verbraucherzentrale
Nordrhein-Westfalen

Zinaida Benenson

DATENSCHUTZ IM INTERNET DER DINGE

Können Datentreuhänder helfen?

Vortrag 14 der Reihe „Zu treuen Händen“ | Februar 2022

ZU TREUEN HÄNDEN?
Verbraucherdatenschutz und digitale Selbstbestimmung

Eine Online-Vortragsreihe der Verbraucherzentrale NRW e. V.

mit Unterstützung durch das
Institut für Verbraucherinformatik der Hochschule Bonn-Rhein-Sieg

Impressum

Verbraucherzentrale Nordrhein-Westfalen e.V
Kompetenzzentrum Verbraucherforschung NRW.
Mintropstraße 27
40215 Düsseldorf
zutreuenhaenden@verbraucherzentrale.nrw

Gefördert durch

Ministerium für Umwelt, Landwirtschaft,
Natur- und Verbraucherschutz
des Landes Nordrhein-Westfalen

ORIGINALBEITRAG

Verbraucherzentrale NRW, Düsseldorf 2022

AUTORIN

Dr. rer. nat. Zinaida Benenson leitet die Forschungsgruppe „Human Factors in Security and Privacy" an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Ihre Forschungsschwerpunkte umfassen benutzbare IT-Sicherheit sowie IT-Sicherheit für das Internet der Dinge.

DOKUMENTATION „ZU TREUEN HÄNDEN?“
Alle Videos und Paper der Vortragsreihe finden Sie unter
https://www.verbraucherforschung.nrw/zu-treuen-haenden-tagungsreihe-datenintermediaere-datentreuhaender-60831

INHALT

I. ABSTRACT

Das Internet der Dinge soll unseren Alltag durch die Anpassung der digitalen Systeme zu unseren Präferenzen erleichtern. Dafür ist die Auswertung personenbezogener Daten unabdingbar – für Verbraucher jedoch oft intransparent. Außerdem werden IoT-Systeme von mehreren Personen gleichzeitig benutzt, und können sogar unsichtbar sein. Dieser Beitrag erläutert die Besonderheiten der Datenverarbeitung und die Berücksichtigung von Datenschutzpräferenzen in diesen komplexen Systemen.

II. EINLEITUNG[1]

Das Internet der Dinge (Internet of Things, IoT) verspricht, unseren Alltag durch allgegenwärtige Automatisierung und Anpassung der digitalen Systeme zu unseren Präferenzen zu erleichtern. Insbesondere soll alles „smart“ werden: Smarte Beleuchtung schaltet sich ein, wenn man nach Hause kommt; die smarte Heizung passt Temperatur und Luftfeuchtigkeit den Präferenzen der Bewohner an; ein smarter Saugroboter erstellt den Plan der Wohnung, um effizient saugen zu können; die smarte Türklingel filmt die Besucher; smarte Türschlösser lassen den Paketboten rein und die smarte Hauskamera beobachtet, dass er nur in einen vorher bestimmten Bereich der Wohnung geht; smarte Alarmanlagen schützen vor unbefugtem Zutritt. Und das Ganze wird mithilfe von Smartphone-Apps und smarten Sprachassistenten verwaltet. Solche smarten Systeme gibt es nicht nur in privaten Wohnungen und Häusern, sondern auch in Bürogebäuden, Fabriken, Hotels.

Der Begriff Internet of Things wurde in 1999 zum ersten Mal verwendet (Ashton 2009), und hat seitdem den ursprünglichen Begriff Ubiquitous Computing (Weiser 1991) weitgehend ersetzt. Jedoch meinen die beiden Begriffe im Wesentlichen dieselben technischen Zusammenhänge: Computer, Sensoren und Aktoren, eingebettet in die Gegenstände des alltäglichen Lebens und verbunden miteinander (d.h., mit anderen Gegenständen) und mit dem Internet. Sensoren messen Umgebungsparameter, Computer verarbeiten diese Messungen lokal und leiten sie womöglich weiter und aufgrund dieser Vorgänge können Aktoren bestimmte Handlungen autonom ausführen. So würde ein smarter Rauchmelder nicht nur eine Sirene aktivieren, sondern die Bilder der Umgebung an die Besitzer oder an die Feuerwehr senden und eventuell Löschanlagen aktivieren, wenn laut der verarbeiteten Sensorinformationen ein Feuer ausgebrochen ist.

Um smart zu sein, sammeln Systeme persönliche Daten und verraten teilweise sehr viel über die Menschen, die sich in ihrer Nähe aufhalten – seien es die Besitzer der Systeme, ihre bewussten Benutzer oder Unbeteiligte, die eventuell gar nicht wissen, dass das System da ist. Folgen dieses Datensammelns sind für Laien sehr schwer einzuschätzen, und auch in der Industrie und in der akademischen Forschung noch nicht ausreichend untersucht. So stellte sich in der Vergangenheit heraus, dass intelligente Strommesser (auch Smart Meters genannt), falls sie mit einer hohen Granularität den Energieverbrauch in Haushalten messen, den Tagesablauf der Bewohner sowie die im Haushalt vorhandenen Geräte bestimmen lassen (Hart 1989; Molina-Markham et al. 2010). Im Laufe der Jahre wurden verschiedene Techniken vorgeschlagen, um die Ri-

[1] Durchgesehene und vereinzelt um Literaturangaben ergänzte Schriftfassung meines Vortrags am 20. Januar 2022 in der (virtuellen) Vortragsreihe „Zu treuen Händen?“ der Verbraucherzentrale NRW e. V. Die Vortragsform wurde beibehalten.

siken für die Privatsphäre zu mindern, die mit der intelligenten Strommessung zusammenhängen (Rial und Danezis 2011; Yang et al. 2012; Reinhardt et al. 2015). Diese Erkenntnisse haben dazu beigetragen, dass für Smart Metering in Deutschland hohe Datenschutzanforderungen gelten (BSI 2014). Für andere smarte Systeme sind diese Anforderungen jedoch weitgehend nicht festgelegt.

III. DATENFLÜSSE IN IOT-SYSTEMEN

Smarte Systeme sammeln Nutzerdaten in einer bisher beispiellosen Qualität und Quantität (Langheinrich 2009). Nicht nur statische Daten (Name, Geburtsdatum etc.) oder dynamische digitale Daten (z. B. Kaufverhalten), sondern viele Datentypen, die unmittelbar mit der physischen Welt zusammenhängen, können gemessen werden: Ortsdaten, Umgebungsparameter (ist das Licht an oder aus?), physiologische Daten (Puls, Blutdruck, Schlafverhalten, Bewegung). Da die Systeme oft in alltägliche Gegenstände eingebettet sind, können sie mit der Umgebung verschmelzen und unsichtbar werden, sodass die Menschen überhaupt nicht merken, dass das System da ist und ihre Daten sammelt. Auch wenn smarte Systeme bewusst genutzt werden, können Nutzerinnen und Nutzer oft nicht unmittelbar den Systemzustand herausfinden. Zum Beispiel ist es oft unklar, ob ein System an oder aus ist, und wie das System ausgeschaltet werden kann.

So berichten Teilnehmende in Nutzerstudien, dass sie unsicher sind, ob ihre smarten Sprachassistenten ihren Gesprächen lauschen, und wie sie überprüfen können, ob sensible Inhalte aufgezeichnet wurden (Lau et al. 2018, Malkin et al. 2019). Nicht alle wussten, dass ihre Geräte einen physischen Ausschaltknopf haben, oder vertrauten dem Knopf nicht und berichteten, dass sie den Sprachassistenten ganz vom Strom trennen würden, falls sie sichergehen wollten, dass nichts aufgezeichnet wird. Ähnlich unsicher waren sich Nutzerinnen und Nutzer bei smarten Sicherheitskameras, ob sie gefilmt und ihre Gespräche aufgenommen werden, und berichteten, dass sie ihre Geräte entweder vom Strom trennen oder abdecken, wenn sie zu Hause sind (Zeng et al. 2017, Haney et al. 2020). Insgesamt sind Kenntnisse über die Funktionsweise der smarten Umgebungen, über ihre Sensoren und Datenflüsse, unvollständig und fehlerhaft (Abdi et al. 2019, Harper et al. 2020).

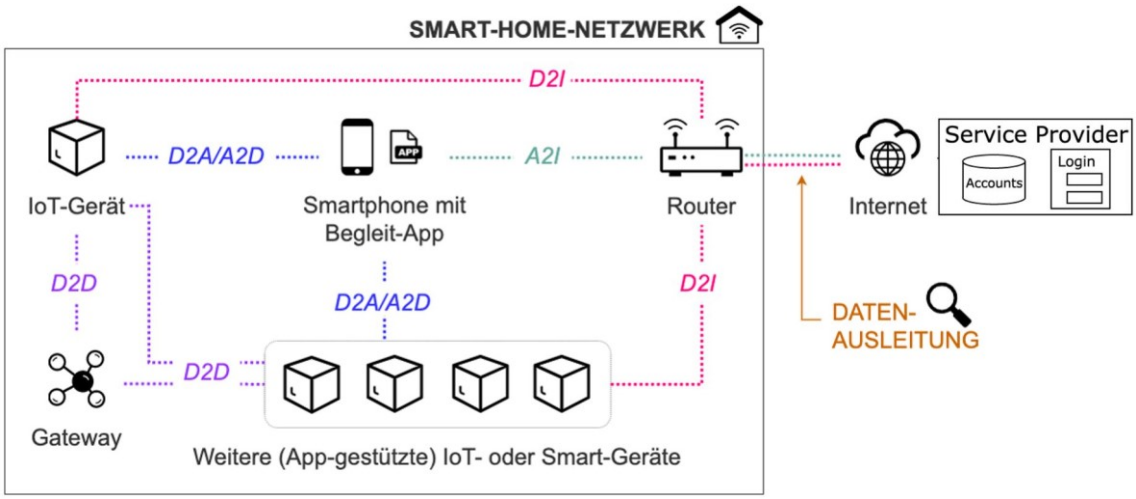

Abbildung 1: Datenflüsse in Smart-Home-Systemen (eigene Darstellung).

Es ist nicht verwunderlich, dass die Verbraucher verunsichert sind. Die IoT-Systeme sind oft komplex und unübersichtlich und bieten den Laien oft keine Anhaltspunkte zur Feststellung ihrer Datenflüsse. Dabei sind unterschiedliche Funktionsweisen möglich, die sich unter anderem in ihren Datenschutzmaßnahmen erheblich unterscheiden können. Diese Möglichkeiten sind schematisch in Abbildung 1 dargestellt am Beispiel von Smart-Home-Systemen. Diese Systeme bestehen aus mehreren Geräten, die miteinander direkt oder mittels eines Gateways kommunizieren (Datenflüsse D2D: device-to-device). Die Geräte können über Begleit-Apps bedient werden. Dabei können Apps und Geräte direkt über lokale drahtlose Netze (z. B. WLAN oder Bluetooth) miteinander kommunizieren (Datenflüsse D2A und A2D). Allerdings ist es auch möglich, dass die Kommunikation vollständig oder teilweise über das Internet stattfindet: Die Apps verbinden sich mit den Servern der Anbieter, wo Nutzerinnen und Nutzer ihre Accounts haben (Datenflüsse A2I), die Anfragen werden an auf den Servern der Anbieter verarbeitet und die Befehle von dort über die App an die Geräte geschickt. Außerdem können die Geräte über einen Router mit dem Internet kommunizieren und insbesondere Daten an die Anbieter der Systeme und an Dritte senden, zum Beispiel zur Analyse, wie es bei Sprachassistenten üblich ist (Datenflüsse D2I).

Zusammenfassend kann man sagen, dass es für die Nutzerinnen und Nutzer oft nicht feststellbar ist, ob die Kommunikation mit den IoT-Geräten und die Verarbeitung und Speicherung der Daten nur lokal stattfindet oder über die Server im Internet läuft. Lokale Datenverarbeitung ist dabei deutlich datenschutzfreundlicher. Insgesamt bieten IoT-Systeme zu wenig Transparenz und sind oft zu komplex, um informierte Kauf- und Nutzungsentscheidungen zu ermöglichen.

IV. INFERENZEN AUS DEN IOT-DATEN

In IoT-Systemen geht es oft nicht nur darum, welche Daten gesammelt werden, sondern auch darum, wie diese Daten ausgewertet werden. So können beispielsweise Audiodaten, die die Sprachassistenten aufzeichnen, nicht nur zum Umsetzen der Befehle der Nutzerinnen und Nutzer verwendet werden. Insbesondere können aus Audiodaten mittels fortgeschrittener Analysetechniken sehr sensible Informationen abgeleitet werden: Alter, Herkunft, mentale und physische Gesundheit, Stimmungen und Emotionen, Alkoholisierung, Schläfrigkeit und Erschöpfung (Kröger et al. 2022). Welche Inferenzen aus welchen Daten gewonnen werden können, ist Nutzerinnen und Nutzern oft nicht bewusst. So gaben über 40 Prozent der Teilnehmenden in einer repräsentativen Umfrage (insgesamt 683 Teilnehmende aus dem Vereinigten Königreich) an, dass ihnen solche Inferenzen nicht bewusst waren, das heißt, sie haben nie über diese Möglichkeit nachgedacht (Kröger et al. 2022).

2017 haben meine Kollegen und ich eine bis dahin vermutete, aber nicht überprüfte Inferenzmöglichkeit empirisch untersucht: Kann man aus den Raumklimadaten, die smarte Heizungssysteme sammeln (Raumtemperatur und relative Luftfeuchtigkeit) sensible Daten über die Nutzerinnen und Nutzer ableiten? Insbesondere wollten wir herausfinden, ob man die Präsenz der Menschen in einem Raum erkennen kann, und welchen Tätigkeiten diese Menschen nachgehen (Morgner et al. 2017). Um zu überprüfen, ob Raumklimadaten eine Bedrohung für die Privatsphäre darstellen könnten, haben wir eine Serie von kontrollierten Experimenten durchgeführt. Wir haben drei Büroräume mit Temperatur- und Luftfeuchtigkeitssensoren ausgestattet. Diese Sensoren haben regelmäßig, mit Abstand von wenigen Sekunden, Messungen durchgeführt und diese drahtlos an einen Rechner geschickt. Wir haben insgesamt 36 Teilnehmende rekrutiert, die

in diesen Räumen eine im Voraus abgesprochene Sequenz von Aktivitäten durchgeführt haben. Insgesamt haben wir circa 90 Stunden Sensordaten gesammelt und mithilfe von maschinellem Lernen analysiert.

Insgesamt war unser Inferenzangriff recht erfolgreich. Wir konnten die Anwesenheit von einer Person mit einer Erkennungsrate von über 90 Prozent bestimmen, je nach Standort und Position der Sensoren, was deutlich höher ist als das Raten (50 Prozent). Wir konnten zwischen vier Aktivitäten (Lesen, Stehen, Gehen und Arbeiten am Laptop) mit Erkennungsraten von über 55 Prozent unterscheiden, was ebenfalls deutlich besser ist als Raten (25 Prozent). Obwohl in einer kontrollierten Umgebung durchgeführt, haben unsere Experimente gezeigt, dass Raumklimadaten datenschutzrelevante Informationen preisgeben und zu einer Verletzung der Privatsphäre beitragen können.

Es wurde zwar noch nicht untersucht, ob den Verbraucherinnen und Verbrauchern die Inferenzmöglichkeiten aus den Raumklimadaten bewusst sind. Das Messen dieser Daten durch smarte Heizungssysteme passiert jedoch noch unauffälliger als das Aufzeichnen der oben erwähnten Audiodaten durch Sprachassistenten. Insoweit ist anzunehmen, dass das Bewusstsein für diese Art der Angriffe auf die Privatsphäre ebenfalls fehlt. Gleichzeitig ist die Weitergabe von Smart-Home-Daten an Anbieter und Dritte eine beliebte Idee und ein kontroverses Thema. So wurde in einer repräsentativen Befragung von 461 Erwachsenen aus den USA durch Pew Research Center (Rainie und Duggan 2016) den Teilnehmenden ein Szenario mit der Installation eines intelligenten Thermostats vorgeschlagen. Im Gegenzug für die Installation und die Ersparnis der Heizkosten würden die Befragten in diesem hypothetischen Szenario die Daten über einige Aktivitäten in ihrem Haus, beispielsweise wann Personen anwesend sind und wann sie sich von Raum zu Raum bewegen, mit dem Provider des Systems teilen. Dabei gaben 55 Prozent der Befragten an, dass dieses Szenario für sie nicht akzeptabel sei. Weitere 27 Prozent sagten, es sei akzeptabel, und die restlichen 17 Prozent antworteten: „Es kommt darauf an.“ Darüber hinaus sagten in einer weltweiten Umfrage mit 9.000 Befragten aus neun Ländern (Australien, Brasilien, Kanada, Frankreich, Deutschland, Indien, Mexiko, Großbritannien und den USA) 54 Prozent der Befragten, dass sie bereit wären, ihre persönlichen Daten, die von ihrem Smart Home gesammelt werden, gegen Geld mit Unternehmen zu teilen (Intel Security 2016).

Die Idee der smarten Heizungssysteme ist populär, sowohl aufgrund von Kostenersparnis als auch aufgrund der Umweltschonung durch bessere Energieeffizienz. Laut einer aktuellen repräsentativen Umfrage mit 1269 Teilnehmenden aus Deutschland verfügten im Jahr 2021 ca. 17 Prozent der Haushalte über ein smartes Heizungssystem (Bitkom e. V. 2021). Insoweit erscheint eine Auseinandersetzung der politischen Entscheidungsträger und des Verbraucherschutzes mit den möglichen Inferenzen aus Raumklimadaten unabdingbar. Wie detailliert dürfen diese Daten von Providern gemessen werden? Ab welchem Detailgrad sind diese Daten besonders schützenswert? Wie könnte ein Schutzprofil für smarte Heizsysteme aussehen?

Möglichkeiten für Inferenzangriffe auf die Privatsphäre mittels unscheinbaren IoT-Daten werden in der Zukunft weiter zunehmen. Es ist deswegen besonders wichtig, das Bewusstsein in der Gesellschaft dafür zu schärfen, dass potenziell alle IoT-Daten personenbezogen sind und geschützt werden sollen, auch wenn nicht unmittelbar klar ist, welche Inferenzen daraus technisch möglich sind. So wie für die oben erwähnten Smart-Metering-Systeme sollte auch für andere IoT-Anwendungen eine Balance gefun-

den werden zwischen der wertvollen Datenanalyse, die zur Verbesserung der Lebensqualität beiträgt, und der Tendenz, einfach „alles“ in beliebiger Granularität zu sammeln.

V. DIGITALE SELBSTBESTIMMUNG IN DER IOT-WELT

Das Internet der Dinge wird in Deutschland immer relevanter, insbesondere im Bereich Smart Home. Laut der im vorigen Kapitel zitierten Bitkom-Studie (Bitkom e. V. 2021) berichteten 2018 ca. 26 Prozent der Befragten über Smart-Home-Anwendungen in ihren Haushalten, 2021 waren es bereits ca. 41 Prozent der Befragten. Die vorigen Kapitel haben dargestellt, dass Sammlung und Verarbeitung der IoT-Daten, und insbesondere Sensordaten, in einer Quantität und Qualität passiert, die für Verbraucher intransparent und teilweise unsichtbar ist und unüberschaubare Konsequenzen nach sich ziehen kann.

Digitale Selbstbestimmung geht im IoT-Bereich jedoch noch einige Schritte weiter als Bewusstsein und Kontrolle über die eigenen Daten. Denn die IoT-Systeme, im Gegenteil zu Rechnern und Mobiltelefonen, werden oft gemeinsam verwendet. Darüber hinaus ist diese gemeinsame Nutzung praktisch nicht zu vermeiden. Die Forschung hat dokumentiert, dass in Haushalten normalerweise eine einzige Person, oft männlich und jung bis im mittleren Alter, die Rolle des „Administrators“ der IoT-Systeme einnimmt (Geeng und Roesner 2019). Alle anderen Personen im Haushalt, beispielsweise Lebenspartner, Kinder, Eltern oder Mitbewohner, sind der Wirkung dieser Systeme ausgesetzt. Ihr Mitspracherecht bei der Nutzung von IoT-Systemen ist entscheidend davon abhängig, wie insgesamt die Machtverhältnisse im Haushalt verteilt sind. In der Praxis können unterschiedliche Präferenzen, beispielsweise bezüglich Raumklima oder Lichtautomatisierung, zu Konflikten führen. Außerdem erlauben IoT-Geräte eine unauffällige Beobachtung der An- und Abwesenheiten von Partnern und Kindern, ihre Unterhaltungen und Aktionen. Dieses Machtgefälle (power imbalance) kann in schlimmsten Fällen häusliche Gewalt begünstigen, was zu Handlungsaufrufen zu entsprechenden Designrichtlinien für Smart-Home-Anwendungen geführt hat (McKay und Miller 2021). Aufgrund der Neuartigkeit dieses Themas sind jedoch IoT-Systeme, die diesen Richtlinien genügen, nach unserem besten Wissen noch nicht vorhanden, bis auf wenige Ideen und Prototypen in der internationalen Forschung (He et al. 2018, Zeng und Roesner 2019, Sikder et al. 2020).

Nicht nur Personen, die permanent im Haushalt wohnen, nutzen Smart-Home-Systeme mehr oder weniger aktiv, und mehr oder weniger bewusst. Auch temporäre Besucher und Dienstleistende, wie zum Beispiel Freunde, Nachbarn, Gäste, Haushaltshilfen, Handwerker, Babysitter und Postboten, kommen mit IoT-Systemen in Kontakt und nutzen sie, üblicherweise passiv, und manchmal unfreiwillig oder unbemerkt (Yao et al. 2019, Marky et al. 2020, Cobb et al. 2021). Diese gelegentlichen Nutzer und Nutzerinnen geben an, dass sie sich nicht ganz wohl in der Gegenwart von Smart-Home-Geräten fühlen, signalisieren jedoch auch eine gewisse Resignation gegenüber ihren Möglichkeiten, ihre Daten in dieser Situation zu schützen, auch nicht zuletzt, weil sie befürchten, dass das zu viel Zeit und Aufwand kosten würde. Die Besitzer der Smart-Home-Geräte wiederum wären im Prinzip bereit, die Datenschutzpräferenzen der Unbeteiligten zu berücksichtigen, befürchten jedoch, dass die Änderungen der Einstellungen, die eventuell schon vorher sorgfältig auf die Einwohner kalibriert wurden, sich zu

ihrem Nachteil auswirken könnten. Insgesamt gibt es noch recht wenige Ideen dazu, wie diese widersprüchlichen Anforderungen umgesetzt werden könnten.

VI. FAZIT UND HANDLUNGSEMPFEHLUNGEN

Nicht nur die Kontrolle über die Menge und die Arten der gesammelten Daten spielt für die digitale Selbstbestimmung im Internet der Dinge eine Rolle, sondern auch mögliche Inferenzen aus diesen Daten, und insbesondere die Nutzung der IoT-Systeme von mehreren Menschen gemeinsam. Mitnutzende können unterschiedliche, teilweise widersprüchliche oder aufgrund von Machtgefälle nicht realisierbare Datenschutzpräferenzen haben. Wie und ob diese Präferenzen berücksichtigt werden können, ist eine offene Forschungsfrage und eine Herausforderung für Industrie, Verbraucherschutz und Politik. Es ist daher auch nicht klar, wie in dieser Situation Datenintermediäre tätig werden können, und ob sie helfen können.

Folgende Handlungsempfehlungen können als Hilfe bei Kaufentscheidungen und Nutzung von IoT-Systemen umgesetzt werden:

1. **Datenflüsse in IoT-Systemen und Funktionsweise ohne Internet.** Es sollen Möglichkeiten geschaffen werden, die die Verbraucher zuverlässig (nicht auf freiwilliger Basis), verständlich und zum richtigen Zeitpunkt (am besten vor und während der Kaufentscheidung) darüber informieren, welche Datenflüsse in einem IoT-System existieren und welche nicht. Besonders wichtig sind Informationen darüber, ob die IoT-Geräte ohne eine Internetverbindung betrieben werden können, und welche eventuellen Auswirkungen das auf die Funktionalität der Systeme haben könnte. Ein guter Ansatz dafür wären entsprechende Labels mit weiterführenden Informationen auf einer vertrauenswürdigen Webseite, ähnlich zu dem von der Mozilla Foundation online betriebenen Kaufleitfaden „privacy not included“ (Mozilla 2021).
2. **Bewusstsein und Richtlinien für Inferenzen aus den Daten.** Es ist zwar wichtig zu wissen, welche Daten von IoT-Systemen gesammelt werden, aber es ist noch wichtiger zu wissen, welche Inferenzen aus diesen Daten möglich sind, und ob es gesetzlich erlaubt oder verboten ist, diese Inferenzen zu bestimmen. Schutzprofile und andere Richtlinien für gängige Datentypen in IoT-Systemen können dabei helfen, dass sich nur solche Systeme auf dem Markt durchsetzen, die die Möglichkeit der Inferenzen minimieren (privacy by design), ohne auf die entsprechende Funktionalität verzichten zu müssen.
3. **Systeme für mehrere (Haupt-)Nutzer.** Es soll bei der Kaufentscheidung leicht und zuverlässig feststellbar sein, ob die IoT-Systeme eine gemeinsame Nutzung mithilfe von dedizierten Accounts zulassen, und ob es möglich ist, mehr als einen Account mit Administratorrechten einzurichten (Hauptnutzer-Account). Die soziale Realität in Haushalten benötigt mehrere Hauptnutzer, die sich miteinander bezüglich ihrer Präferenzen bei der IoT-Nutzung ähnlich absprechen müssen wie bei der Nutzung von anderen gemeinsamen Ressourcen, wie beispielsweise Geld, Autos und Urlaubszeiten und -orte. Dabei kann man die Gefahr eines Machtgefälles zwar nicht vermeiden, jedoch sollten Systeme mit einem einzigen Hauptnutzer-Account nicht automatisch ein solches Machtgefälle schaffen. Außerdem werden auch Accounts mit Steuerungsmöglichkeiten für

andere Mitbenutzer benötigt, wie beispielsweise Kinder, Haushaltshilfen und Gäste.

Um die obigen Empfehlungen auf empirischer Basis umsetzen zu können, besteht Forschungsbedarf in folgenden Bereichen:

1. **Systematische Auswertung der Inferenzangriffe auf IoT-Systeme und evidenzbasierte Erstellung der Richtlinien.** Für die meisten Datentypen, die in IoT-Systemen verarbeitet werden, ist es weitgehend unbekannt, ab welcher Menge und Granularität sie durch Inferenzangriffe eine Gefahr für die Privatsphäre darstellen. Andererseits ist auch unbekannt, ab wann die Datensparsamkeit eine Grenze überschreitet, sodass eine Anpassung an die Nutzer nicht mehr möglich ist. Dieser Kompromiss soll experimentell untersucht werden, um evidenzbasierte Richtlinien für die Datensparsamkeit in IoT-Systemen zu erstellen.
2. **Gebrauchstaugliche Labels und andere Kaufentscheidungshilfen.** Entscheidungshilfen für Verbraucher sollen nicht nur die verfügbaren Informationen auf einer technischen Ebene darstellen. Auch hier sollte das Prinzip der evidenzbasierten Forschung gelten: Jegliche Labels, Webportale und ähnliche Objekte sollen mit den Mitteln der Human-Computer-Interaction entwickelt und auf Verständlichkeit, Nützlichkeit und Praktikabilität evaluiert werden. Sonst würde sie sehr wahrscheinlich ein Schicksal ereilen, das dem Secure Messaging Scorecard (EFF 2017) zuteilwurde: Diese wohlgemeinte, von Experten sorgfältig erstellte Entscheidungshilfe zur Wahl der sicheren Messenger-Apps hat sich als völlig unverständlich für diejenigen herausgestellt, für die sie erstellt wurde: nichtfachkundige Nutzerinnen und Nutzer (Abu-Salma et al. 2017).
3. **Datenschutzkonzepte für Mitbenutzer der IoT-Systeme.** Wie im vorigen Kapitel dargestellt, ergeben sich in der IoT-Welt neuartige Datenschutzprobleme dadurch, dass die IoT-Systeme von mehreren Parteien mit unterschiedlichen, teilweise kollidierenden Datenschutzpräferenzen und Bedürfnissen benutzt werden. Die Entwicklung geeigneter Datenschutzkonzepte für diese Konstellation ist eine offene Forschungsfrage, die weiter untersucht werden sollte.

VII. ABBILDUNGSVERZEICHNIS

VIII. LITERATURVERZEICHNIS

Abdi, Noura, Kopo M. Ramokapane und Jose M. Such. 2019. More than smart speakers: Security and privacy perceptions of smart home personal assistants. In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 451–466. Santa Clara, CA, USA: USENIX Association, August. https://www.usenix.org/conference/soups2019/presentation/abdi (Zugriff: 17.02.2022).

Abu-Salma, Ruba, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina und Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In: *2017 IEEE Symposium on Security and Privacy (SP)*, 137–153. San Jose, CA, USA: IEEE, Mai. https://doi.org/10.1109/SP.2017.65.

Ashton, Kevin. 2009. That ‘internet of things’ thing. *RFID Journal* 22, Nr. 7: 97–114. https://www.rfidjournal.com/that-internet-of-things-thing (Zugriff: 17.02.2022).

Bitkom e.V. 2021. Das intelligente Zuhause: Smart Home 2021. Ein Bitkom-Studienbericht. Oktober. Berlin: Bitkom. https://www.bitkom.org/Bitkom/Publikationen/Das-intelligente-Zuhause-Smart-Home-2021 (Zugriff: 15. Februar 2022).

BSI (Bundesamt für Sicherheit in der Informationstechnik). 2014. Protection profile for the gateway of a smart metering system (smart meter gateway PP) BSI-CC-PP-0073-2014. Bonn: BSI. https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0073.html (Zugriff: 17.02.2022).

Cobb, Camille, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. 2021. „I would have to evaluate their objections“: Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies*, Nr. 4: 54–75.

EFF (Electronic Frontier Foundation). 2017. Secure Messaging Scorecard https://www.eff.org/pages/secure-messaging-scorecard (Zugriff: 15. Februar 2022).

Geeng, Christine und Franziska Roesner. 2019. Who’s in control?: Interactions in multi-user smart homes. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–13. Glasgow: ACM, 2. Mai. https://doi.org/10.1145/3290605.3300498.

Haney, Julie M., Susanne M. Furman und Yasemin Acar. 2020. Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In: *HCI for Cybersecurity, Privacy and Trust*, hg. von Abbas Moallem, 393–411. Lecture Notes in Computer Science 12210. Cham: Springer. https://doi.org/10.1007/978-3-030-50309-3_26.

Harper, Scott, Maryam Mehrnezhad und John C. Mace. 2021. User privacy concerns and preferences in smart buildings. In: *Socio-Technical Aspects in Security and Trust*, hg. von Thomas Groß und Luca Viganò, 85–106. Lecture Notes in Computer Science 12812. Cham: Springer. https://doi.org/10.1007/978-3-030-79318-0_5.

Hart, George W. 1989. Residential energy monitoring and computerized surveillance via utility power flows. *IEEE Technology and Society Magazine* 8, Nr. 2: 12–16. https://doi.org/10.1109/44.31557.

He, Weijia, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes und Blase Ur. 2018. Rethinking access control and authentication for the home internet of things (iot). In: *27th USENIX Security Symposium (USENIX Security 18)*, 255–272. Baltimore, MD: USENIX Association, August. https://www.usenix.org/conference/usenixsecurity18/presentation/he (Zugriff: 17.02.2022).

Intel Security. 2016. Intel security's international internet of things smart home survey shows many respondents sharing personal data for money. https://newsroom.intel.com/newsreleases/intel-securitys-international-internet-of-things-smart-home-survey (Zugriff: 15. Februar 2022).

Kröger, Jacob Leon, Leon Gellrich, Sebastian Pape, Saba Rebecca Brause und Stefan Ullrich. 2022. Personal information inference from voice recordings: User awareness and privacy concerns. *Proceedings on Privacy Enhancing Technologies*, Nr. 1: 6–27. https://doi.org/10.2478/popets-2022-0002.

Langheinrich, Marc. Privacy in Ubiquitous Computing. 2009. In: Ubiquitous computing fundamentals, hg. von John Krumm, 109–174. New York: Chapman and Hall/CRC. https://doi.org/10.1201/9781420093612.

Lau, Josephine, Benjamin Zimmerman und Florian Schaub. 2018. Alexa, are you listening? Pivacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (November): 1–31. https://doi.org/10.1145/3274371.

Malkin, Nathan, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman und David Wagner. 2019. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies*, Nr. 4: 250–271. https://doi.org/10.2478/popets-2019-0068.

Marky, Karola, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder und Max Mühlhäuser. 2020. "I don't know how to protect myself": Understanding privacy perceptions resulting from the presence of bystanders in smart environments. In: *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, 1–11. Tallinn Estonia: ACM, 25. Oktober. https://doi.org/10.1145/3419249.3420164.

McKay, Dana und Charlynn Miller. 2021. Standing in the way of control: A call to action to prevent abuse through better design of smart technologies. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–14. Yokohama, Japan: ACM, 6. Mai. https://doi.org/10.1145/3411764.3445114.

Molina-Markham, Andrés, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet und David Irwin. 2010. Private memoirs of a smart meter. In: *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building - BuildSys '10*, 61-66. Zurich, Switzerland: ACM Press. https://doi.org/10.1145/1878431.1878446.

Morgner, Philipp, Christian Müller, Matthias Ring, Björn Eskofier, Christian Riess, Frederik Armknecht und Zinaida Benenson. 2017. Privacy implications of room climate data. In: *Computer Security – ESORICS 2017*, hg. von Simon N. Foley, Dieter Gollmann und Einar Snekkenes, 10493:324–343. Lecture Notes in Computer Science. Cham: Springer. https://doi.org/10.1007/978-3-319-66399-9_18.

Mozilla Foundation. 2021. Privacy not included buyer's guide. https://foundation.mozilla.org/en/privacynotincluded (Zugriff: 15. Februar 2022).

Rainie, Lee und Maeve Duggan. 2016. Pew Research: Privacy and Information Sharing. http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing (Zugriff: 15. Februar 2022).

Reinhardt, Andreas, Frank Englert, and Delphine Christin. Averting the privacy risks of smart metering by local data preprocessing. *Pervasive and Mobile Computing* 16: 171–183. https://doi.org/10.1016/j.pmcj.2014.10.002.

Rial, Alfredo und George Danezis. 2011. Privacy-preserving smart metering. In: *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society - WPES '11*, 49–60. Chicago, IL, USA: ACM Press. https://doi.org/10.1145/2046556.2046564.

Sikder, Amit Kumar, Leonardo Babun, Z. Berkay Celik, Abbas Acar, Hidayet Aksu, Patrick McDaniel, Engin Kirda und A. Selcuk Uluagac. 2020. Kratos: Multi-user multi-device-aware access control system for the smart home. In: *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 1–12. Linz, Austria: ACM, 8. Juli. https://doi.org/10.1145/3395351.3399358.

Weiser, Mark. 1991. The Computer for the 21st Century. *Scientific American* 265, Nr. 3: 94–105.

Yang, Weining, Ninghui Li, Yuan Qi, Wahbeh Qardaji, Stephen McLaughlin und Patrick McDaniel. 2012. Minimizing private data disclosures in the smart grid. In: *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12*, 415–427. Raleigh, NC, USA: ACM Press. https://doi.org/10.1145/2382196.2382242.

Yao, Yaxing, Justin Reed Basdeo, Oriana Rosata Mcdonough und Yang Wang. 2019. Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction* 3, Nr. CSCW: 1–24. https://doi.org/10.1145/3359161.

Zeng, Eric und Franziska Roesner. 2019. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study. In: *28th USENIX Security Symposium (USENIX Security 19)*, 159–176. Santa Clara, CA, USA: USENIX Association, August. https://www.usenix.org/conference/usenixsecurity19/presentation/zeng (Zugriff: 17.02.2022).

Zeng, Eric, Shrirang Mare und Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 65–80. Santa Clara, CA, USA: USENIX Association, Juli. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng (Zugriff: 17.02.2022).