Datenautonomie im Smart Home: eine praktische/prototypische Umsetzung

Christopher Ruff, Alexander Orlowski, Andrea Horch

Zusammenfassung

In diesem Paper stellen wir einen Meta-Assistenten - Transparenter Datenautonomie Meta-Assistent (DAMA) - vor, der die informationelle Selbstbestimmung der Nutzer:innen von Smart Home-Systemen erhöht, indem er über Verdatung informiert und (semi-)automatische Kontrollmöglichkeiten gibt.

1. Das Home wird Smart

Smart Home-Geräte ermöglichen die Automatisierung und Fernsteuerung von Haushaltsfunktionen wie Beleuchtung, Heizung und Sicherheitssystemen über vernetzte Technologie. Die Nutzung und Verbreitung von Smart Home-Geräten ist in den letzten Jahren deutlich gestiegen. Nach einer BITKOM-Studie (Moltrecht/Schnaack 2022) ist die Nutzung von Smart Home-Anwendungen in deutschen Haushalten von 26 % im Jahr 2018 stetig auf 43 % im Jahr 2022 angestiegen. Hierbei wird das Smart Home zumeist per Smartphone (85 %) gesteuert. 55 % nutzen jedoch auch Sprachsteuerung, wobei bei 87 % ein stationärer Sprachassistent, wie z. B. Amazon Echo oder Google Home, eingesetzt wird. Die Studie hat zudem ermittelt, dass Smart Home-Geräte in Zimmern mit erhöhtem Bedarf an Privatsphäre, wie z. B. Wohnzimmer (79 %), Schlafzimmer (69 %), Badezimmer (57 %), Arbeitszimmer (49 %) oder Kinderzimmer (24 %), verwendet werden. Dies deckt sich mit einer Studie zur Nutzung von Smart Speakern (Brandt 2020), die von 67 % im Wohnzimmer, von 44 % im Arbeitszimmer, von 43 % im Schlafzimmer und von 35 % im Badezimmer genutzt werden. Daraus ergeben sich hohe Anforderungen an Privatheit und Datenschutz, insbesondere bei der Erhebung und Verarbeitung personenbezogener Daten (Feldmeier u.a. 2022). Diese Anforderungen sind in Deutschland gesetzlich geregelt (Feldmeier u.a. 2022). Bei der Speicherung und Verarbeitung der Daten im Ausland kann sich die rechtliche Lage verkomplizieren. Nach der BIT-

KOM-Studie sind Hemmnisse für den Einsatz von Smart Home-Geräten vor allem die Angst vor Hacker-Angriffen (47 %), die Befürchtung des Missbrauchs der persönlichen Daten (37 %) sowie die Angst um die eigene Privatsphäre (29 %) (Moltrecht/Schnaack 2022). Verstärkt werden diese Bedenken durch Medienberichte über den Zugriff auf Bilder der eigenen Sicherheitskamera durch Dritte (Breithut 2020) oder das Erscheinen von Bildern von Privatpersonen im Internet, die von ihrem Saugroboter erstellt wurden (Hensen 2022).

Betrachtet man die von den aufgeführten Studien ermittelten Hemmnisse für die Nutzung von smarten Geräten, wird klar, dass diese auf fehlende Transparenz der Anbieter bezüglich der Datenerhebung, Datenverarbeitung und Datenspeicherung basieren. Es existieren zwar Ansätze zur Erhöhung der Sicherheit in smarten Umgebungen (BSI 2022), aber keine ausreichenden Regulierungssysteme. Die Erfassung und die Verarbeitung sind daher nicht vollständig unter Kontrolle der Menschen, die Smart Home-Systeme nutzen oder die sich in smarten Umgebungen befinden.

In diesem Kapitel arbeiten wir die Relevanz von Datenautonomie im Smart Home-Kontext heraus und präsentieren eine Möglichkeit für Nutzer:innen, diese zu verbessern. Dazu stellen wir die Ergebnisse des Projekts »Transparenter Datenautonomie Meta-Assistent (DAMA)« vor. DAMA wirkt den o.g. Hemmnissen mit einem Meta-Assistenten für smarte Umgebungen entgegen und will diese möglichst beseitigen. Hierfür reguliert der Meta-Assistent die smarten Geräte oder gar einzelnen Sensoren der Geräte kontextbasiert. Zudem schafft er Transparenz, indem er den Benutzer:innen und auch den Gästen von smarten Umgebungen angeschaltete Geräte, die Sensoren für die Datenerfassung besitzen, anzeigt. Zusätzliche Transparenz schafft der Meta-Assistent durch die Anzeige von Veränderungen, wenn sich beispielsweise der Kontext der smarten Umgebung ändert (z. B. eine Person ist allein in der Umgebung vs. mehrere Personen sind anwesend) und deswegen einzelne Geräte oder Sensoren an- bzw. abgeschaltet werden. Nach der Darstellung der Funktionen und ihrer technischen Umsetzung gehen wir auf verschiedene Szenarien ein, in denen der Meta-Assistent Anwendung finden kann. Darüber hinaus skizzieren wir Ergebnisse aus der Evaluation mit potenziellen Nutzer:innen.

2. Smart Home-Geräte als Herausforderung für die Datenautonomie

Die Wohnung als typischer Nutzungskontext von Smart Home-Geräten genießt eigentlich besonderen Schutz vor Überwachung. So ist in Art. 13 GG verankert, dass „die Wohnung [...] unverletzlich" ist. Durch die Nutzung von Smart Home-Geräten werden nun in diesem Bereich eine Vielzahl an Sensoren eingebaut, die verschiedenste, möglicherweise sensible Daten erheben. So verfügen beispielsweise Sprachassistenten über Mikrofone oder smarte Kühlschränke und Türklingeln über Kameras. Dadurch werden bei der Nutzung Daten und Informationen aufgezeichnet, aber auch viele weitere Meta-Informationen gesammelt, die bei der allgemeinen Nutzung dieser Geräte anfallen (Lutz/Newlands 2021).

Dies erzeugt in mehrerlei Hinsicht Konflikte, denn generell sollte Datenerhebung nur erfolgen, wenn die Nutzer:innen dieser aktiv zustimmen. Nur dann ist die informationelle Selbstbestimmung (Jandt 2016) gegeben, wie sie auch im Volkszählungurteil (BVerfG 1983) festgelegt wurde. Dabei bedeutet informationelle Selbstbestimmung, dass eine Person bewusst und informiert dem Teilen ihrer Daten zustimmen muss. Informiert heißt, dass der Umfang und die Konsequenzen des Datensammelns bekannt sind, und die Nutzer:innen sich auf Basis dieses Wissens explizit dafür entscheiden, diese Daten zweckgebunden zu teilen. Insbesondere das eigene Zuhause sollte dabei als Rückzugsort gelten, in dem ein freies und unbeobachtete Leben garantiert ist. Das untergraben Smart Home-Gegenstände jedoch aus mehreren Gründen, die im Folgenden näher dargestellt werden.

2.1 Allgegenwärtige und kontinuierliche Datenerfassung

Die Erfassung von Daten durch Smart Home-Geräte findet kontinuierlich und unauffällig statt. Insbesondere da die Geräte so gestaltet sind, dass sie mit der Umgebung verschmelzen (Rajkumar u.a, 2010) und eben nicht im Alltag auffallen, unterlaufen sie die bewusste Zustimmung. So kann ein Sprachassistent, wie ein Amazon Echo Dot, in einem Bücherregal stehen und so gerade von Gästen übersehen werden (Marky u.a. 2020). Das Mikrofon darin kann jedoch jederzeit angehen. Dies kann auch passieren, wenn es gar nicht intendiert ist, beispielsweise wenn das Wakeword aus Versehen ausgesprochen wird oder ein ähnliches Wort als Wakeword missinterpretiert wird und zu einer Aktivierung des Mikrofons führt. Doch selbst wenn bekannt ist, dass diese Geräte im Raum sind, ist für die Nut-

zer:innen meist nicht transparent, wann die Geräte Daten erheben und für welche Zwecke (Guhr u.a. 2020; Hern 2019).

2.2 Prädiktive Privatheit

Der Begriff „prädiktive Privatheit" (Mühlhoff 2020) beschreibt das Phänomen, wenn ursprünglich nicht personenbezogene Daten so mit anderen Daten in Kontext gesetzt werden oder vorhergesagt werden können, dass daraus sensible Informationen abgeleitet werden können. Denn selbst wenn bekannt ist, welche Daten übermittelt werden, reicht das nicht unbedingt aus, um eine informierte Entscheidung für eine Zustimmung zu treffen. Zwar ist es offensichtlich, dass Daten, wie zum Beispiel aufgenommene Unterhaltungen, personenbezogen sind. Es gibt jedoch eine Vielzahl an Informationen, die von Smart Home-Geräten gesammelt werden, bei denen dies nicht auf den ersten Blick klar ist, beziehungswiese das Ausmaß der Zustimmung nicht bekannt ist. Dabei können scheinbar unverdächtige Daten detaillierte Rückschlüsse über Personen zulassen, obwohl sie von Sensoren stammen, die auf den ersten Blick harmlos wirken (Kröger 2019). Beispielsweise lassen die Daten von einem CO_2-Sensor mit entsprechenden Vergleichswerten Rückschlüsse zu, ob gerade eine oder mehrere Personen in einem Raum anwesenden sind (ebd.). Dadurch kann ggf. gefolgert werden, dass zu einem bestimmten Zeitpunkt Besucher:innen anwesend waren. Ein weiterer Fall wäre, dass es durch den entsprechenden Abgleich mit Vergleichsgruppen möglich ist, aus den Sehgewohnheiten von Fernsehzuschauer:innen abzuleiten, welcher sozialen Gruppe diese angehören (Ghiglieri u.a. 2016). Welche Daten welche Rückschlüsse zulassen, beziehungsweise in Zukunft zulassen könnten, ist also nicht vorherzusagen.

Der Prozess des Ableitens wird als *inferencing* (Wachter 2018) bezeichnet. Durch gestiegene Rechenleistungen und insbesondere Fortschritte im Bereich künstlicher Intelligenz werden immer mehr Inferenzen möglich. Dementsprechend ist es nicht möglich, zu einem bestimmten Zeitpunkt zu sagen, welche Rückschlüsse aus bestimmten Daten in Zukunft möglich sein werden. Deshalb können Informationen, die zum Zeitpunkt der Zustimmung nicht personenbezogen sind, in Zukunft durch Inferenz zu personenbezogenen Daten werden.

2.3 Deanonymisierung

Die zunehmende Rechenleistung macht es nicht nur möglich, dass aus den Daten Rückschlüsse über Personen gezogen werden, sondern ermöglicht auch, eigentlich anonymisierte Daten wieder so in Kontext zu setzen, dass sie wieder einer Person zugeordnet werden können (Wachter 2018). Selbst wenn also zu einem bestimmten Zeitpunkt Daten anonymisiert weiterverarbeitet werden dürfen, ist es möglich, dass sie zu einem späteren Zeitpunkt doch wieder deanonymisiert werden können.

Durch die in diesem Kapitel beschrieben Faktoren wird das Recht auf informierte Selbstbestimmung mehrfach unterlaufen, sodass eine informierte Einwilligung im Smart Home wiederholt unterlaufen wird, weder für die Bewohner:innen der Wohnung, aber erst recht nicht für mögliche Besucher:innen ist es möglich, informierte Entscheidungen zu treffen. Deshalb ist es notwendig, andere Wege zu finden, zu kontrollieren, wann welche Daten erhoben werden.

3. Meta-Assistent

Aufgrund dieser vielfältigen Problematik haben wir einen Meta-Assistenten entwickelt, der es Smart Home-Nutzer:innen ermöglichen soll, ihre informationelle Selbstbestimmung zu verbessern. Der *transparente Datenautonomie Meta-Assistent* (DAMA) soll die im vorherigen Kapitel beschriebenen Probleme adressieren und eine Hands-on-Lösung bieten, die eine bewusstere Nutzung der Geräte zulässt. Das System ist dabei als Überbrückung gedacht, bis notwendige juristische und technische Regulierung eingreift. Im Nachfolgenden skizzieren wir die Ziele von DAMA und wie wir diese umsetzen.

3.1 Ziele von DAMA

Transparenz

Benutzer:innen von intelligenten Assistenten und Geräten wissen oft nicht genau, ob und wann ihre Daten aufgezeichnet und übertragen werden. Darüber hinaus haben die Hersteller solcher Geräte oft Gründe, dies zu verschleiern, da sie die Daten z. B. für Diagnose- und Werbe-Zwecke

nutzen möchten und um das Benutzer:innen-Verhalten zu studieren. Der Meta-Assistent schafft hier Transparenz für die Benutzer:innen, indem auf verschiedenen Kommunikationskanälen, je nach Wunsch der Benutzer:innen, (z. B. Sprachdurchsage und/oder Anzeige auf einem Smart-TV, Smartphone oder Tablet) darüber aufgeklärt wird, welche smarten Geräte sich in der Umgebung befinden, über welche Sensoren diese verfügen und ob diese an- oder ausgeschaltet sind. Dadurch wird zum einen Aufmerksamkeit darauf gelenkt und der Tendenz smarter Geräte entgegengewirkt, im Raum zu verschwinden. Zum anderen wird allgemein Bewusstsein geschaffen, wie oft Daten im Smart Home erhoben werden.

Kontext-basierte, automatische Regulierung von Geräten

Ein weiteres Ziel des Datenautonomie-Assistenten ist die möglichst automatisierte Regulierung der smarten Geräte anhand der Datenschutzpräferenzen der Benutzer:innen in spezifischen Situationen. In den meisten Fällen sollten die Funktionen der Geräte nutzbar sein und ihren Zweck erfüllen. In einigen, von den Benutzer:innen festgelegten Situationen, überwiegt aber das Bedürfnis nach Datenschutz. Im Zuge des DAMA-Projektes wurden mehrere empirische Studien durchgeführt, um das Bedürfnis nach Datenschutz in unterschiedlichen Situationen zu ermitteln und welche Geräte, bzw. Sensoren dabei besonders heikel sind. Durch die Automatisierung bleibt der grundsätzliche Mehrwert der Convenience von Smart Home Systemen erhalten. Denn häufig werden Lösungen die datenschutzsensibel sind, eben nicht verwendet, weil sie einen höheren Aufwand mit sich bringen (Sheridan 2019).

In DAMA wird die Sicherung des Datenschutzes im Smart Home auf drei grundlegende Arten gesichert:

- Sicherstellung der Privatsphäre der Hausbesitzenden durch Verhinderung von Datenlecks in die Cloud, beispielsweise durch Gerätehersteller, Hacker:innen oder Nachrichtendienste.
- Gewährleistung der Privatsphäre von Gästen durch Verhinderung von Datenabflüssen in die Cloud.
- Schutz der Privatsphäre der Hausbesitzenden vor Datenlecks durch Personen mit temporärem Zugang zur smarten Umgebung.

3.2 Technische Umsetzung

Um diese Ziele zu erreichen, muss das System zum einen in der Lage sein, Informationen über die aktuelle Situation im Smart-Home zu erlangen und zum anderen, diese Informationen zu verarbeiten und daraufhin eine *Steuerung* der Geräte vorzunehmen. Um mehr *Transparenz* zu erreichen, sind sog. Aktoren – also Geräte, die eine Aktion ausführen können, wie z. B. den Benutzer:innen aktuelle Informationen über die Smart Home-Geräte und das System selbst zu geben – integriert.

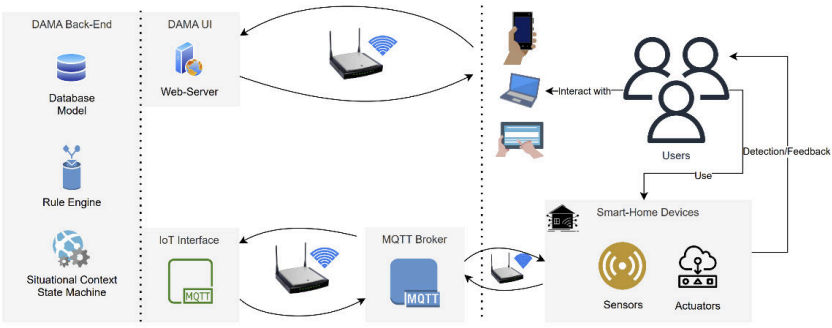

Abbildung 1: Architektur des Datenautonomie-Assistenten

Abbildung 1 zeigt den schematischen Aufbau der Architektur von DAMA. Auf der linken Seite befindet sich das sog. „Back-End". Dieses kommuniziert über die Kommunikations-Ebene (Mitte) mit den Benutzer:innen über die Präsentations-Ebene (rechts). Die smarten Geräte mit diversen Sensoren und Aktoren werden genutzt, um die nötigen Kontextinformationen zu bekommen und auch um die Regulierung dieser Geräte selbst zu verändern. Im Folgenden werden die einzelnen Ebenen näher erläutert.

Back-End

Im „Back-End" werden die von verschiedenen Sensoren und Geräten erfassten Daten und Informationen gesammelt und verarbeitet. Basierend auf der Benutzerkonfiguration, einschließlich der Einstellung verschiedener Situations-Modi, ist die Business-Logik des Datenautonomie-Assistenten für die Verarbeitung und Steuerung der Geräte im Smart Home durch Geräte- (Device-) Ebene verantwortlich.

Persistenz (Database Model)

In einer relationalen Datenbank werden die Informationen über smarte Geräte und Komponenten, sowie die Informationen über Situationsmodi und automatisierte Regeln dauerhaft gespeichert.

In das System ist eine *Regel-Engine* integriert, welche die Nutzer:innen in der Oberfläche einfach konfigurieren können. So können die automatisierten Regulierungen der Geräte ausgelöst werden. Die Regeln müssen persistent abgelegt werden, um jederzeit abrufbar zu sein.

Des Weiteren ist hier die Logik zum Wechsel der Situations-Modi hinterlegt, die die Informationen der Sensoren verarbeitet, mittels der Regel-Engine Entscheidungen trifft und dann über entsprechende Schnittstellen die Regulierung der Geräte veranlasst.

Kommunikations-Ebene

DAMA kann mit verschiedenen Aktoren und Sensoren kommunizieren, um die gewünschte Regulierung und Transparenz für die Benutzer:innen herzustellen. Es wird das MQTT-Protokoll eingesetzt (falls unterstützt), um zwischen dem Back-End und den Geräten zu Informationen zu übermitteln. Das System ist erweiterbar, sodass verschiedene weitere Geräte unterstützt werden können.

Präsentations-Ebene

Diese Ebene ist durch eine webbasierte Benutzeroberfläche bedienbar, die auf mobilen Endgeräten wie Tablets und Smartphones, sowie anderen Geräten (z. B. Smart-TV) angezeigt werden kann. In der endgültigen Version wird die Datenverbindung zwischen Geräten und dem Controller TLS-Verschlüsselung verwenden, um Manipulation der gesendeten Informationen vorzubeugen. Die Benutzer:innen können sich hier einen Account anlegen, der durch ein Passwort geschützt wird. In einem Haushalt mit mehreren Personen sind mehrere Benutzer:innen mit verschiedenen Situations-Modi möglich.

3.3 Situationserkennung

Die Situationserkennung umfasst Komponenten, die Informationen über sensorische Systeme sammeln, wie Mikrofone in Sprachassistenten, Umweltsensoren, aber auch KI-gestützte Algorithmen in Verbindung mit Kameraaufnahmen. In unseren empirischen Studien zeigt sich, dass für das Bedürfnis nach Privatheit mitentscheidend ist, wie viele, bzw. welche Menschen sich im Smart-Home aufhalten. Deshalb versucht das System, zu erkennen, wer und wie viele Personen sich in der aktuellen Smart Home- (oder Büro-) Umgebung aufhalten, auf die der DAMA-Assistent Zugriff hat. Da DAMA darauf ausgelegt ist, die Privatsphäre zu maximieren, verwendet das System minimalinvasive Detektionstechnologie und vermeidet biometrische Erkennung, wie Gesichts-, Sprach- oder Iriserkennung. Kameras befinden sich in weniger privaten Bereichen, wie dem Eingang, konzentrieren sich nur auf einen kleinen Bereich und nur von oben. Die KI versucht lediglich, Personen beim Betreten oder Verlassen zu erkennen, und zeichnet keine biometrischen Informationen auf. Die Datenverarbeitung erfolgt ausschließlich lokal.

Weitere Komponenten und Sensoren können an das System angeschlossen werden, um noch weitere Situationen zu erkennen und darauf reagieren zu können. Im aktuellen System ist ein digitaler Kalender angeschlossen, womit sich – je nach geplantem Ereignis, Änderungen an den smarten Geräten anstoßen lassen. So kann beispielsweise der Besuch einer bestimmten Person im Kalender vermerkt werden, worauf das System schon im Vorfeld die gewünschten Privatsphäre-Einstellungen vornimmt.

Benutzeroberfläche

Es wurde eine Web-basierte Benutzeroberfläche implementiert, über die alle Funktionen von DAMA genutzt und gesteuert werden können.

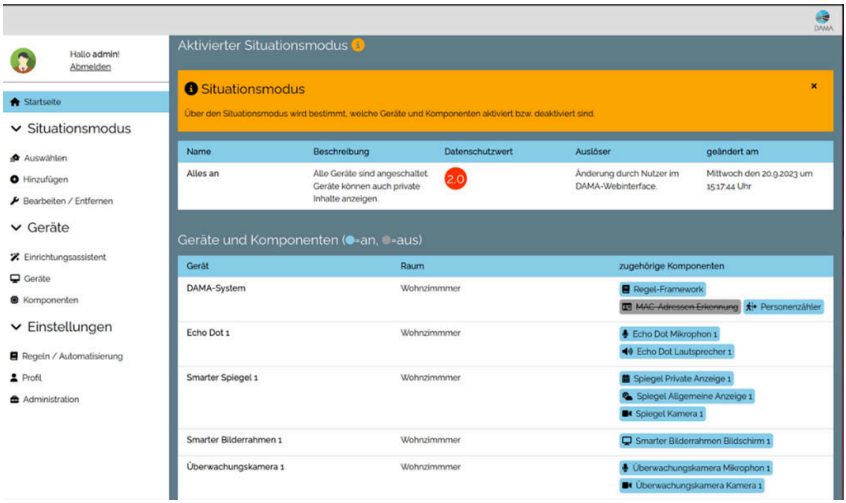

Abbildung 2: Bedienoberfläche

Die Oberfläche umfasst die folgenden Funktionen:

- *Startseite:* Übersicht über den aktuellen Situationsmodus samt allen dazu eingeschalteten smarten Geräten und Komponenten. Ein daraus errechneter Datenschutzwert wird einfach sichtbar und farblich hervorgehoben dargestellt, um die Benutzer:innen zu informieren.
- *Situationsmodus bearbeiten:* Hier können die Benutzer:innen den aktuell eingestellten Modus manuell ändern, neue Situationsmodi erstellen oder diese anpassen.
- *Einrichtungsassistent:* Über einen leicht zu bedienenden Assistenten wird der Nutzer durch die Einrichtung der smarten Geräte geführt. Dies muss nur bei der Einrichtung des Systems oder beim Hinzufügen eines neuen Geräts geschehen. Ziel ist es, die technischen Hürden bei der Nutzung so niedrig wie möglich zu halten.
- *Regeln/Automatisierung:* Hier können Benutzer:innen verschachtelte Regeln anlegen, wie das System auf Ereignisse reagieren und damit die Situationsmodi ändern soll. Als Beispiel könnte eine Regel angelegt werden, anhand derer bei Eintritt einer bestimmten Person in das Smart-Home der Sprachassistent und die Anzeige eines Privaten Kalenders abgeschaltet wird, bis die Person das Smart-Home wieder verlässt.
- *Geräte/Komponenten:* Hier können die Geräte und Komponenten, die bereits im System eingerichtet sind, verwaltet werden. Namen und Da-

ten, wie beispielsweise für die Berechnung des Datenschutzwertes, können hier ebenfalls modifiziert werden.
- *Administration:* Hier können bestimmte Benutzer:innen die Profile der anderen Benutzer:innen und grundlegende Einstellungen des Systems verwalten.

Integration und Test-Aufbau

Abbildung 3: Grundriss des Smart Home bzw. Smart Office Bereichs

Das DAMA-System wurde in das Smart Home / Smart Office Labor im Bürogebäude des Fraunhofer IAO in Stuttgart integriert. Das Labor ist in einen Smart Home-Bereich (links) und einen Smart Office-Bereich (rechts) unterteilt, wie in Abbildung 3 dargestellt. In der Evaluations-Phase des Projektes wurde der Smart-Home Bereich genutzt. Der Smart Home-Bereich umfasst Geräte wie einen intelligenten Kühlschrank, ein intelligentes Sofa, einen intelligenten Couchtisch, einen intelligenten Spiegel und einen intelligenten Fernseher. Außerdem sind zwei Tablets, verschiedene smarte Steckdosen, mehrere Sprach-Assistenten (Amazon Alexa), Web-Cams und der Smart-Home Hub „Homey" integriert. Kern der Applikation ist ein Kleinst-Rechner, auf dem das System selbst läuft.

4. Szenarien

Durch verschiedene Szenarien adressieren wir die unterschiedlichen Herausforderungen für den Datenschutz im Smart Home und berücksichtigen typische Konstellationen an Geräten und Akteuren. Die Szenarien sind auch Grundlage für die Evaluation, anhand derer überprüft wird, ob der von uns entwickelte Prototyp wirklich zu einer Verbesserung für Nutzer:innen geführt hat. Dazu haben wir fünf Szenarien erarbeitet, in denen sich typische Anwendungsfälle konkret widerspiegeln. Sie sind stark an die Nutzungsrealität angelehnt, um eben genau für diese eine Verbesserung zu erzielen. Die von uns entwickelten Szenarien decken dabei eine Bandbreite von Situationen und Akteurskonstellationen ab, wie sie in der alltäglichen Nutzung vorkommen, aber abstrakt genug sind, um für die Entwicklung verallgemeinerbare Prinzipien und Ziele anlegen zu können. Es können dabei jedoch nicht alle Datenschutz-Aspekte im Smart Home erfasst werden. Wir sind jedoch der Überzeugung, dass diese Szenarien eine gute Basis für die Entwicklung sind und die Nutzungsrealität gut abbilden. Das System selbst lässt sich auch für anderweitige Szenarien flexibel anpassen.

4.1 Szenario 1: Bewohner:in kommt nach Hause (DAMA aktiviert alle Smarten Geräte)

Das erste Szenario ist eine Basisversion und spiegelt die häufigste Ausgangsposition bei der Nutzung wider: eine Person, die in einem Smart Home lebt. Wir gehen davon aus, dass eine Person die eigenen Smart Home-Gegenstände in ihrem normalen Alltag ihre Smart Home Gegenstände auch nutzen will, sonst hätte sie diese nicht angeschafft. Deshalb werden die Geräte angeschaltet, sobald die Person alleine nach Hause kommt. Durch einen Sensor des Systems wird erkannt, dass jemand das Haus oder die Wohnung betritt. Dass es sich dabei um den bzw. die Bewohner:in handelt, wird über einen Mac-Adressen-Scanner festgestellt, der die Person über ihr Smartphone als Besitzer:in des Smart Home identifiziert. Daraufhin werden alle smarten Gegenstände durch DAMA freigegeben und aktiviert. Dieses Basisszenario erweitern wir Schritt für Schritt und adaptieren es entsprechend.

4.2 Szenario 2: Bekannte Personen kommen zu Besuch

Eine erste Abweichung, die eine Abschaltung von Geräten erfordern könnte, ist die Anwesenheit einer anderen Person, also von Besuch. Wenn diese Person nicht darüber informiert ist, dass Smart Home-Geräte Daten aufzeichnen, liegt keine informierte Einwilligung vor. Dementsprechend sollten die Smart Home-Geräte, die Daten über die Besucher aufzeichnen können, deaktiviert sein. So sollen beispielsweise persönliche Gespräche nicht zufällig durch aktive Mikrofone mitgeschnitten werden, insbesondere, wenn sehr private Dinge besprochen werden.

Wenn die Person dem oder der Bewohner:in bekannt ist, kann es sein, dass diese über die Geräte bereits Bescheid weiß, aber trotzdem bestimmte Sensoren nicht aktiviert haben möchte. Um die Person von einer nicht bekannten Person zu unterscheiden, kann diese ebenfalls durch den Mac-Adressen-Scanner erkannt werden[1], und der Meta-Assistent schaltet dann automatisch um auf das für die jeweilige Besucher:in festgelegten Situationsmodus. Für den Besuch können aber auch die Besitzer:innen ihre eigenen Einstellungen festlegen, so können beispielsweise private Anzeigen wie Kalender deaktiviert werden.

4.3 Szenario 3: Unbekannte Person kommt ins Smart Home

Es können unterschiedliche Gruppen und Konstellationen im Smart Home anwesend sein. So macht es einen großen Unterschied, wenn es sich nicht um eine bekannte Person handelt, die das Haus betritt, sondern eine bisher unbekannte Person, beispielsweise ein:e Handwerker:in.

In diesem Fall ist es nicht mehr möglich, diese Person durch den Mac-Adressen-Scanner zu identifizieren, sondern sie muss alternativ erkannt werden (z. B. durch einen Personenzähler), und es kann durch das Fehlen eines freundschaftlichen Verhältnisses nicht davon ausgegangen werden, dass die Person davor über das Vorhandensein von Smart Home Geräten informiert ist. Neben dem Aspekt, dass diese Person nicht ohne Informierung Daten abgibt, möchte man als Bewohner:in möglicherweise nicht,

1 Dafür müsste die bekannte Person mit ihrem Smartphone in das WLAN eingewählt sein. Dies passiert in den meisten Fällen, in denen privater Besuch vorbei kommt automatisch. Zusätzlich braucht es dann die Einwilligung der Person, dass die MAC-Adresse des Smartphones von DAMA erkannt werden darf.

dass private Daten, zum Beispiel auf Anzeigen, für diese fremden Personen sichtbar sind.

4.4 Szenario 4: Home-Office

Wenn eine Person allein zu Hause ist, kann dennoch nicht gewollt sein, dass bestimmte Sensoren etwas aufzeichnen können. Sollten die Bedürfnisse der Bewohner:in in einer Situation von der Basiseinstellung abweichen, kann sie über DAMA den Situationsmodus jederzeit unkompliziert anpassen, sodass Geräte und Sensoren gemäß den Wünschen deaktiviert werden. Hierdurch sollen die Daten der Person geschützt werden. Es muss jederzeit eine Abwägung zwischen Nützlichkeit der Geräte und Risiko der Datenweitergabe erfolgen. Basierend auf dieser Abwägung stellt sich also die Frage, in welchen Situationen die Geräte dann abgeschaltet werden sollen. Dies spiegelt sich im Szenario Home-Office wider.

So sollte eine Telefonkonferenz, die im Smart Home geführt wird, nicht durch ein Smart Home-Geräte mitaufgezeichnet werden. Hinzu kommt aber auch ein zweiter Aspekt, es sollten auch keine privaten Informationen aus Versehen veröffentlicht werden. Zum Beispiel, wenn ein Gerät etwas durchsagt oder Anzeigen im Hintergrund zu sehen sind. Deshalb ist es sinnvoll, gewisse Geräte abzuschalten. Dies kann auch automatisch passieren durch eine Verbindung mit dem eigenen Kalender, sodass während eines Meetings Sprachassistenten oder digitale Anzeigen automatisch deaktiviert werden.

4.4 Szenario 5: Mehrere Personen wohnen im Smart Home

Die bisherigen Szenarien waren dadurch gekennzeichnet, dass es eine klare Unterscheidung/Hierarchie gab zwischen Bewohner:in und Besucher:innen. Wenn es mehrere Bewohner:innen gibt, ist dies nicht mehr der Fall. Die Herausforderung dabei ist es, abzuwägen, was zu tun ist, wenn diese verschiedene Interessen haben. Eine Erkennung der verschiedenen Personen wäre grundsätzlich ebenfalls durch den Mac-Adressen-Scanner möglich.

Wenn beispielsweise eine Person Home-Office macht und im Schlafzimmer sitzt, wo auch der gemeinsame Schreibtisch steht. Dort hat sie gerade eine wichtige Besprechung mit einem Kunden per Telefon. Deswegen hat

sie alle anderen Kameras und Mikrofone durch DAMA im Schlafzimmer deaktivieren lassen. Während ihres Calls kommt die zweite Person von der Arbeit nach Hause. DAMA weiß, dass diese, um sich vom Arbeitstag zu erholen, gerne Musik hört und aktiviert deshalb die Smart Speaker, als diese heimkommt.

Hier zu entscheiden, welche Präferenz bevorzugt werden soll, ist deutlich schwieriger und war Teil der dritten Umfrage unserer Evaluation.

5. Evaluation

Um sicherzustellen, dass die Funktionen des Prototyps die oben beschrieben Ziele erfüllen und um während der Entwicklung Perspektiven von Nutzer:innen einzubeziehen, haben wir im Projekt zu verschiedenen Zeitpunkten Nutzerbefragungen durchgeführt. Eine erste Umfrage zielte dabei darauf ab, generelle Präferenzen der Benutzer:innen zu identifizieren – also deren Vorwissen zu Privatsphäre abzuschätzen und einzuschätzen, ob geplante Funktionen angenommen werden. In der zweiten Umfrage ging es darum für die Automatisierung des Meta-Assistenten nützliche Gruppierungen der Geräte- und Komponentengruppen zu finden, die für eine sinnvolle Vorbelegung von Situations-Modi nützlich wären. In den abschließenden Experimenten haben wir anhand der Szenarien getestet, ob die Bedienung des Prototyps selbsterklärend ist und Nutzer:innen dadurch mehr Transparenz erfahren und Kontrolle über den Abfluss ihrer Daten ausüben können. Grundsätzlich lassen die Studien dabei auch Rückschlüsse auf die Nutzung smarter Geräte im Allgemeinen und die Präferenzen zur Privatsphäre zu.

5.1 Umfrage 1

Die erste Umfrage wurde als quantitative Erhebung mittels eines standardisierten Fragebogens durchgeführt. Sie bestand hauptsächlich aus Fragen mit einer 6-stufigen Likert-Skala, sowie einigen offenen Fragen und wurde mit dem Umfragetool Lime-Survey erstellt. Am Ende lagen von 607 Teilnehmenden auswertbare Fragebögen vor, die mittels deskriptiver und Inferenzstatistik mit dem Programm SPSS analysiert wurden. Die Ergebnisse sind:

- Die Befragten finden die Erhebung mit Kameras und Mikrofonen deutlich problematischer als die Erhebung von Meta-Daten (wie z. B. Nutzungsdaten von Steckdosen oder MAC-Scannern). Das zeigt, dass für Risiken durch die Übertragung solcher Daten ein zu niedriges Bewusstsein herrscht, trotz der in Kapitel 2 dargestellten Probleme.
- Insgesamt wünschen sich die Befragten, über Sensoren von Smart Home-Gegenständen informiert zu werden (bspw. ist für 94,05 % der Befragten eine Informierung über das Vorhandensein von Kameras wichtig).
- Kontrolle über die Sensoren auszuüben, ist den Befragten ebenfalls wichtig (83,89 % der Befragten ist die Möglichkeit zur Deaktivierung von Kameras wichtig).
- Je früher über Kameras, Mikrofone und weiteres informiert wird, desto besser wird dies bewertet (83,44 % der Befragten finden eine Informierung beim Betreten eines Smart-Homes für „eher gut" bis „sehr gut").
- Sie präferieren dabei, über Anzeigen informiert zu werden oder aber durch das eigene Smartphone, gegenüber Durchsagen. (84,55 % der Befragten befinden die Informierung via Displayanzeige „eher gut" bis „sehr gut", 69,03 % via Smartphone und nur 41,90 % per Durchsage).
- 85,38 % der Smart-Home Nutzer:innen halten einen Privacy-Meta-Assistenten für teilweise nützlich bis essenziell. Personen, die bereits Smart Home-Geräte benutzen, sind auch als Besucher:innen in der Tendenz eher bereit, gewisse Daten für DAMA bereitzustellen und Funktionen des Meta-Assistenten benutzen. Personen, die bisher keine Geräte benutzen, sind tendenziell eher skeptisch gegenüber dem Meta-Assistenten und ihre Daten stärker schützen zu wollen. Auch sehen sie die Automatisierung kritischer.
- Sowohl der Meta-Assistent als auch Smart Home-Geräte im Allgemeinen erzeugen bei einigen Befragten Skepsis. Hier muss es durch Transparenz und Optionalität der Funktionen gelingen, diese Bedenken auszuräumen. Deswegen ist es umso wichtiger zu reflektieren, wie Funktionen dargestellt werden und dass die grundlegende Funktion von DAMA auch ohne Automatisierung, sondern nur durch eine manuelle Bedienung funktionieren muss (Datensparsamkeit).

5.2 Umfrage 2

In einer weiteren Online-Umfrage standen Präferenzen von Nutzern bezüglich der Abschaltung bestimmter Komponenten und Geräte in bestimmten Situationen im Fokus. Hier wurden qualitative und quantitative Daten erfasst und ausgewertet. Durch Clustering-Verfahren sollte erforscht werden, ob es gewisse Patterns bei der Bewertung von Situationen in Zusammenhang mit Smart-Home Geräten und Komponenten gibt.

Die Ergebnisse unserer Online-Umfrage mit insgesamt 495 vollständig und sorgfältig (Bearbeitungszeit > 3 Minuten) ausgefüllten Fragebögen bestätigten die Relevanz von Situationsmodi bei Entscheidungen zur Deaktivierung von Gerätekomponenten.

Eine Gemeinsamkeit lag im Wunsch der Teilnehmenden, bestimmte Komponenten gemeinsam zu deaktivieren, insbesondere, wenn sie ähnliche Funktionen hatten, wie Mikrofon, Kamera oder Lautsprecher. Die Funktion ist dabei ausschlaggebender als das Gerät, in dem sie realisiert ist. Komponenten, die Bild und/oder Ton aufzeichnen, wurden dabei als potenziell größte Gefahr für die Privatsphäre eingeschätzt.

Ein Beispiel verdeutlicht diese Ergebnisse: Wenn Personen allein zu Hause waren, wollten 51,5 % in bestimmten Situationen mindestens die Sensoren (Mikrofone) des Smart-TV und des Sprachassistenten gemeinsam deaktivieren, weitere Funktionen aber gerne behalten.

Es zeigte sich zudem, dass mit zunehmender Ungewissheit der Situation der Wunsch nach Deaktivierung von Komponenten stärker ausgeprägt war, wie beispielsweise, wenn die Situation schwieriger zu bewerten ist, z. B. durch die Anwesenheit unbekannter Personen. Dies äußerte sich in einer Reduktion der Anzahl von Clustern und einer verbesserten Qualität des Clusterings. Der Wunsch, Sensor-Komponenten gemeinsam zu deaktivieren, war dann besonders ausgeprägt. Hier wäre eine granulare Steuerung von Gerätekomponenten gewünscht (z. B. nur die Mikrophone verschiedener Geräte temporär zu deaktivieren), was die meisten Hersteller solcher Geräte jedoch nicht unterstützen. Eine interessante Ausnahme bildete die Situation »Fremde zu Besuch im eigenen Smart-Home«, wo der Sicherheitswunsch überwog, und deshalb die im Smart-Home-Szenario vorhandene Kamera nicht deaktiviert werden sollte.

Insgesamt verdeutlichten diese Ergebnisse die Vielschichtigkeit der Entscheidungsprozesse im Zusammenhang mit der Deaktivierung von Gerätekomponenten und die Bedeutung einer differenzierten Betrachtung des Kontextes.

5.3 Umfrage 3

Bei der dritten Erhebung wurden User-Tests im Smart-Home Labor des Fraunhofer IAO durchgeführt, um die implementierten Funktionalitäten, Konzepte und Anwendungspotenzial von DAMA zu evaluieren. Dabei wurde stärker auf qualitative Methoden gesetzt. Insgesamt haben 13 Proband:innen an den Experimenten teilgenommen. Die Tests setzten sich dabei sowohl aus einem theoretischen Part als auch aus einem praktischen, interaktiven Part zusammen. Im interaktiven Part sollten die Versuchspersonen das System ohne vorherige Einweisung nutzen. Der Versuch an sich wurde mit der Thinking Aloud-Methode durchgeführt und mit Interviews und kurzen Fragebögen abgerundet.

Das Ergebnis der Versuche war, dass die Versuchspersonen durch DAMA besser informiert sind und beispielsweise Gefahren für den Datenschutz erkennen, die ihnen davor nicht bewusst waren. Die Bedingung des Meta-Assistenten gelang ihnen dabei meist intuitiv, und sie konnten für vorgegebene Situationen die vorhandenen Smart Home-Gegenstände und deren Sensoren so steuern, dass sie sich in der Umgebung wohlfühlten und ihre Privatheit verbessert war.

Im Rahmen der Experimente haben wir die Versuchspersonen befragt, wie sie sich in Konfliktsituationen entscheiden würden. Also Situationen, in denen sich mehrere Personen im Smart Home befinden und nicht übereinstimmen, welche Geräte und Sensoren deaktiviert werden sollen. In den vorgestellten Szenarien haben sich die Versuchspersonen überwiegend für die Option entschieden, die datenschutzsensibler ist, also dafür Geräte abzuschalten, auch wenn deren Verwendung von Personen in der Situation gewünscht wurde. Wenn zum Beispiel ein Gast sie als Bewohner:in bitten würde, Smart Home Geräte abzuschalten, würden dies 92 % der Versuchspersonen tun. Jedoch sind die Versuchspersonen dabei immer darum bemüht einen Kompromiss zu finden oder die andere Seite zu überzeugen, statt ihren Willen einfach durchzusetzen. Das heißt, hierfür ist eine technische Lösung nicht unbedingt die optimale Variante. Was der Assistent jedoch leisten kann, ist 1.) Die Personen erstmalig auf die Geräte hinzuweisen. 2.) Alle notwendigen Informationen für die Entscheidung geben. Auch wenn die letztendliche Kompromissfindung bei den Personen liegt, können diese durch DAMA die Basis für ihre informationelle Selbstbestimmung in solchen Situationen verbessern.

6. Schluss

Smarte Geräte und KI-basierte Assistenten werden in privaten sowie professionellen Umgebungen aktuellen Trends nach in Zukunft noch stärker als heute zum Einsatz kommen. Da Geräte- und Ökosystemhersteller wenig Transparenz und Kontrolle über die Sammlung der Daten ermöglichen und meist entgegengesetzte Interessen und Motive haben, wird so die Datenautonomie und Transparenz für die Benutzer:innen abnehmen und weitestgehend unkontrollierbar.

In diesem Paper stellten wir den Smart-Home Privacy-Assistenten »DAMA« in seiner aktuellen Ausprägung vor. Das System kann durch situative Erkennung des Kontextes und das Konzept der Situations-Modi semi-automatisch Sensoren und Aktoren in smarten Umgebungen dahingehend regulieren, dass eine erhöhte Transparenz für die Benutzer:innen erreicht wird, als auch eine Stärkung der Privatsphäre und Datenautonomie möglich wird. Es wurde ein funktionsfähiger Prototyp implementiert und seine Architektur und Funktionsweise dargestellt. Darüber hinaus wurde das System anhand der Ergebnisse mehrerer Nutzerstudien weiterentwickelt und evaluiert. Das System liefert so einen praktischen und Beitrag zur Stärkung der Datenautonomie in Umgebungen mit smarten Geräten und KI-basierten Assistenten. Die Nutzung der Geräte und Funktionen bleibt weiterhin gegeben und wird nur in vom Benutzer gewünschten Situationen temporär, feingranular und automatisch reguliert. Benutzer:innen, aber auch Gäste in smarten Umgebungen werden dabei durchgehend über die im Einsatz befindlichen Geräte und deren Satus aufgeklärt und können so wohlinformierte Entscheidungen treffen.

Danksagung

Wir danken ausdrücklich der Baden-Württemberg Stiftung für die finanzielle Unterstützung unserer Forschungsarbeit. Ihre fachliche und finanzielle Unterstützung war für den Erfolg des Projektes entscheidend.

Literatur

Brandt Mathias (7. Januar 2020): Wo Alexa und Co. im Einsatz sind. URL: https://de.statista.com/infografik/20414/orte-an-denen-smart-speaker-genutzt-werden/ (besucht am 19.6.2020).

Breithut Jörg (3. Januar 2020): Kamerabesitzer konnte in fremde Wohnungen schauen. *SPIEGEL Online* URL: https://www.spiegel.de/netzwelt/gadgets/xiaomi-kamera besitzer-sah-in-fremde-wohnungen-google-reagiert-a-1303518.html (besucht am 19.6.2020).

Bundesamt für Sicherheit in der Informationstechnik BSI (06 Mai 2022): IT-Sicherheitskennzeichen jetzt auch für smarte Verbraucherprodukte. Pressemitteilung. URL: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220504_IT-SiK-Erweiterung.html (besucht am 8.8.2022).

BVerfGE 65, 1 - 71 - 1 BvR 209/83 -, Rn. 1-215.

Feldmeier Felix; Hermann, Maximilian; Kohou, Lukas; Lauenroth, Kim; Salomon, Gabriela; Thiel, Christian und Westermeier, Michael (2022): Neue Mehrwerte im Smart Home durch Daten. Berlin: BITKOM. URL: https://www.bitkom.org/sites/main/files/2022-09/220909_LF_Neue-Mehrwerte-im-Smart-Home-durch-Daten.pdf (besucht am 8.8.2022).

Ghiglieri, Marco; Hansen, Marit; Nebel, Maxi; Pörschke, Julia Victoria und Simo Fhom, Hervais (2016): Smart-TV und Privatheit: Bedrohungspotenziale und Handlungsmöglichkeiten. Forschungsbericht. Karlsruhe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. URL: https://plattform-privatheit.de/p-prv-wAssets/wp-content/uploads/Forschungsbericht-Smart-TV-und-Privatheit_Druckfassung-1.pdf (besucht am 11. Juni 2024)

Guhr, Nadine; Werth, Oliver; Blacha, Philip Peter Hermann und Breitner, Michael H. (2020): Privacy concerns in the smart home context. *SN Applied Sciences*, 2(2). doi: 10.1007/s42452-020-2025-8.

Hensen, Christian (2022): Saugroboter mit Kamera reinigte ihr Bad – danach landeten Bilder einer Frau auf der Toilette im Netz. *STERN.De*. URL: https://www.stern.de/digital/online/saugroboter-mit-kamera--bilder-einer-frau-auf-der-toilette-landeten-im-netz-33027364.html (besucht am 19.6.2020).

Hern, Alex (2019): 'Amazon staff listen to customers' Alexa recordings, report says: Staff review audio in effort to help AI-powered voice assistant respond to commands. *The Guardian*. URL: https://www.theguardian.com/technology/2019/apr/11/amazon-staff-listen-to-customers-alexa-recordings-report-says (besucht am 19.6.2020).

Jandt, Silke (2016): Informationelle Selbstbestimmung. In: Heesen, Jessica (Hrsg.): *Handbuch Medien- und Informationsethik*. Stuttgart: J.B.Metzler, S. 195-201. doi: 10.1007/978-3-476-05394-7_26.

Kröger, Jacob (2019): Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things. In: Strous, Leon und Cerf, Vinton (Hrsg.): *Internet of Things. Information Processing in an Increasingly Connected World. IFIPIoT 2018*. Cham: Springer, S. 147–159. doi: 10.1007/978-3-030-15651-0_13.

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.

Marky, Karola; Prange, Sarah; Krell, Florian; Mühlhäuser, Max und Alt, Florian (2020): "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In: Cauchard, Jessica und Löchtefeld, Markus (Hrsg.): *MUM 2020: Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia*. New York: ACM Press, S. 83–95. doi: 10.1145/3428361.3428464.

Moltrecht, Klaas und Schnaack, Greta (2022): Das intelligente Zuhause: Smart Home 2022. Ein Bitkom-Studienbericht. Berlin: BITKOM. URL: https://www.bitkom.org/sites/main/files/2022-09/220912_Bitkom_Smart_Home_Chartbericht_2022_final.pdf (besucht am 19.6.2020).

Mühlhoff, Rainer (2020): Prädiktive Privatheit: Warum wir alle „etwas zu verbergen haben". In: *KI als Laboratorium? Ethik als Aufgabe!* Berlin: Berlin-Brandenburgische Akademie der Wissenschaften, S. 38–45. URL: https://www.bbaw.de/files-bbaw/user_upload/publikationen/BBAW_Verantwortung-KI-3-2020_PDF-A-1b.pdf (besucht am 19.6.2020).

Rajkumar, Ragunathan; Lee, Insup; Sha, Lui and Stankovic, John (2010): Cyber Physical Systems: The Next Computing Revolution. In: *DAC '10: Proceedings of the 47th Design Automation Conference*. New York: ACM Press, S. 731-736. doi: 10.1145/1837274.1837461.

Sheridan, Kelly (2019): Consumers Care About Privacy, but Not Enough to Act on It. *DarkReading*. URL: https://www.darkreading.com/threat-intelligence/consumers-care-about-privacy-but-not-enough-to-act-on-it (besucht am 01.02.2024).

Wachter, Sandra (2018): Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. *Computer Law & Security Review*, 34 (3), S. 436-449. doi: 10.2139/ssrn.3083554.