2013; Marwyck/boyd 2014; Steijn/Vedder 2015; Suh/Hargittai 2015).

2.2 Smart Speaker und Privatheit

Bevor in der Folge das theoretische Programm dieses Aufsatzes näher ausgeführt wird und der konkrete Umgang mit antizipierten Privatheitsbedrohungen durch Smart Speaker im häuslichen Umfeld eingegangen wird, stellt der folgende Abschnitt einen Überblick zu bestehender Forschung zu Smart Speakern bereit. Gerade in Bezug auf Privatheitsfragen existiert eine

große Bandbreite an Forschungen, die im Folgenden skizziert wird.
Einige Publikationen widmen sich der Frage, was Menschen zur Nutzung von Smart Speakern bewegt. Dabei sind es insbesondere Motive der Erleichterung, die herausstechen, etwa in Bezug auf die Optimierung alltäglicher Aufgaben wie dem Schreiben von Einkaufslisten, Unterhaltung oder Bequemlichkeit (Rzepka 2019; Malodia 2024). Gleichwohl stellen Privatheitsbedenken ein Hindernis dar: Je ausgeprägter diese sind, desto weniger werden Smart Speaker genutzt (Buteau/Lee 2021).

Dabei herrscht Konsens, dass Nutzer:innen sich des Ausmaßes der Datensammlung nicht bewusst sind (Gautam 2022; Kröger u. a. 2022; Malkin u. a. 2019). Zudem verfügten sie nicht über die technischen Kompetenzen, dies einzuschätzen (Zeng u. a. 2017; Lau u. a. 2018a). Und auch, wenn Sensibilität in Bezug auf Privatheitsfragen vorhanden ist, ist es unwahrscheinlich, dass weitreichende Schutzmaßnahmen getroffen werden – ein Umstand, der in der Forschung als Privacy Pragmatism bzw. Privacy Cynicism beschrieben wird (Hoffmann u. a. 2016; Lutz/Newlands 2021). Was jedoch die Maßnahmen angeht, die Menschen zum Schutz ihrer Privatheit ergreifen, ist die Forschungslage nicht eindeutig: So geben Nutzer:innen auch bei geringer Kenntnis der tatsächlichen Bedrohung vorsorglich etwa bestimmte Informationen nicht an ihren Smart Speaker weiter (Brause 2020). Andererseits herrsche insgesamt wohl eine geringe Motivation, die eigene Privatheit zu schützen – weil Nutzer:innen sich keine Sorgen machen oder sich schlichtweg nicht damit auseinandersetzen. Dabei verfügen sie über elaborierte Begründungsfiguren, warum sich Schutzmaßnahmen nicht lohnen, etwa, weil sie den Wert der preisgegebenen Informationen als gering einschätzen oder argumentieren, dass ihre Informationen ohnehin schon an anderer Stelle erhoben werden (Lau u. a. 2018a). Auch die bewusste Aufgabe von Privatheit, um bestimmte Funktionen nutzen zu können, spielt dabei eine Rolle (Lau u. a. 2018b).

Die folgenden Abschnitte haben zum Ziel, genau diese Perspektiven auf Privatheit systematisch in den Blick zu nehmen: Was bewegt Menschen dazu, in ganz unterschiedlicher Art und Weise mit Privatheitsbedrohungen umzugehen? Im Kontext der Nutzung von Smart Speakern werden, um Beate Rössler erneut aufzugreifen, verschiedene Dimensionen von Privatheit angesprochen und potenziell bedroht; sei es in Bezug auf die räumliche Integrität des häuslichen Umfelds oder in der Entscheidungsgewalt darüber, welche Daten gesammelt und ausgewertet werden. Zu welchen Schritten greifen Nutzer:innen, um diesem Umstand zu begegnen? Dafür

wird zunächst eine theoretische Grundlage bereitgestellt, bevor diese Fragen in der Analyse empirischen Materials beantwortet werden.

3. Eine pragmatistische Theorieperspektive

Nutzer:innen weisen i. d. R. Sensibilität in Bezug auf Privatheit auf, handeln in der konkreten Nutzung das potenzielle Risiko aber in ganz individueller Weise aus. In diesem Abschnitt wird diese Aushandlung unter Rückgriff auf eine pragmatistische Theorietradition als erfahrungsgeleiteter Umgang mit einer neuartigen Technologie beschrieben. Es wird herausgestellt, dass menschliches Handeln nicht in einer Umsetzung von intentional und objektiv-rational geleiteten Motiven besteht, sondern in einer individuellen Auseinandersetzung mit der Umwelt auf Grundlage persönlicher Erfahrungswerte. Mit dem Begriff des Attachments wird verdeutlicht, dass diese Erfahrungen die Person konstituieren und somit den jeweiligen Umgang mit der Umwelt prägen.

Der Pragmatismus setzt sich seit seinen Anfängen im 19. Jahrhundert kritisch mit dem Begriff der ‚objektiven Wahrheit', der bis dahin große Teile der damals zeitgenössischen Philosophie prägte, auseinander. Diese Perspektive scheint daher geeignet, auch einen monolithischen Begriff der Privatheit, wie er im ‚Privacy-Paradox' zum Ausdruck kommt, zu dekonstruieren. Für William James (1842-1910), einen Gründervater des Pragmatismus, bedeutet ebendieser die „Herrschaft der empirischen Stimmung und ehrliches Aufgeben des rationalistischen Temperamentes" (James 1994, S. 22). Nicht mehr an einer objektiven Ratio soll das Handeln von Menschen gemessen werden, sondern durch ein Ernstnehmen der Empirie in einer gleichsam unendlichen Differenzierung aufgehen. Entsprechend schreibt James: „Der Pragmatismus fühlt sich nicht wohl, wenn er weit weg ist von Tatsachen. Der Rationalist fühlt sich nur in der Nähe von Abstraktionen behaglich" (ebd., S.35). Insoweit beschreibt der Pragmatismus zunächst eine Methode, die „aus jedem […] Wort seinen praktischen Kassenwert heraus[zu]bringen" (ebd. S.23) bestrebt ist – um soziale Zusammenhänge zu verstehen, plädiert James für einen „radikalen Empirismus". Nicht in der begrifflichen Abstraktion der Phänomene liege entsprechend der Erkenntnisgewinn, sondern vielmehr in der empirischen Ausdifferenzierung.

Ähnlich skeptisch ist der Pragmatismus in Bezug auf Intentionalität, die menschliches Handeln stets als geplant und zweckgerichtet beschreibt; Hans Joas versteht die pragmatistische Perspektive als „einen Bruch mit

einem teleologisch verengten Verständnis von Intentionalität" (Joas 1996, S. 366). So seien Handlungsverläufe „auch bei individuellem Handeln nie auf einzelne Intentionen zurückzuführen" (ebd., S. 228). Vielmehr stelle sich die Wirklichkeit der Person als widerständig dar: Personen begegnen Phänomenen stets vor dem Hintergrund in Routinen geronnener Erfahrung – nur passen diese häufig nicht zu den etablierten Weisen, der Welt zu begegnen. Daher sei es ein stetiges Ausprobieren und Testen, ein „kreative[s] Verarbeiten von Widerfahrnissen", welches das Handeln charakterisiere (ebd., S.366).

Unter Rückgriff auf einen weiteren Autor in pragmatistischer Tradition, Antoine Hennion, wird deutlich, dass Personen ihre Privatheit in Bezug auf die Smart-Speaker-Nutzung stets vor dem Hintergrund eines spezifischen *Attachments* vornehmen. Das Attachment – als die Erfahrungen, die der jeweiligen Person zu eigen sind und diese entsprechend konstituieren – prägt die Art und Weise, wie Menschen mit der Umwelt interagieren. Handlungen sind daher nicht allein als Ergebnis von Intentionalität zu verstehen, sondern als Ergebnis eines Wechselspiels mit dem jeweiligen Attachment (Hennion 2017, S. 74). Dieses bezieht sich auf eine individuelle Verhaftung in materiellen Konstellationen, persönlichen Beziehungen, Ideen und Diskurse, die performativ aktualisiert werden; auf diese Weise modelliert und reflektiert sich die Person auf eine Weise, die ihre eigene ist. Das Attachment ist gleichsam „die Rechnung, welche die Vergangenheit der Gegenwart präsentiert" (Hennion 2011, S. 94). Personen bilden in ihrer individuellen Gewordenheit einen Nexus aus Erfahrungen, Wissensbeständen und Praktiken, der vorprägt, wie neue Erfahrungen bearbeitet werden. Dieser Nexus symbolisiert gewissermaßen den Werkzeugkoffer (im Sinne von zur Verfügung stehenden Mitteln), mit dem Personen ihre Umwelt bearbeiten; gleichzeitig beschränkt er die Person in ihren Handlungsmöglichkeiten insofern, als die geronnene Erfahrung auch die Grenzen des Zugriffs definiert. Personen wechseln entsprechend zwischen 'aktiv' und 'passiv': Aktiv in der bewussten Bearbeitung der Umwelt unter Rückgriff auf etablierte Praktiken, passiv im Ausgesetzt-Sein dieser spezifischen Gewordenheit (Hennion/Gomart 1999, S. 243).

Das Attachment beschreibt also eine je individuelle Verhaftung in materiellen Settings, Praktiken und Diskursen, die den Menschen als solchen hervorbringen und die ihm in besonderer Weise gewohnt sind. Soziales Tun besteht in dieser Perspektive aus einem Wechselspiel aus Sich-hervorbringen und Hervorgebracht-werden, das zwischen der Person und ihrer Umwelt besteht. Der Begriff des Attachments erklärt, warum sich die Zu-

gänge, die technischen Kompetenzen und auch die Antizipation von Gefährdungspotential in Bezug auf Privatheit in der Smart-Speaker-Nutzung so unterschiedlich darstellen. Anstatt diese nach Konsistenz zu bewerten, müssen diese vielmehr als Ausdruck eines individuellen Weltzugriffs perspektiviert werden. Für eine verstehende Auseinandersetzung des Umgangs von Personen mit Privatheitsbedrohungen in der Smart Speaker-Nutzung muss also, um dem pragmatistischen Imperativ nachzukommen, zunächst die Komplexität empirischer Vielfalt ernst genommen werden, die sich am deutlichsten in einer materialnahen Analyse zeigt; der Begriff des Attachments hilft dann dabei, diese Komplexität theoretisch einzuordnen.

In Bezug auf die Datensammlung von Smart Speakern lautet die leitende Hypothese, dass der Umgang mit Privatheitsfragen durch Kenntnis potenzieller Risiken und technischer Zusammenhänge grundiert ist, die von Person zu Person differieren. Dies bedeutet zunächst: Wer über kein entsprechendes Attachment verfügt, hat auch kaum eine Vorstellung davon 1) was Daten überhaupt sind 2) wie sie angeeignet werden können und von wem das auf welche Weise technisch bewerkstelligt wird sowie 3) was mit den Daten anschließend passiert, etwa wie und zu welchem Zweck sie ausgewertet werden. Privatheit als relevantes Thema wird in den Interviews durchaus reflektiert adressiert – der jeweilige Umgang macht jedoch deutlich, dass die Bearbeitung der Thematik stets vor einem spezifischen Attachment vorgenommen wird. Wie also handeln Personen in Bezug auf Smart Speaker, und worin besteht die Kreativität der Auseinandersetzung? Was sind die Attachments, gleichsam die Blaupausen der Erfahrung, die mit dem neuen technischen Artefakt in Einklang gebracht werden müssen, wo die Bruchlinien? Im folgenden Abschnitt wird zunächst der methodische Zugang dargestellt, bevor anschließend verschiedene Dimensionen (im pragmatistischen Sinne:) kreativer Privatisierung als Ausdruck des personenspezifischen Attachments erarbeitet werden.

4. Methodischer Zugang

Der Datenkorpus, der die Grundlage der folgenden Auswertung bildet, umfasst Material aus ethnografischen Besuchen in zehn Haushalten. Die Datenerhebung fand also im häuslichen Umfeld der Studienteilnehmer:innen statt. Für die Rekrutierung der Studienteilnehmer:innen wurde zunächst eine Zeitungsannonce geschaltet; anschließend wurde das Sample nach einem Schneeballsystem ergänzt, um eine höhere Heterogenität zu

erreichen. Hatten sich auf die Annonce zunächst überzeugte Nutzer:innen von Smart Speakern gemeldet, wurde in der Folge insbesondere darauf geachtet, auch kritischere Stimmen einzufangen, etwa von Personen, die den Smart Speaker kaum benutzen oder wieder abgeschafft hatten. Die Haushalte befanden sich im städtischen wie im ländlichen Bereich und waren unterschiedlich mit smarter Technik ausgestattet; es wurden häusliche Umgebungen sogenannter ‚early adopter' ebenso erhoben wie Haushalte, die lediglich über einen einzigen Smart Speaker verfügten – in einem Falle wurde der Smart Speaker sogar ‚aus Versehen' angeschafft, nämlich in eine Lautsprecherbox integriert. Die Gesprächspartner:innen lebten entweder alleine oder in Partnerschaft. In letzterem Fall wurde entweder mit beiden Partner:innen gesprochen oder mit einer Person, wobei darauf geachtet wurde, nicht nur mit jenen Interviews zu führen, welche die Anschaffung der Smart Speaker ursprünglich initiiert hatten. Das Alter der befragten Personen variierte ebenso wie der Bildungsgrad (im Studium; abgeschlossene Ausbildung; Hochschulabschluss). Bis auf eine Ausnahme lebten in den erhobenen Haushalten keine Kinder.

In der Erhebungssituation wurde zunächst eine Techniksichtung vorgenommen, in der sämtliche smarten Geräte, insbesondere Smart Speaker, in Augenschein genommen wurden: Wo stehen diese und wie fügen sie sich in das häusliche Arrangement ein? Wie sind sie miteinander vernetzt und wie werden sie gesteuert? Wofür werden sie benutzt? Im Fokus standen dabei insbesondere die individuellen Motive der Nutzer:innen für die jeweilige Smart Speaker-Nutzung (Hine 2019). Für eine umfassende Rekonstruktion der Forschungsumgebung wurde der gesamte Besuch mit einem Sprachrekorder aufgenommen sowie Feldnotizen für ergänzende Beobachtungen angelegt; außerdem wurde das Gezeigte über Fotomaterial dokumentiert. Anschließend wurde mit den Studienteilnehmern ethnografische Interviews geführt, in denen diese die Smart-Speaker-Nutzung ausführlich reflektierten (Spradley 2016). Der Hausbesuch wurde schließlich in einem Protokoll festgehalten, um den Charakter der Forschungssituation zu konservieren.

In der Auswertung nach den Maßgaben der Grounded Theory wurde das Interviewmaterial transkribiert und anschließend mitsamt der Feldnotizen offen kodiert; im Analyseprozess wurden dabei stetig Memos angelegt. So ergaben sich sukzessive übergeordnete Muster aus dem Material, die anschließend theoretisch perspektiviert wurden (Pentzold u. a. 2018).

5. Kreative Privatisierung

In den Interviews wurde durchgehend das Bewusstsein artikuliert, dass Smart Speaker Daten sammeln. Gleichwohl bestanden graduelle Unterschiede abhängig von der technischen Kompetenz der Gesprächspartner:innen. Es war bekannt, dass Smart Speaker, um reagieren zu können, Sprachdaten verarbeiten und zu diesem Zwecke diese zumindest temporär speichern müssen. Ebenso wurde reflektiert, dass Unternehmen auf diese Daten zurückgreifen, um ihr jeweiliges Angebot zu verbessern, etwa in Bezug auf personalisierte Werbeanzeigen auf Grundlage der jeweiligen Nutzung – dass, abgesehen von den Herstellern wie Google oder Amazon, je nach Anwendung, eine ganze Reihe an Unternehmen auf die erhobenen Daten zugreifen, kam allerdings nicht zur Sprache. Welche Daten dabei konkret gesammelt werden, wie diese ausgewertet werden und welche Konsequenzen das potenziell haben kann, blieb für die Nutzer:innen unklar. Den Umgang von Personen mit diesen Unwägbarkeiten in Bezug auf Privatheit in der Smart-Speaker-Nutzung bezeichne ich im Anschluss an Hans Joas als „kreative Privatisierung". Kreativ meint – wie oben – ein je individuelles Vernetzen von Erfahrungsbeständen, Kompetenzen, Routinen und Bewertungen, das vor dem Hintergrund des jeweiligen Attachments vorgenommen wird.

Im Folgenden werden zwei verschiedene Arten des in diesem Sinne kreativen Umgangs mit dem diffusen Gefühl potenziell bedrohter Privatheit vorgestellt:

- Vertrauen: Aufgrund der Komplexität technischer Zusammenhänge, der Unmöglichkeit, das konkrete Vorgehen der datenerhebenden Unternehmen zu eruieren und der Schwierigkeit, das in der Zukunft liegende Risiko einzuschätzen, rekurrieren Befragte auf eine Praxis des Vertrauens im Sinne einer Schließung kontingenter Zusammenhänge.
- Analogisierung: Die Unsicherheit in Bezug auf das Maß der Privatheitsbedrohung führt zu einem Rückgriff auf Strategien der Analogisierung, die Sicherheit versprechen, indem sie einen scheinbar vordigitalen Zustand herbeiführen.

5.1 Blindes Vertrauen?

Für Niklas Luhmann ist Vertrauen ein Schließungsmechanismus für kontingente Zusammenhänge – die Welt habe sich „zu unkontrollierbarer

Komplexität auseinandergezogen“ (Luhmann 2000, S. 27) und die Entscheidung, zu vertrauen, mache ein Handeln im „hier und jetzt“ möglich (ebd., S. 28). Außerdem gehe „Vertrauen stufenlos in Kontinuitätserwartungen über“ (ebd., S. 29). Damit ist gemeint, dass in der Entscheidung, zu vertrauen, zugleich die Erwartung angelegt ist, dass sich die Dinge nicht unvorhergesehen entwickeln – der schlimmste anzunehmende Fall ist nicht maßgeblich für diese Entscheidung. Damit erschließe Vertrauen „Handlungsmöglichkeiten, die ohne [es] unwahrscheinlich und unattraktiv geblieben, also nicht zum Zuge gekommen wären“ (ebd., S. 30). Insofern mische sich im Terminus des Vertrauens „Wissen und Nicht-Wissen“ (ebd., S.31). Dies bezieht sich auf Situationen, in denen Unsicherheit herrscht und etwas auf dem Spiel steht; die Art des Vertrauens beschreibt den spezifischen Umgang mit diesen. Insofern ist Vertrauen als „Lösung für spezifische Risikoprobleme“ zu verstehen (Luhmann 2001, S. 144).

Den Studienteilnehmer:innen ist bewusst, dass sie häufig zum einen nicht über die nötigen Informationen oder Fertigkeiten verfügen, die sie bräuchten, um potenzielle Gefährdungen für sie abzuschätzen, und zum anderen die Motivation derer, die Daten sammeln, nicht grundsätzlich bewerten können, ohne eine komplizierte systemkritische Perspektive einzunehmen. Sie fangen entsprechend an, auf verschiedene Weise zu vertrauen. Anhand empirischer Beispiele zeige ich im Folgenden, in welcher Form dieses Vertrauen vor dem Hintergrund spezifischer Attachments an Gestalt gewinnt und sich etwa als Vertrauen in 1) Bezug auf Staatlichkeit, 2) die beteiligten Unternehmen, oder 3) als ‚Trade-Off‘ zeigt.

Zunächst berichte ich dafür aus einem Videointerview mit einer Personalerin, wohnhaft im ländlichen Bereich Sachsens. Sie wohnt mit ihrem Partner in einem Neubau, der von Grund auf ‚smart‘ gestaltet ist. Entsprechend besitzen sie auch mehrere Smart Speaker in verschiedenen Ausführungen. Im Gespräch über potenzielle Bedrohungen von Privatheit durch Alexa, schildert sie mir, wieso sie sich dahingehend eigentlich keine Sorgen mache:

> „Da ist man ja in Deutschland, glaub ich, gut aufgehoben (lacht) was das Thema angeht, aber ich glaube, da macht man sich, wenn man [woanders] wohnen würde, anders Gedanken drüber, ja, durchaus, aber ich glaub, in Deutschland muss man sich da keine Gedanken machen und deswegen hab‘ ich mir da ehrlich gesagt auch noch nicht so viele Gedanken drüber gemacht, dass das da irgendwelche persönlichen Nachteile haben könnte…“ (Ausschnitt Transkript 4)

Die angerufene Instanz, der Vertrauen geschenkt wird, ist hier also der deutsche Staat. Zunächst wird darauf verwiesen, dass Deutschland in Privatheitsfragen im internationalen Vergleich eine Sonderstellung habe. Dies könnte sich auf spezifische gesetzliche Regelungen beziehen oder ganz allgemein auf den rechtstaatlichen Charakter; vermutlich ist (so ließe das Lachen schließen) aber auch insgesamt eine gewisse Regelungswut, die als ‚typisch deutsch' markiert wird, angesprochen. Anschließend verweist sie darauf, dass sie sich damit grundsätzlich nicht viel beschäftigt habe. Hier kommt ein spezifisches Attachment zum Ausdruck, das in der Gewohnheit besteht, innerhalb eines gesetzlich verfassten Rahmens bislang keine Willkür erfahren zu haben. Dies bildet den Erfahrungshintergrund der Person, von dem aus sie die Entscheidung, zu vertrauen, reflektiert. Hier kommt idealtypisch zum Ausdruck, was Luhmann mit Kontinuitätserwartung des Vertrauens beschrieben hat – da sich diese Einstellung bisher bewährt habe, bestehe keine Notwendigkeit für eine kritischere Reflexion.

Im nächsten Beispiel ist nicht die Staatlichkeit Adressat des Vertrauens, sondern die Unternehmen, die Smart Speaker im Portfolio haben. Ich unterhalte mich mit einem jungen Familienvater, der als Ingenieur eine gewisse technische Grundaffinität aufweist. In Privatheitsfragen macht er sich ebenso keine Gedanken und begründet dies so:

> „Jaaa, ein gewisses Vertrauen muss man sowieso in die Hersteller haben, weil, natürlich ist da Missbrauch, na was heißt Tür und Tor geöffnet, die Frage ist, was können die denn damit anfangen? Das müsste ja dann irgendein Hacker sein, der einen dann damit erpresst oder so. [....] Das ist halt das Risiko, das wir eingehen, aber ich hab jetzt nicht irgendwie Bedenken, dass also Google oder Amazon oder Apple jetzt irgendwie die Daten gegen einen verwenden. Also, die werden sicher Target-Werbung machen oder so, ok. […] Es ist mir bewusst, ja, es ist halt Aufwand und Nutzen. Oder: Nutzen und Gegenwert. Sozusagen." (Ausschnitt Transkript 8)

Hier wird direkt ein Vertrauen in die Hersteller angesprochen: Zunächst wird ein kritisches Bewusstsein markiert: Die Tatsache, dass Daten gesammelt werden, sei grundsätzlich problematisch. Sogleich wird aber differenziert: Im Grunde bestehe nur ein Problem, wenn Dritte auf die Daten zugreifen könnten, von den Unternehmen an sich gehe keine Gefahr aus (freilich ließe sich einwenden, dass auch Unternehmen als Dritte gelten müssten, ein Umstand, der vom Gesprächspartner aber nicht angeführt wird). Dahingehend präzisiert der Studienteilnehmer an anderer Stelle im

Interview, dass die Unternehmen ja in staatliche Regelungszusammenhänge eingebunden seien und insofern bei Zuwiderhandlung verklagt würden – über Umwege ist also auch hier die Staatlichkeit Adressat des Vertrauens. Dass Unternehmen die Daten allerdings kapitalisieren, wird nicht kritisch gesehen, sondern vielmehr als ‚Trade-Off' markiert. Gleichwohl wird in der kurzen Passage deutlich, dass das ‚Risiko' nicht vollends überschaut werden kann; dennoch werden Begründungsfiguren in Anschlag gebracht, die als Ausdruck eines spezifischen Attachments gelesen werden können: Die Verbindung von Problembewusstsein, technischer Argumentation und Zustimmung zum Geschäftsmodell als individueller Perspektive meines Gesprächspartners kennzeichnen diese konkrete Form des Vertrauens.

Das Motiv des ‚Trade-Offs', das bereits im vorangegangenen Beispiel zutage trat, findet sich differenzierter im nächsten Interviewausschnitt. Im Gespräch mit einer jungen Akademikerin kommen wir ebenso auf Privatheitsfragen zu sprechen und sie äußert eine dezidierte Meinung:

> „Es ist ja eigentlich scheißegal, ob du jetzt Alexa hast oder nicht, deine Daten werden so oder so abgezogen, es sei denn wahrscheinlich, du hast noch ein altes Nokia und keinerlei Social Media Account, aber auch dann nimmst du dich ja quasi aus dem gesellschaftlichen Leben raus. Grad in [meinem] Alter jetzt, das ist halt…ja, im Endeffekt kann man zwar immer sagen, wir haben eine freie Wahl, aber im Endeffekt, wenn du auch partizipieren willst, hast du keine ganz freie Wahl, würde ich sagen, ist es nicht. Weil du…im Endeffekt hast du einfach nur die Entscheidung zwischen: Ich gebe vielleicht auch nur einen Teil meiner Daten ab oder ich exkludier mich halt sozial total. Das hat jetzt nichts mit Alexa zu tun, weil Alexa braucht man nicht, um sozial teilhaben zu müssen, aber ich glaub, dass da die Hemmschwelle auch einfach ist, ja, jetzt hast du deine Daten…also wie gesagt es haben schon zwei Großkonzerne meine Daten, tut dann wirklich weh, wenn die ein dritter auch noch hat?" (Ausschnitt Transkript 7)

In diesem Exzerpt wird eine Fülle an Begründungen in Anschlag gebracht, die alle in ein Motiv sozialen Anschlusses münden; die Befragte abstrahiert vom Thema Smart Speaker und macht generell zum Thema, dass der Verzicht auf Teilhabe an (technischer) Innovation in die soziale Isolation führe. Sie habe dahingehend nicht einmal „freie Wahl" – sie tauscht also imaginär das Risiko potenziellen Datenmissbrauchs gegen die Möglichkeit, an Gesellschaft teilzunehmen. Diese Risikobereitschaft charakterisiert die Haltung der Gesprächspartner:in als Vertrauen in Abgrenzung zu reiner

Zuversicht. Die komplexe Struktur der Gegenwart, in der die Differenzierung sozialer Sphären durch die übergreifende Datensammlung gleichsam technisch aufgehoben wird, führt weiterhin zu der Argumentation, dass ein selektives kritisches Bewusstsein ohnehin nicht zielführend sei. Entsprechend führt sie an, dass ihre Daten ohnehin in der Welt seien und sich also in dieser Sache eine Sensibilität in Privatheitsfragen schlicht nicht lohne. Hier kommt das Attachment in doppelter Hinsicht zum Tragen: Einerseits bildet die – auch generationstypische – selbstverständliche Einbindung in gesellschaftlichen Fortschritt (Smartphone, Social Media) den Hintergrund der Entscheidung, an einen lohnenden Trade-Off als Grundlage des Vertrauens zu glauben. Andererseits ist auch hier, wie bereits oben ausgeführt, die Kontinuitätserwartung Teil der Erwägung – man sei das Risiko ja in der Vergangenheit bereits eingegangen, da könne ein weiteres Mal ja nicht schaden. Das Vertrauen als Schließungsmechanismus wird dabei argumentativ von einer fatalistischen Perspektive grundiert, die man durchaus als zynisch verstehen kann (Hoffmann u. a. 2016; Lutz/Newman 2021). Während sich in den vorangegangenen Beispielen das Vertrauen also auf konkrete Akteure, nämlich den Staat oder Unternehmen bezieht, wird hier darin vertraut, dass sich der Trade-off auszahlt: Einerseits durch soziale Teilhabe, die durch die freiwillige Abgabe von Daten durch Nutzung spezieller Technologien ermöglicht werde, anderseits, indem sich potenzielle Bedrohungen schlichtweg nicht realisieren.

Vertrauen darauf, dass die Smart Speaker-Nutzung über den Abfluss von Daten nicht zum eigenen Nachteil wird, ist ein zentrales Motiv in der Antwort auf die Frage, wie Menschen mit der potenziellen Bedrohung ihrer Privatheit umgehen. Dabei hat dieser Abschnitt verdeutlicht, welch unterschiedliche Gestalt dieses Vertrauen vor dem Hintergrund verschiedener Attachments annehmen kann. Diesem Vertrauen gehen, wie von Luhmann ausgeführt, verschiedene Reflexionen voran, die dem jeweiligen Vertrauen ihren individuellen Charakter verleihen und sind gewissermaßen als Rückversicherungen zu verstehen, die dem jeweiligen Umgang mit Privatheitsbedrohungen durch Smart Speaker begleiten. Welche Reflexionen vorgenommen werden, ist dabei von Person zu Person verschieden und gründet in der jeweiligen Verhaftung in Gewohnheiten, Diskursen und Überzeugungen. Die Reflexionen sind dabei durchaus widersprüchlich strukturiert und nur bedingt geeignet, das Vertrauen angemessen zu begründen, etwa wenn in Zeiten globaler Informationsflüsse die Hoffnung auf den Staat als Kontrollgewalt angeführt wird. Die angeführten Begründungen für das Vertrauen spiegeln entsprechend eher die individuelle dis-

kursive Verhaftung der Person wider als eine objektiv-rationale Abwägung. Insofern ist Vertrauen aus pragmatistischer Perspektive als Teil einer individuellen Praxis im Sinne einer erfahrungsgeleiteten Auseinandersetzung zu verstehen, die in ganz verschiedenen und meist widersprüchlichen – weil eben das persönliche Attachment und nicht eine objektiv-rationale Auseinandersetzung widerspiegelnden – Begründungsfiguren mündet.

5.2 Analogisierung

Ebenso wie das Vertrauen eine Möglichkeit darstellt, Unsicherheit und Nicht-Wissen bearbeiten zu können und Handlungsfähigkeit zu ermöglichen, gilt dies auch für die im Folgenden beschriebenen Strategien der Analogisierung. Helen Nissenbaum hat bereits herausgearbeitet, dass Privatheit keinen statischen Wert darstellt, sondern je nach Kontext eigene Erfordernisse des Abschlusses oder der Öffnung nötig sind (Nissenbaum 2010). Ebenso ist auch das Zuhause als Privatraum nicht durchgehend gleich strukturiert. Vielmehr können auch innerhalb eines Haushaltes verschiedene Kontexte nebeneinander existieren, die unterschiedlichen Umgang mit potenziellen Privatheitsbedrohungen nötig machen. Um dem Umstand zu begegnen, dass Smart Speaker potenziell auch ungewollt sowie trotz etwaiger Einstellungen Daten aufzeichnen, berichten Befragte, dass sie in besonderen Fällen einen räumlichen Kontext zu schaffen bestrebt sind, der ihnen sicher erscheint. Entsprechend berichten zahlreiche Gesprächspartner:innen umgekehrt, dass sie ungern einen Smart Speaker im Bade- oder Schlafzimmer aufstellen. So berichtet meine Gesprächspartnerin:

> „Naja, die zeichnet ja auch auf, die speichert, was machst du in deinem Schlafzimmer? Wie gesagt, ich hab da tatsächlich auch öfter nachgedacht, ich hab das dann alles ausgestellt, die speichert ja nichts, aber da ist auch wieder die Frage, wie sehr glaubst du dem…aber dann ist auch wieder die Frage, gut, was hörst du da? [Im Zweifel] schieb ich's einfach auf meine Schwester (lacht) die klingt genauso wie ich (lacht) […] es ist ja auch noch was anderes, wenn's deine Küche ist oder dein Schlafzimmer. Das ist ja doch nochmal vielleicht ne andere Ebene." (Ausschnitt Transkript 7)

Auch hier wird also darauf verwiesen, dass das Zuhause in Bezug auf die Anforderungen an Privatheit unterschiedlich kartiert ist. In diesem Fall hat

sich die Person für eine Alexa im Schlafzimmer entschieden, aber offenbar ausführlich reflektiert, wie sie im Falle eines Datenmissbrauchs reagieren würde, wenngleich sie die Aussage in einen Scherz kleidet; es bleibt dennoch zu bezweifeln, dass eine akustische Ähnlichkeit der Stimmen zu einer tatsächlichen ‚Obfuscation'[4] führt, also der Unmöglichkeit einer Personalisierung durch Verschleierung. Welche konkreten Folgen ein Abhören des Schlafzimmers haben könnte, wird nicht ausgeführt, jedoch scheint hier Scham eine Rolle zu spielen. Diese Scham speist sich aus Erfahrungen im Analogen – der Smart Speaker wird gewissermaßen vermenschlicht, indem er behandelt wird wie ein potenzieller Stalker. Dies sagt wenig aus über die tatsächliche potenzielle Verwendung von Sprachdaten, verdeutlicht aber, dass das Analoge als Blaupause der Erfahrung die Referenz für die Einschätzung von Privatheitsbedrohungen bildet.

Analogisierung ist ein häufig gewähltes Mittel für die Bearbeitung von potenziellen Privatheitsbedrohungen. Die Grundlage dafür kann freilich stark differieren. So berichtet mir im nächsten Interviewausschnitt ein Gesprächspartner, dass er gelegentlich Themen bespreche, die sich am Rande der Legalität bewegten:

> „Aber…nee, z. B. Kontonummern et cetera, ne? Sowas ist dort nicht hinterlegt und sowas kriegen die dort auch nicht raus, und sowas nenn ich auch nicht, indem ich sage, Alexa hier ist meine Kontonummer, ne? […] In diesem Raum ist das völlig ok, da kann man frei sprechen. Wenn, dann drück ich auf's Mikro, wenn's hier mal um Dinge geht, die…das mach ich auch." (Ausschnitt Transkript 5)

Zunächst definiert mein Gesprächspartner Informationen, die er nicht teilen würde; dies betrifft – wenig überraschend – Finanzdaten. Dabei ist aufschlussreich, dass er es laut Aussage vermeidet, seine Kontonummer in der Nähe der Smart Speaker laut auszusprechen; er behandelt den Smart Speaker entsprechend wie eine dritte Partei und sensible Daten in seinem Wohnraum wie ein Geheimnis. Zwar ist nicht klar, ob die Informationen zum eigenen Nachteil eingesetzt werden können, aber die bewährte Praxis

4 Der Begriff der *Obfuscation* bezeichnet eine Verschleierungstaktik, die sich die Eigenheiten digitaler Technik zu eigen macht. In ihrem gleichnamigen Buch geben die Autor:innen Nutzer:innen eine Handreichung, ihre digitalen Spuren durch bestimmte Praktiken vor Missbrauch zu schützen (Nissenbaum/Brunton 2016). Die Verschleierung der eigenen Informationen als spezifischen Umgang mit Fragen der informationellen Selbstbestimmung als Subjektivierungsangebot des 21. Jahrhunderts beschreibt Carsten Ochs als *blurry self* (Ochs 2022, S. 435f.).

des Verheimlichens wird nichtsdestotrotz angewandt. Anschließend kommt er auf Situationen zu sprechen, in denen er den Smart Speaker ausschalten würde: „[W]enn's hier mal um Dinge geht" bezieht sich auf, so wird an anderer Stelle deutlich, Gespräche über Drogenkonsum. Hier öffnet sich also ein Graben, der mit Vertrauen nicht überbrückt werden kann und der eine Handlung nötig macht, die dieses Unsicherheitsgefühl bearbeitet. Dabei bleibt unklar, ob den Mikrofonschalter zu drücken geeignet ist, die räumliche Integrität wiederherzustellen. Ein anderer Gesprächspartner bemerkt auf meine Frage hin, ob er ab und an das Mikrofon stumm schalte, entsprechend: „Wenn ich [mit dem Abhören in bestimmten Situationen] ein Problem hätte, dann würde ich wahrscheinlich eher den WLAN-Stecker, also den Rooterstecker ziehen." (Ausschnitt Transkript 7). Hier zeigt sich also eine weitergehende Praxis der Analogisierung. Man könnte konstatieren, dass im ersten Fall ein Vertrauen in das Versprechen der Anbieter, die Aufzeichnung über die Mikrofontaste kontrollieren zu können, besteht, das im zweiten Fall als Teil des Risikos minimiert werden soll. Dennoch ist das Ziel, nämlich das Herstellen eines analogen Zustandes identisch; die Wahl der Mittel differiert mit unterschiedlichem Attachment, das sich hier in einer spezifischen Risikoabwägung äußert.

Abschließend berichte ich von einem Gesprächspartner, der ebenfalls in einer ländlichen Region beheimatet ist. Er ist Pendler und daher unter der Woche viel unterwegs; in Bezug auf Smart Speaker ist er äußerst bewandert und programmiert sogar eigene ‚Skills', also Anwendungen für den Smart Speaker; so beispielsweise auch ein elektronisches Türschloss, das sich auf einen Sprachbefehl hin öffnet. Gefragt, ob das für ihn nicht ein Risiko darstelle, kontert er mit dieser launigen Erklärung:

> „Ich wohn hier […] im Dorf, und es sind so viele alte Leute hier bei mir rundrum – wir sind, glaube ich, mit die Jüngsten – die sind den ganzen Tag daheim. Also, ich brauch eigentlich auch gar keine Alarmanlage. Weil, wenn ich Besuch bekomme, dann wissen die das auf jeden Fall, und wenn meine Partnerin nicht da ist, dann weiß auf jeden Fall meine Partnerin spätestens einen halben Tag später, dass hier Besuch da war. Und so ist's auch andersrum. Wenn für sie Besuch da ist, und ich bin nicht da, und ich komm das Wochenende heim, dann hab' ich garantiert einen halben Tag später die Information, wer hier in der Woche alles ein- und ausgegangen ist. Das funktioniert ganz gut bei uns (lacht)." (Ausschnitt Transkript 1)

Auf ein potenzielles Risiko durch die Programmierung des Türschlosses über den Smart Speaker wird hier gar nicht dezidiert eingegangen. Vielmehr wird mit der Eigenheit des Sozialraumes eines kleinen Dorfes argumentiert: Die nachgerade panoptischen Zustände machen einen Missbrauch der Technologie unwahrscheinlich. Es wird auf einen Raum verwiesen, der übersichtlich und vorhersehbar strukturiert ist. Daher ist auch nachrangig, ob diese Beschreibung tatsächlich den Hintergrund für die Risikoeinschätzung bildet. Vielmehr ist der Verweis auf analoge Prinzipien, die das Sozialleben in diesem Dorf kennzeichnen, zentral. Die Potenzialität eines Missbrauchs der Smart Speaker-Technologie wird verhandelt, aber entkräftet durch den Verweis auf etablierte analoge Praktiken der Beobachtung und mündlichen Kommunikation. Bemerkenswerterweise wird hier, in humoristischer Weise und provokanter Zuspitzung, die Bereitschaft angezeigt, sich überwachen zu lassen. Wenn sie der eigenen Sicherheit zuträglich ist, sei eine – hier beinahe fürsorgliche – Überwachung durchaus wünschenswert.

Das Analoge bildet also einerseits den Ausgangspunkt der Einschätzung der Privatheitsbedrohung durch den Smart Speaker wie den Fluchtpunkt der Versicherung. Im Analogen haben Menschen gelernt, Privatheitsbedrohungen zu moderieren; durchgehend muss in verschiedenen Kontexten und sozialen Konstellationen das Verhältnis von Offenbarung und Verheimlichung austariert werden. Im Kontakt mit dem Smart Speaker löst sich diese Gewissheit auf, weil die Kriterien der Einschätzung verschwimmen; es bedeutet einen immensen Aufwand, eine gewissenhafte Prüfung der tatsächlichen Bedrohung vorzunehmen, und zugleich verbleibt vieles im Unklaren und kann nicht abschließend eingeschätzt werden.[5] Es zeigt sich außerdem in diesem Zusammenhang, dass Dimensionen der Privatheit , wie von Beate Rössler erarbeitet (lokal, informationell, dezisional) zwar theoretisch unterscheidbar, allerdings empirisch miteineinander verzahnt sind – die Entscheidung über den Informationsfluss etwa ist stets

5 So macht beispielsweise das BSI (Bundesamt für Sicherheit in der Informationstechnik) acht Empfehlungen, um die eigene Privatsphäre vor potenziellen Übergriffen via Smart Speaker zu schützen: 1. Separates WLAN einrichten; 2. Smart Speaker mit Bedacht platzieren; 3. Personalisierte Sprachprofile; 4. Passwortsicherung; 5. Datenschutzeinstellungen anpassen; 6. Gespeicherte Daten kontrollieren; 7. Nur vertrauenswürdige (sic!) Erweiterungen installieren; 8. Smart Speaker abschalten, vgl.: https://social.bund.de/@bsi/112002894812746815 (zuletzt aufgerufen am 28.2.2024). Diese Maßnahmen benötigen einigen Aufwand oder Technikkompetenz; bemerkenswerterweise werden auch hier Techniken der Analogisierung empfohlen (Nr. 2 und 8).

lokal gebunden und macht eine Umsetzung in einem konkreten materiellen Arrangement nötig.

Das Analoge, als primäre Referenz persönlicher Erfahrung – kondensiert im Attachment – bildet den Hintergrund der Einschätzung unüberschaubarer Zusammenhänge. Zugleich ist die Überführung in das Analoge, etwa durch das Ziehen des Steckers, eine Strategie, einen kontrollierbaren Raum zu schaffen, und mithin das Mittel, Sicherheit zu schaffen in Situationen, in denen Vertrauen keine Option ist. Dabei wirkt die Analogisierung auf eine denkwürdige Weise unzeitgemäß und spiegelt gewissermaßen eine Überforderung angesichts der rasanten digitalen Transformation. Kreativ sind diese Formen der Privatisierung in pragmatistischem Sinne allemal, als sie eine individuelle und erfahrungsgeleitete Auseinandersetzung beschreiben; dem Anspruch, tatsächlichen Privatheitsbedrohungen angemessen zu begegnen, werden sie dabei jedoch nicht gerecht. Das Attachment als Theorieangebot ist geeignet, zu erklären, wieso Personen auf diese Strategien zurückgreifen – in der Empirie tritt die Verhaftung der Gesprächspartner:innen in analogen Zusammenhängen deutlich zu Tage und bildet den Hintergrund der jeweiligen Formen der Privatisierung. Dies verweist jedoch zugleich auf eine übergeordnete Problematik: Die Komplexität der datenökonomischen Infrastrukturen im Kontext der digitalen Transformation führt zu einer Hilflosigkeit, die entweder nur durch Vertrauen – begleitet von spezifischen Rationalisierungen und gelegentlich garniert mit Fatalismus und Zynismus – oder durch gleichsam antiquierte Strategien der Analogisierung, die höchstens situativ Sicherheit verschaffen, aufgelöst werden kann.

6. Fazit

Dieser Beitrag hat gezeigt, dass Menschen potenzielle Privatheitsbedrohungen durch Smart Speaker vor dem Hintergrund eines spezifischen Attachments vornehmen. Wie Menschen sich dieser Bedrohungen bewusst sind, wie sie ein potenzielles Risiko bewerten und welche Schritte sie zur Wahrung ihrer Privatheit unternehmen, ist dabei von Person zu Person verschieden und als erfahrungsgeleitete Auseinandersetzung zu verstehen. Das Attachment prägt dabei einen bestimmten Umgang mit Privatheitheitsansprüchen vor; das betrifft Routinen der Selbstinformation zur Bearbeitung von Unsicherheit oder die Verarbeitung von potenziellem Risiko ebenso wie konkrete Schritte der Privatisierung. Menschen behandeln Fragen der

Privatheit in der Smart Speaker-Nutzung mit den Mitteln, die sie für geeignet halten und die ihnen als Bearbeitungsmodi vertraut sind. Dabei wurde gezeigt, dass diese Bearbeitungen in bestimmten Formen des Vertrauens sowie der Analogisierung münden; diese weisen insofern Ähnlichkeit auf, indem sie in unterschiedlicher Intensität Risiko bearbeiten. Freilich sind sie i. d. R. nicht geeignet, ein Risiko tatsächlich aufzulösen: Ob Vertrauen sich gelohnt hat, ist allein im Nachhinein zu beurteilen, und auch, ob Analogisierung zum Schutz der Privatheit geeignet ist, bleibt zumindest fraglich. Dass Menschen trotz ausgestellter Sensibilität keine umfassenden Maßnahmen zum Schutz ihrer Privatheit ergreifen oder diese sich nicht eignen, das Risiko auszuschließen, ist, soviel ist deutlich geworden, zwar als widersprüchliches, allerdings nicht zielführend als paradoxes Verhalten zu bezeichnen. Die jeweilige Form des Vertrauens oder der Analogisierung und die entsprechende argumentative Manifestation gründet vielmehr in einem spezifischen Attachment, das Ausdruck der jeweiligen Erfahrungsbestände der Person ist.

Eine pragmatistische Perspektive legt nahe, dass sich mögliche Inkonsistenzen nicht zuletzt aus der fehlenden Widerständigkeit des digitalisierten Umfelds ergeben – abgesehen etwa von personalisierter Werbung bleibt das Potential vollkommen unbestimmt, in welchem Maße Datensammlung auf die Lebenswirklichkeit der Nutzer:innen zurückwirkt. Das Risiko ist schlichtweg nicht greifbar, da mögliche Konsequenzen nur in den seltensten Fällen auftreten, sondern i. d. R. Gegenstand fiktiver Gedankenspiele bleiben. Es besteht daher kaum eine Veranlassung, Privatisierung als Anspruch ernstzunehmen und entschiedene Maßnahmen zur Privatisierung im Alltag zu ergreifen. Insofern verweist das vermeintliche Paradoxon eines nachlässigen Umgangs mit Privatheitsbedrohungen durch den Smart Speaker, bei gleichzeitigem Bewusstsein über die Datenaneignung durch privatwirtschaftliche Akteure, auf konkrete Defizite: Die unzureichende Kenntnis in Bezug auf technische Zusammenhänge und die Verwertungsketten in einer globalen Datenökonomie und damit einhergehenden Risiken. Diese Umstände machen deutlich, dass die digitale Transformation in einem Tempo von Statten geht, das es schwerlich möglich macht, in Privatheitsfragen aufgrund eigener Erfahrungsbestände angemessen zu agieren; insofern stellen Konzepte wie informationelle Selbstbestimmung Nutzer:innen häufig vor kaum zu lösende Aufgaben – eine Erkenntnis, die als Aufforderung für systemische Lösungen dieser Fragen auf rechtlicher Ebene ebenso wie für verstärkte, institutionell verankerte und gesamtgesellschaftlich angelegte Aufklärungsarbeit verstanden werden muss.

Literaturverzeichnis

Agi, Benjamin und Jullien, Nicolas (2018): Is the Privacy Paradox in Fact Rational? doi: http://dx.doi.org/10.2139/ssrn.3109695.

Acquisti, Alessandro und Grossklags, Jens (2005): Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy,* 3(1). doi: http://doi.org/10.1109/MSP.2005.22.

Arendt, Hannah (2002): *Vita activa oder Vom tätigem Leben*. München: Piper.

Barnes, Susan (2006): A privacy paradox: Social networking in the United States. *First Monday* 1. URL: https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312.

Bhatt, Jiten Jwalant (2019): I Think I Can Trust Alexa, But How Much? *Intersect* 13 (1). URL: https://ojs.stanford.edu/ojs/index.php/intersect/article/view/1410.

Brause, Saba R. und Blank, Grant (2020): Externalized Domestication: Smart Speaker Assistants, Networks and Domestication Theory. *Information, Communication & Society,* 23 (5), S. 751–63. doi: https://doi.org/10.1080/1369118X.2020.1713845.

Brause, Saba R. und Blank, Grant (2024): 'There Are Some Things That I Would Never Ask Alexa' – Privacy Work, Contextual Integrity, and Smart Speaker Assistants. *Information, Communication & Society,* 27 (1), S. 182–97. doi: https://doi.org/10.1080/1369118X.2023.2193241.

Buteau, Emily und Lee, Joonghwa (2021): Hey Alexa, Why Do We Use Voice Assistants? The Driving Factors of Voice Assistant Technology Use. *Communication Research Reports,* 38 (5), S. 336–45. doi: https://doi.org/10.1080/08824096.2021.1980380.

Cho, Eugene, S. Shyam Sundar, Saeed Abdullah, und Nasim Motalebi. 2020. „Will Deleting History Make Alexa More Trustworthy? Effects of Privacy and Content Customization on User Experience of Smart Speakers". *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, S. 1–13. doi: https://doi.org/10.1145/3313831.3376551.

Endress, Martin (2003): *Vertrauen*. Bielefeld: transcript.

Gautam, Sanjana (2022): In Alexa, We Trust. Or Do We?: An Analysis of People's Perception of Privacy Policies. arXiv. URL: http://arxiv.org/abs/2209.00086.

Gomart, Emilie und Hennion, Antoine (1999): A Sociology of Attachment: Music Amateurs, Drug Users. *The Sociological Review,* 47(1), S. 220-247. doi: https://doi.org/10.1111/j.1467-954X.1999.tb03490.

Habermas, Jürgen (1990): *Strukturwandel der Öffentlichkeit*. Frankfurt: Suhrkamp.

Hennion, Antoine (2011): „Offene Objekte, Offene Subjekte? Körper und Dinge im Geflecht von Anhänglichkeit, Zuneigung und Verbundenheit." *Zeitschrift für Medien- und Kulturforschung,* 2 (1), S. 93–110.

Hennion, Antoine (2017): From Valuation to Instauration: On the Double Pluralism of Values. *Valuation Studies*, 5 (1), S. 69–81.

Hine, Christine (2020): Strategies for Reflexive Ethnography in the Smart Home: Autoethnography of Silence and Emotion. *Sociology,* 54 (1), S. 22-36. doi: https://doi.org/10.1177/0038038519855325

Hoffmann, Christian Pieter; Lutz, Christoph und Ranzini, Giulia (2016): Privacy Cynicism: A New Approach to the Privacy Paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4). doi: http://dx.doi.org/10.2139/ssrn.3319830.

James, William (1994): *Was ist Pragmatismus?* Weinheim: Beltz.

James, William (2006): *Pragmatismus und radikaler Empirismus*. Frankfurt: Suhrkamp.

Joas, Hans (1996): *Die Kreativität des Handelns*. Frankfurt: Suhrkamp.

Kang, Hyunjin und Oh, Jeeyun (2023): Communication Privacy Management for Smart Speaker Use: Integrating the Role of Privacy Self-Efficacy and the Multidimensional View. *New Media & Society* 25 (5), S. 1153–75. doi: https://doi.org/10.1177/14614448211026611.

Kröger, Jacob Leon; Gellrich, Leon; Pape, Sebastian; Brause, Saba R. und Stefan Ullrich (2022): Personal Information Inference from Voice Recordings: User Awareness and Privacy Concerns. *Proceedings on Privacy Enhancing Technologies,* 2022 (1), S. 6–27. doi: https://doi.org/10.2478/popets-2022-0002.

Lamla, Jörn (2019): Selbstbestimmung und Verbraucherschutz in der Datenökonomie. *Aus Politik und Zeitgeschichte,* 69 (24-26).

Lamla, Jörn; Büttner, Barbara; Ochs, Carsten; Pittroff, Fabian; Uhlmann, Markus (2022): Privatheit und Digitalität. Zur soziotechnischen Transformation des selbstbestimmten Lebens. In: Roßnagel, Alexander und Friedewald, Michael (Hrsg.): *Die Zukunft von Privatheit und Selbstbestimmung*. Wiesbaden: Springer, S.125-158.

Lau, Josephine; Zimmermann, Benjamin und Schaub, Florian (2018a): Alexa, Stop Recording: Mismatches between Smart Speaker Privacy Controls and User Needs. Poster presented at the *14th Symposium on Usable Privacy and Security (SOUPS 2018)*. URL: https://www.usenix.org/sites/default/files/soups2018posters-lau.pdf.

Lau, Josephine; Zimmermann, Benjamin und Schaub, Florian (2018b): Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction* 2 (CSCW), S. 1–31. doi: https://doi.org/10.1145/3274371.

Luhmann, Niklas (2000): *Vertrauen*. Stuttgart: Lucius&Lucius.

Luhmann, Niklas (2001): Vertrautheit, Zuversicht, Vertrauen. Probleme und Alternativen. In: Hartmann, Martin und Offe, Claus (Hrsg.): *Vertrauen. Die Grundlage sozialen Zusammenhalts*. Frankfurt: Campus.

Lutz, Christoph und Newlands, Gemma (2021): Privacy and smart speakers: A multi-dimensional approach. *The Information Society,* 37(3), S. 147-162. doi: 10.1080/01972243.2021.1897914.

Malodia, Suresh; Islam, Nazrul; Kaur, Puneet und Dhir, Amandeep (2024): Why Do People Use Artificial Intelligence (AI)-Enabled Voice Assistants? *IEEE Transactions on Engineering Management 71*, S. 491–505. doi: https://doi.org/10.1109/TEM.2021.3117884.

Malkin, Nathan; Deatrick, Joe; Tong, Allen; Wijesekera, Primal; Egelman, Serge und Wagner, David (2019): Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies,* 2019 (4), S. 250–71. doi: https://doi.org/10.2478/popets-2019-0068.

Mittal, Mehak und Manocha, Sanjay (2022): Alexa! Examine Privacy Perception and Acceptance of Voice-Based Artificial Intelligence among Digital Natives. *Journal of Information and Optimization Sciences,* 43 (7), S. 1679–92. doi: https://doi.org/10.1080/02522667.2022.2134367.

Mols, Anouk; Wang, Yijing und Pridmore, Jason (2022): Household Intelligent Personal Assistants in the Netherlands: Exploring Privacy Concerns around Surveillance, Security, and Platforms. *Convergence: The International Journal of Research into New Media Technologies,* 28 (6), S. 1841–60. doi: https://doi.org/10.1177/13548565211042234.

Nassehi, Armin (2019): *Muster. Theorie der digitalen Gesellschaft*. München: C.H. Beck.

Nissenbaum, Helen (2010): *Privacy in Context*. Stanford: Stanford University Press.

Nissenbaum Helen und Brunton, Finn (2016): *Obfuscation*. Cambridge: MIT Press

Ochs, Carsten (2022): *Soziologie der Privatheit. Informationelle Teilhabebeschränkung vom Reputation Management bis zum Recht auf Unberechenbarkeit*. Weilerswist: Velbrück.

Pentzold, Christian; Bischof, Andreas und Heise, Nele (Hrsg.): *Praxis Grounded Theory: theoriegenerierendes empirisches Forschen in medienbezogenen Lebenswelten: ein Lehr- und Arbeitsbuch. Lehrbuch*. Wiesbaden: Springer VS 2018.

Pridmore, Jason und Mols, Anouk (2020): Personal Choices and Situated Data: Privacy Negotiations and the Acceptance of Household Intelligent Personal Assistants. *Big Data & Society,* 7 (1). doi: https://doi.org/10.1177/2053951719891748.

Roessler, Beate und Mokrosinska, Dorota (2013): Privacy and Social Interaction. *Philosophy and Social Criticism,* 39 (8), S. 771-791.

Rzepka, Christine (2019): Examining the Use of Voice Assistants: A Value-Focused Thinking Approach. *Twenty-fifth Americas Conference on Information Systems*. URL: https://aisel.aisnet.org/amcis2019/human_computer_interact/human_computer_interact/20.

Sennett, Richard (1993): *Verfall und Ende des öffentlichen Lebens. Die Tyrannei der Intimität*. Frankfurt: Fischer.

Solove, Daniel J. (2021): The Myth of the Privacy Paradox. *Washington Law Review,* 1/2021. URL: https://scholarship.law.gwu.edu/faculty_publications/1482/.

Spradley, James (2016): *The Ethnographic Interview*. Long Grove: Waveland.

Trepte, Sabine; Scharkow, Michael und Dienlin, Tobias (2020): The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior*, 104. doi: https://doi.org/10.1016/j.chb.20.

Whitaker, Reg (1999): *Das Ende der Privatheit. Überwachung, Macht und Kontrolle im Informationszeitalter*. München: Kunstmann.

Zeng, Eric; Mare, Shrirang und Roesner, Franziska (2017): End User Security & Privacy Concerns with Smart Homes. *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. URL: https://www.usenix.org/system/files/conference/soups2017/soups2017-zeng.pdf.

Zuboff, Shoshanna (2018): *Das Zeitalter des Überwachungskapitalismus*. Frankfurt/New York: Campus.