

Einfache Sensoren, komplexe Folgen: Privatheit als soziale Praxis im vernetzten Haushalt

Tanja Lehmann, Franziska Baum, Albrecht Kurze, Arne Berger und Andreas Bischof

Zusammenfassung

Smart-Home-Systeme wie Kühlschränke, Thermostate und Rauchmelder bringen eine Vielzahl an Sensoren in die Häuslichkeit. Deren Funktionsweisen und Dimensionen der Datenerfassung sind häufig unbekannt. Eine Auseinandersetzung mit den Sensoren des *Smart Homes* und ihren Daten ist in Privatheitsdiskursen noch selten. Vor diesem Hintergrund zeigt der Artikel, dass *Smart-Home*-Sensoren (z. B. Temperatur, Luftfeuchte, Helligkeit, Bewegung, Lautstärke) erhebliche Implikationen für Privatheit im (in der Regel geteilten) Zuhause haben. In Haushalten werden diese Daten routinemäßig mit Alltagswissen verknüpft und zu Geschichten über Anwesenheit, Rhythmen, Aktivitäten oder Abweichungen verdichtet; Messwerte erhalten dadurch soziale Bedeutung und autoritativen Status. Das ermöglicht laterale Überwachung, Normdurchsetzung und Konflikte, auch ohne bössartige Absicht und verstärkt Informationsasymmetrien zwischen primären Administrator:innen und sekundären Nutzer:innen (Kinder, Partner:innen, Besucher:innen, Dienstleister:innen). Der Beitrag schlägt daher vor, Privatheit als relationalen Aushandlungsraum zu verstehen und zu gestalten. Methodisch nutzt die Studie, auf der dieser Beitrag wesentlich aufbaut, ein *Sensorkit*, das über zwei Wochen in Haushalten Daten erhebt, auf einem Tablet visualisiert und diese Daten in Aufgaben, Interviews sowie Gruppendiskussionen partizipativ interpretieren lässt. Die Auswertung der Interviews und Gruppendiskussionen erfolgt qualitativ-inhaltsanalytisch in Gruppeninterpretationen der interdisziplinären Forschendengruppe. So werden Interpretierbarkeit, Machtpraktiken, Akteurskonstellationen und mentale Modelle von Nutzer:innen und Betroffenen solcher nicht-audiovisueller Sensorik sichtbar. Daraus folgen Design- und Nutzungsempfehlungen: rollenbasierte Zugriffsrechte, transparente Datenerfassung, Zweckbindung, datensparsame Defaults, lokale Speicherung, einfache Pausen-/Löschfunktionen, sowie Aushandlungs- und Bildungsfor-

mate und regulatorische Mindeststandards, um Privatheit im vernetzten Zuhause situativ zu stabilisieren und Machtmissbrauch im Nahfeld wirksam vorzubeugen.

1. Einleitung

Das Zuhause gilt seit jeher als besonders geschützter Raum der Privatheit. Mit der zunehmenden Verbreitung von *Smart-Home*-Technologien gerät diese Sphäre unter Druck. *Smart-Home*-Systeme basieren ganz wesentlich auf Sensoren und der Erfassung verschiedener Umweltparameter. Solche Sensoren, die u. a. Temperatur, Luftfeuchtigkeit, Helligkeit oder Bewegung erfassen, erscheinen zunächst trivial und technisch unproblematisch, da sie auf den ersten Blick keine personenbezogenen Informationen liefern. Gleichwohl ermöglichen gerade diese scheinbar simplen Daten Rückschlüsse auf An- und Abwesenheiten, Routinen und Aktivitäten der Haushaltsmitglieder, insbesondere wenn sie im Zusammenspiel mit alltäglichen Praktiken interpretiert werden. Daten, die technisch neutral wirken, erhalten durch ihre soziale Einbettung eine privatheitsrelevante Bedeutung und können normative Bewertungen, Kontrolle oder Konflikte im Alltag hervorrufen (Fischer u. a. 2016; Morgner u. a. 2017; Tolmie u. a. 2016).

Eine exemplarische Episode verdeutlicht die Risiken solcher Datenpraktiken: Eine Teilnehmerin einer unserer Studien (s. u.) nutzte Sensordaten, um die Angaben ihres Partners zu überprüfen, der behauptet hatte, direkt nach der Arbeit in den Garten gegangen zu sein. Die Sensoren zeigten jedoch, dass er die Wohnung nicht verlassen hatte. Die Teilnehmerin konfrontierte ihn mit der Diskrepanz, ohne zu erklären, wie sie die Informationen erlangt hatte, wodurch der asymmetrische Informationszugang wirksam wurde. Dieses Beispiel illustriert, wie selbst einfache Sensordaten laterale Überwachung, d. h. die Überwachung eines Haushaltsmitglieds durch ein anderes, ermöglichen und Fehlinterpretationen hervorrufen können, die Privatheit und Sicherheit im Zuhause direkt beeinflussen (Kurze u. a. 2020; Richter u. a. 2018).

Privatheit muss im *Smart Home* daher als sozialer Aushandlungsraum verstanden werden, in dem verschiedene Akteure, wie Bewohner:innen, Besucher:innen, Vermieter:innen, Hersteller und Plattformen bzw. *Service-provider*, interagieren. In diesen komplizierten Akteurskonstellationen manifestieren sich Informationsasymmetrien und Konflikte, die vor allem über Kontrolle über Sensoren und den Zugang zu Daten verhandelt werden. Ins-

besondere Nutzer:innen, die Daten erzeugen, ohne Zugriff auf die *Smart-Home*-Daten zu erhalten, laufen Gefahr, in ihren Handlungsspielräumen eingeschränkt, überwacht oder sogar Opfer von Gewalt und Straftaten aus dem Nahfeld zu werden. *Smart-Home*-Systeme und die darin verbauten Sensoren verstärken und institutionalisieren somit soziale Machtverhältnisse im Zuhause.

Das Verbundprojekt *Simplications*¹ untersucht vor diesem Hintergrund die gesellschaftlichen und technischen Implikationen vermeintlich einfacher Sensordaten, wie sie häufig in *Smart-Home*-Systemen verbaut sind, deren Nutzung nicht intendierte bis potenziell „böartige“ Effekte entfalten kann (Kurze u. a. 2020; Kurze/Bischof 2021). Diese negativen Effekte entstehen nicht allein aus technischen Funktionsweisen oder ökonomischen Interessen „von außen“ (Saqib u. a. 2025), sondern aus der Verflechtung von Sensortechnologie, Nutzungspraxis, sozialen Beziehungen und interpretativen Praktiken. *Simplications* verfolgt zu deren Rekonstruktion einen interdisziplinären Ansatz, der Soziologie, *Human-Computer-Interaction* (HCI), Design und Medienbildung miteinander verknüpft. Von Interesse sind dabei folgende Fragen:

- Welche konkreten Konflikte und Informationsasymmetrien entstehen durch *Smart-Home*-Datenpraktiken innerhalb von Haushalten?
- Welche Konsequenzen bzw. *Implications for Use* ergeben sich daraus für eine informierte, souveräne Nutzung durch verschiedene Typen von Nutzer:innen?
- Welche *Implications for Design* ergeben sich für die bessere Ausgestaltung von diesen und ähnlichen Technologien?

Das Studiendesign verfolgt dabei einen Ansatz von *Privacy by Co-Design* und fragt gemeinsam mit Nutzer:innen danach, wie aus der Perspektive der tatsächlichen Anwendungen Perspektiven zur Ergänzung von *Privacy by Design* entwickelt werden können². Die gewonnenen Erkenntnisse fließen in die Entwicklung mediendidaktischer Formate ein, sodass technische Potenziale und soziale Praktiken gleichzeitig adressiert werden.

1 Das Projekt wurde vom BMFTR im Rahmen der Plattform Privatheit/ Vernetzung und Sicherheit digitaler Systeme gefördert (FKZ 16KIS1868K, Laufzeit: 06.2023 bis 12.2026). Projektpartner: Technische Universität Chemnitz, Hochschule Anhalt, Verbraucherzentrale Sachsen e. V., Leipzig.

2 Der Unterschied zwischen *Privacy by Design* und *Privacy by Co-Design* besteht in erster Linie darin, die Nutzenden in die Technikentwicklung einzubeziehen und nicht nur die *Developer*, vgl. Abschnitt 2, Forschungsstand.

Im vorliegenden Beitrag werden zunächst zentrale Forschungsbefunde zum Thema *Smart Home* und Privatheit mit Relevanz für die genannten Fragestellungen vorgestellt (2). Darauf aufbauend erfolgt die Erläuterung der methodischen Umsetzung der Studie. Es wird beschrieben, wie durch ein *Sensorkit* zur Erhebung einfacher Daten, Anwendungspraxen und idealen Einsatz- und Designvorstellungen in partizipativen Feldstudien erhoben wurden (3). Anschließend werden die Ergebnisse der Studie gegliedert nach vier zentralen Dimensionen präsentiert. Zunächst wird dargestellt, wie Sensordaten von Nutzer:innen interpretiert werden und welche Inferenzpotenziale sich daraus ergeben. Darauf folgt die Analyse, wie und wofür Daten als Ressource für soziale Kontrolle innerhalb von Haushalten genutzt werden. Im Anschluss werden Akteurskonstellationen betrachtet und die damit verbundene Diffusion von Verantwortung analysiert, bevor die Rolle von Privatheitsvorstellungen und des Problembewusstseins für die Nutzung und Reflexion von Sensordaten diskutiert wird (4). Aufbauend auf diesen Befunden erfolgt anschließend die Ableitung der Implikationen für eine informierte Anwendung und Design. Diese umfassen Empfehlungen für die Gestaltung technischer Systeme, Hinweise für einen informierten Einsatz im Alltag, Ansätze für Transfer und Intervention sowie möglicher Regulierungsansätze (5). Den Abschluss bildet eine Zusammenfassung der zentralen Erkenntnisse, in der die praktische Relevanz reflektiert und gezeigt wird, wie Technik, Nutzungspraxis und Bildung zusammenwirken, um die Privatheit im *Smart Home* relational und situativ zu stabilisieren (6).

2. Forschungsstand

Der aktuelle Forschungsdiskurs in der HCI zeigt, dass Privatheit im *Smart Home* zunehmend als situatives und relationales Phänomen verstanden werden muss. Frühere Studien konzentrierten sich vor allem auf abstrakte Datenschutzfragen und individuelle Einstellungen, sogenannte Datenschutzbedenken (*privacy concerns*) und die Identifikation von Nutzer:innen-Typen. Jüngere Studien diversifizieren zunehmend Typologien von Nutzer:innen und Abstufungen von Betroffenheit und Einfluss (Saqib u. a. 2025). Die Autor:innen unterscheiden beispielsweise zwischen Eigentümer, Hauptnutzer (*primary user*) und Beteiligten (*bystander*). *Bystander* werden weiter unterteilt in Besuchende, wie Gäste und Hausangestellte, im Haushalt lebende Personen wie Partner:in und Kinder und nicht involvierte Umstehende wie Nachbarn. Studien, die sich mit Genderfragen im

Smart Home befassen, stellen zudem die spezifischen Schwachstellen von Forschung und Entwicklung heraus, die ihren Fokus ausschließlich auf anschaffende und initialisierende Nutzer:innen – die Hauptnutzer:innen – legen (Lopez-Neira u. a. 2019, Schulz u. a. 2023). Während der Begriff der *bystander* zuletzt öfter aufgegriffen wurde, ist die Bezeichnung „sekundäre Nutzer:innen“ passender, da er den Grad der Betroffenheit von Haushaltsmitgliedern und Besuchenden, sowie deren Rolle für (oftmals nicht stattfindende) Aushandlungsprozesse aktiver setzt (Schulz u. a. 2023). Das problematische Verhältnis aus Betroffenheit bei mangelndem Bewusstsein für problematische Implikationen von *Smart-Home*-Systemen für die eigene Rolle bilden Studien ab, die (falsche) mentale Modelle von Nutzer:innen als Gefahr für Privatheit markieren (Marky u. a. 2021). Auf Grundlage einer Literaturübersicht identifizierten Saqib u. a. (2025) zehn spezifische Datenschutzbedenken sekundärer Nutzer:innen. Als häufigste Befürchtungen wurden bewusste Geheimhaltung, mangelndes Bewusstsein über die Implikationen der Daten, fehlende oder eingeschränkte Kontrolle, fehlende Einwilligung, Datenmissbrauch, auch für Belästigung oder diskriminierende oder unfaire Behandlung, Manipulation von Werten, die Datenverarbeitung durch Hersteller, sowie externe Bedrohungen rekonstruiert (ebd.).

Die HCI-Forschung zu *Data Legibility* und *Sense-Making* innerhalb von Haushalten zeigt, dass Menschen aus Sensordaten Rückschlüsse auf Ereignisse ziehen, die über den unmittelbaren Messzweck hinausgehen – und dass auch Fehlinterpretationen dabei eine zentrale privatheitsrelevante Rolle spielen (Fischer u. a. 2016; Kurze u. a. 2020; Tolmie u. a. 2016). Die oben angesprochenen Bedenken der sekundären Nutzer:innen sind also durchaus berechtigt. Selbst vermeintlich einfache Sensoren erzeugen komplexe Inferenzpotenziale. Bewegungs-, Temperatur- oder Luftfeuchtigkeitsdaten erlauben Rückschlüsse auf Anwesenheit, Schlafrhythmen, Alltagsaktivitäten oder Besuchsmuster. Forschungsarbeiten zum Einsatz und zur Nutzung von Sensoren zeigen, dass diese Daten jenseits ihres Messzwecks nutzbar sind und durch Kontextwissen und moralische und normative Ordnungen im Haushalt erst Bedeutung erhalten (Laput u. a. 2017). Diese Bedeutungszuweisungen sind entscheidend für Konflikte und Informationsasymmetrien im häuslichen Alltag. Die Interpretation vermeintlich einfacher Daten ist also nicht technisch determiniert, sondern entsteht im Zusammenspiel von Alltagspraxis, sozialen Normen und individuellen Deutungsmustern (Kurze/Bischof 2021; Morgner u. a. 2017).

Ein weiterer Schwerpunkt der Forschung an der Schnittstelle von Soziologie, *Gender Studies* und HCI liegt auf Macht, Kontrolle und potenziel-

ler digital vermittelter Gewalt im zunehmend vernetzten Zuhause (Lopez-Neira u. a. 2019; Tanczer 2021). Die Sensordaten ermöglichen laterale Überwachung und die subtile Kontrolle von Haushaltsmitgliedern. Die Forschung zu *Gender* und *Internet of Things* zeigt, dass insbesondere sekundäre und vermeintlich passive Nutzer:innen, die Daten erzeugen, ohne in die Nutzung eingebunden zu sein, eingeschränkte Handlungsspielräume haben und potenziell kontrolliert werden können (Marky u. a. 2020; Richter u. a. 2018). Fälle häuslicher Gewalt oder zwanghafte Kontrolle zeigen die Tragweite solcher daten-vermittelter Informationsasymmetrie, die zur Machtressource wird: *Smarte* Geräte eignen sich insbesondere für methodische psychische Gewalt wie *Gaslighting* (Tanczer 2021). Weniger intentional hat soziologische Forschung zu Subjektivierung durch und mit Technik gezeigt, dass intime Überwachung zur Normalität wird, so dass z. B. Kinder und deren Nannys selbstverständlich überwacht werden (Dereymaeker u. a. 2024; Lupton 2016; Mascheroni 2020; Rogers u. a. 2023). Eltern, Partner:innen oder technisch versiertere Haushaltsmitglieder geraten in die Position des permanenten Beobachtens. Das Zuhause wird als Schutzraum definiert, in dem vernetzte Technik den Nutzer:innen eine Ressource bieten, um persönliche Sicherheit durch Überwachung herzustellen – die „sorgende Konsumentin“ wird zur Leitfigur und Überwachung als Sorgepraxis verstanden (Stark/Levy 2018; Mascheroni 2020). So entstehen gerade im Familienalltag und ohne intentional bössartigen Einsatz von Sensorik Grauzonen, in denen Komfort, Kontrolle und normative Bewertungen von Verhalten miteinander verknüpft werden. *Simplications* richtet den Fokus genau auf diese Grenzbereiche zwischen unbedarften Einsatz und problematischer Anwendung.

Die Unterstützung informierter Nutzung und differenzierter Einwilligungsmöglichkeiten hat sich als weiteres Diskursfeld zwischen Verbrauch erforschung und HCI etabliert. So wurden bereits verschiedene Varianten zur Sichtbarmachung von Privatheitsrisiken vorgeschlagen. *Privacy Labels*, bzw. *Label* zur Produktbewertung, enthalten häufig zumindest eine *Privacy*-Komponente (u. a. Caven u. a. 2024; Garg 2021; Ramokapane u. a. 2024; Reinhardt/Railean 2020). Daneben gibt es *community*-basierte bzw. *Co-Design*- Ansätze (Adryan 2015), wie auch das *Open IoTmark* (später *Better IoTmark*) von Deschamps-Sonsino (2018) oder das *ThingsCon/Mozilla Open IoT Studio „Trustmark for IoT“* (Bihr 2017). All diesen Vorschlägen ist gemeinsam, dass sie zwar Nutzer:innen- und Design-Perspektiven einbinden, aber bisher nicht über das Stadium eines konzeptionellen Vorschlags

hinausgekommen sind, und noch keinen Eingang in Produkte und Services rund um das *Smart Home* gefunden haben.

Partizipative Forschung und datenbasierte Reflexion haben sich als zentrale methodische Ansätze vor allem in der HCI erwiesen, um die privatsphärenrelevanten Implikationen von *Smart-Home*-Sensordaten sichtbar und erfahrbar zu machen und auch *IoT* bzw. *Privacy Labels* zu gestalten. Im Kontext von *Privacy-by-Co-Design* werden Nutzer:innen aktiv in die Interpretation eigener Daten einbezogen, wodurch nicht nur Problembewusstsein und Reflexion gefördert werden, sondern auch normative Annahmen über angemessenes Verhalten und Kontrolle im Haushalt aufgedeckt werden. Methoden wie *Design Fiction*, *Critical Design* oder praxisnahe Bildungsformate zeigen, dass die unmittelbare Erfahrung von Daten, ihre Visualisierung, Annotation und die gezielte Irritation durch widersprüchliche Szenarien wirksamer sind als rein kognitive Aufklärung. Solche Interventionen eröffnen Räume, in denen Nutzer:innen ihre mentalen Modelle prüfen, die Wahrnehmung von Risiken und Machtbeziehungen reflektieren und Rückschlüsse für die eigene Praxis ziehen können. Studien im HCI- und Design-Kontext zeigen, dass solche Formate nicht nur die Interpretation und Sensibilisierung erleichtern, sondern auch konkrete Hinweise für Gestaltung, *Usability* und mediendidaktische Anwendungen liefern (Köpferl u. a. 2024; Mucha u. a. 2022). *Co-Design* für Privatheit besteht dabei zumeist auf der Entwicklung von gewünschten oder besser passenden Anwendungsszenarien und Interfaces, wobei die Teilnehmenden in der Regel Verbraucher:innen sind (Leitão 2019; Yao u. a. 2019; Jin u. a. 2022; Hahn u. a. 2024; Zufferey u. a. 2024; Wang u. a. 2025). Forschung, die Privatsphäre-Implikationen partizipativ untersucht, zeigt aber, dass das Bewusstsein für problematische Daten und Konstellationen sowie der eigenen Betroffenheit auch in solchen Kontexten nicht allen Studienteilnehmer:innen klar ist. Vielmehr zeigen unsere Vorarbeiten, dass die Verquickung aus technischer Datensammlung, Wissen über Haushaltsaktivitäten und eine intersubjektive Rekonstruktion in der Gruppe ein informiertes *Privacy-by-Co-Design* ermöglichen (Kurze u. a. 2020, 2025).

Insgesamt verdeutlicht die Forschung die Notwendigkeit eines integrativen Ansatzes, der technische Gestaltung, Nutzungspraxis und partizipative Reflexion kombiniert. Rein technische Lösungen reichen nicht aus, um Privatheit im *Smart Home* zu sichern, da Daten immer relational und situativ interpretiert werden. Bisher beziehen sich *Co-Design Workshops* auf den Gebrauch von Kameras und *Smart Speaker* und nicht auf die vermeintlich weniger privatsphärenrelevante Sensorik des *Smart Homes* (Becker u. a.

2025; Saqib u. a. 2025). Diese Erkenntnisse bzw. Forschungslücken bilden die Grundlage für die Konzeption unseres Studiendesigns, welches wir seit 2017 in mehreren Iterationen entwickelt haben, wie wir im nächsten Abschnitt erläutern.

3. Erforschbarkeit von Datenpraktiken im Smart Home: *Sensorkit* und Studiendesign

Für die empirische Forschung ergeben sich durch *Smart-Home*-Systeme methodische Herausforderungen. Es reicht nicht aus, technische Systeme isoliert auf ihr Gefahrenpotenzial zu analysieren oder hypothetische Szenarien abzufragen. Um die sozialen Implikationen von Sensordaten aus dem Zuhause zu untersuchen, müssen Datenpraktiken im tatsächlichen häuslichen Alltag erhoben werden und zugleich Möglichkeiten geschaffen werden, die Interpretationen und Aushandlungen der Nutzer:innen sichtbar machen zu können. Vor diesem Hintergrund wurde ein Forschungsansatz entwickelt, der Datenerhebung, Visualisierung und partizipative Analyse miteinander verbindet.

Kommerzielle *Smart-Home*-Systeme sind hierfür nur eingeschränkt geeignet. Rohdaten sind meist nicht ohne Weiteres zugänglich, sie werden proprietär und an externe Server übermittelt, wodurch forschungsethische Risiken entstehen. Um diese Abhängigkeiten zu vermeiden, wurde eine eigenständige Forschungsinfrastruktur entwickelt, die Erhebung, Visualisierung und Reflexion von Sensordaten in einem geschlossenen System vereint und vollständig unter Kontrolle der Teilnehmenden lässt.

Das Forschungsdesign zielt auf die Erhebung von diversen Konstellationen und Perspektiven, die in der Forschung noch selten empirisch erhoben wurden.

3.1 Erhebungsinstrument *Sensorkit*

Zentrales Instrument der Forschungen im Projektkontext ist ein *Sensorkit*, ein kleines, einfach zu installierendes Set aus vernetzten, batteriebetriebenen technisch einfachen Sensoren, das über rund zwei Wochen in Haushalten eingesetzt wird. Das *Sensorkit* dient dazu, typische Umweltdaten im Haushalt kontinuierlich zu erfassen und sichtbar zu machen. Die Sensoren erfassen Temperatur, Luftfeuchtigkeit, Helligkeit, Bewegung, Luftqualität

und Lautstärke. Dies wurde in mehreren Studien erprobt, angewendet und stetig weiterentwickelt (Kurze 2022; Kurze/Bischof 2021; Kurze/Reuter 2024; Kurze u. a. 2020; Kurze u. a. 2026; Köpferl u. a. 2024; Kurze u. a. 2025; Reuter 2025; Richter u. a. 2018). Die Auswahl der Messgrößen orientiert sich an den typischen im *Smart-Home*-System verbauten Komponenten, die zudem typischerweise als wenig intrusiv wahrgenommen werden – Anders als Mikrofone und Kameras, wie im bereits gut informierten Diskurs über so genannte *Smart Speaker*.

Die Visualisierung der erhobenen Daten erfolgt lokal auf einem Tablet in Form von Zeitreihen, die Veränderungen über den Tagesverlauf abbilden. Die Darstellung ist so gestaltet, dass auch weniger technisch versierte Personen Muster und Veränderungen im Alltag leicht erkennen können. Alle Daten verbleiben im Haushalt, können jederzeit eingesehen oder gelöscht werden, und es findet keine externe Datenübertragung statt. Damit wird sowohl Datensouveränität gewährleistet als auch die Reproduktion von proprietären Überwachungspraktiken verhindert (Kurze 2022; Kurze u. a. 2025). Abb. 1 zeigt das *Sensorkit* mit seinen verschiedenen technischen Elementen.



Abbildung 1: *Sensorkit* (eigenes Foto).

Die Teilnehmenden der Studien wurden durch verschiedene, an *Cultural Probes* orientierten Aufgaben (Berger u. a. 2018) schrittweise an die Datenerfassung, die Beobachtung der Daten am Tablet, und Möglichkeiten der Verknüpfung von Ereignissen und Daten herangeführt. Die Sensoren des *Sensorkits* lassen sich dabei flexibel im Haushalt platzieren, etwa in Wohnräumen oder in der Nähe von Fenstern oder Heizkörpern, um typische Alltagsbedingungen zu erfassen. Zu Beginn der Studie wurden die Sensoren in allen Haushalten zusammen mit den Teilnehmenden an denselben Orten – Eingangstür, Küche, Wohnzimmer – platziert. Dazu fanden Aufbaugespräche statt, in denen die Funktionsweise, Erwartungen und eventuell vorhandene Bedenken hinsichtlich des Einsatzes von Sensoren und *Smart Home* generell thematisiert werden. Während der Feldphase bearbeiteten die Teilnehmenden täglich kurze Impulsaufgaben zur Selbstbeobachtung bzw. Interpretation der eigenen Daten, wie die Beschreibung von Mustern, die Formulierung von Ursachenhypothesen oder die Identifikation von Abweichungen von Routinen.

Ziel dieser Aufgaben ist nicht die ‚richtige‘ Interpretation, sondern die Förderung von Aufmerksamkeit und Bewusstsein für die Aussagekraft der Sensordaten und Reflexion darüber, was über den eigenen Haushalt durch die Datenmitschnitte erfahrbar wird. Das *Sensorkit* übernimmt dabei lediglich eine Messfunktion und ist nicht mit anderen Objekten im Haushalt verknüpft. Mit zunehmender Vertrautheit wird der Grad der Strukturierung reduziert, um eigene Fragestellungen der Teilnehmenden zu ermöglichen. Der *Privacy-by-Co-Design*-Aspekt in dieser Phase der Studie besteht darin, dass die Teilnehmenden selbst entscheiden können, wo, wofür und wie sie die Sensoren einsetzen – Was durchaus problematische Nutzungsweisen hervorgebracht hat (*siehe unten*). In der Nutzung der Teilnehmenden werden jedoch Einsatzgebiete wie der Abgleich mit anderen, eigenen *Smart-Home*-Sensoren bzw. Systemen oder das Abbilden von Heiz- und Lüftungsroutinen ersichtlich, so dass in der Nutzung Funktionalität entstehen kann.

3.2 Erhebungsinstrument Interviews und Gruppendiskussion

Ergänzend fanden am Ende der Datenerhebung mittels *Sensorkit* qualitative Interviews und *Debriefings* statt, um die Wahrnehmung, Bedenken und Erfahrungen der Teilnehmer:innen zu erheben. In anschließenden Gruppendiskussionen wurden anonymisierte Datenausschnitte mit Teilnehmenden aus jeweils zwei bis drei Haushalten gemeinsam analysiert bzw. disku-

tiert. Dies knüpft direkt an das „*Guess-the-Data-Verfahren*“ an (Kurze u. a. 2020), mit dem gezeigt werden konnte, dass Personen aus einfachen *Smart Home*-Sensordaten nicht nur eigene Routinen, sondern auch das Verhalten anderer Haushaltsmitglieder und Haushalten rekonstruieren können. Zusätzlich macht das Format kollektive Deutungsmuster sichtbar und zeigt, wie stark Interpretationen vom jeweiligen Alltagswissen abhängen. Nur über diese Praxisnähe werden nicht-intendierte Nutzungen, Informationsasymmetrien, Konflikte, Missbrauchspotenziale und Fehlinterpretationen sichtbar. Die Teilnehmenden fungieren so nicht nur als ‚Datenlieferant:innen‘, sondern als doppelte Ko-Interpret:innen der eigenen Daten – sowohl in der individuellen Exploration des *Sensorkits* als auch im kollektiven Deuten im „Daten-Raten“. Indem die Methode die Teilnehmenden dazu anregt, eigene und fremde Daten zu interpretieren, wird implizites Alltagswissen über vermeintlich einfache und nicht datenschutzrelevante Sensorwerte sichtbar.

3.3 Sampling

Das Sampling der Studien folgte einer Minimal-/Maximalkontrast-Logik. In die jüngste Durchführung, die wir hier berichten, wurden Haushalte mit unterschiedlichen sozialen Konstellationen, Technikaffinität und Wohnformen einbezogen. Es nahmen sowohl Einpersonenhaushalte, Paare, Familien mit Kindern als auch Wohngemeinschaften teil. Miet- und Eigentumsverhältnisse wurden ebenfalls berücksichtigt, da sie Einfluss auf Kontrolle und Verantwortungszuschreibung haben können^{3,4}. Die Teilnehmenden wurden über Zeitungsanzeigen, digitale Verteiler und soziale Medien zur Teilnahme aufgefordert. Die aktuelle Studie fand im Raum Chemnitz und Umgebung statt, umfasste 18 Haushalte und wurde in zwei Feldphasen im Frühjahr 2024 (F1) und Frühjahr 2025 (F2) erhoben.

Das Sample der jüngsten Studie besteht insgesamt aus acht Paaren über 60 Jahren, zwei Müttern mit Kindern und Partnern, fünf alleinlebenden Männern im mittleren Alter (teilweise verpartnert), einer WG aus zwei

3 In der Erhebung zeigt sich die Präsenz von *Smart-Home*-Systemen mit ähnlicher Sensorik bspw. zur Steuerung des Energieverbrauchs besonders bei Eigenheimbesitzer:innen.

4 In Mietwohnungen wurde der Einsatz solcher Systeme tendenziell als zu aufwendig, teilweise als Luxus verstanden. In diesen ergibt sich außerdem zunehmend die Problematik des ‚unfreiwilligen‘ Einsatzes von Sensorik (Wolfangel 2024).

männlichen Personen unter 30 Jahren, einem jungen Paar unter 30 Jahren, sowie einer alleinlebenden Frau über 60 Jahren. Bei den älteren Paaren (+60 Jahre) findet sich vermehrt die Konstellation eines männlichen Partners, der über eine berufliche Nähe zur IT-Branche verfügt und bereits ein eigenes *Smart-Home*-System betreibt. In 12 der 18 Haushalte waren *smarte* Geräte wie Alexa, Thermomix bis hin zu komplexen *Smart-Home*-Systemen vorhanden. Das spricht für einen Selbstselektionseffekt anhand des Interesses an *Smart-Home*-Technik, was sich für das Forschungsinteresse zu Bewusstsein und Reflexion über Implikationen der Nutzung als wertvoll erwies.

3.4 Angewendete Auswertungsmethoden

Die Auswertung der Daten erfolgte interdisziplinär und im Methodenmix und jeweils angepasst auf die Form der vorliegenden Daten. So wurden bspw. die Annotationen der Teilnehmenden separat und inhaltsanalytisch ausgewertet (Reuter/Kurze 2025). Die während der Installation und beim Abbau des *Sensorkits* erhobenen Interviews und Gruppendiskussionen wurden transkribiert und interpretativ-rekonstruktiv sowie sequenzanalytisch in Gruppeninterpretationen in der interdisziplinären Forscher:innen-Gruppe ausgewertet. Das Vorgehen orientiert sich an der integrativen Auswertungsmethode von Kruse (2015), die verschiedenen Strategien qualitativer-rekonstruktiver Verfahren vereint und sich daher für die unterschiedlichen Daten (problemzentriertes Interview, Paarinterview, Gruppendiskussionen) besonders eignet.

3.5 Methodisch-ethische Reflexion und Limitationen

Die Untersuchung wurde iterativ durchgeführt. Nach dem ersten Feldstudienzyklus erfolgte eine Auswertung sowie eine Anpassung des Systems und der Aufgabenstellungen, bevor der zweite Feldstudienzyklus durchgeführt wurde. Dadurch konnten insbesondere technische Verbesserungen und zuvor bestehende Verständnishürden berücksichtigt werden. Die Forschungsethik und das bewusste Risikomanagement bilden einen wichtigen Rahmen für den gewählten Ansatz. Ziel ist es, Privatheitsrisiken den Teilnehmenden sichtbar zu machen, ohne sie in der Studie zu erzeugen oder zu verschärfen. Dazu werden Datenminimierung, Anonymisierung und lokale Speicherung

konsequent umgesetzt. Teilnehmende behalten jederzeit Kontrolle über ihre Daten; einschließlich der Möglichkeit zur Löschung. Eine audiovisuelle Erfassung wurde bewusst vermieden. Alle Haushaltsmitglieder und Besucher:innen werden in den Prozess einbezogen, um die informierte Einwilligung und den Schutz aller möglichen Datenlieferant:innen sicherzustellen. Auf diese Weise werden ethische Prinzipien und Designentscheidungen eng miteinander verknüpft, sodass der wissenschaftliche Erkenntnisgewinn und der Schutz der Teilnehmenden zugleich gewährleistet sind.

Insgesamt kombiniert der methodische Ansatz technische Datenerhebung, soziale Interpretation und partizipative Reflexion. Er ermöglicht es, Praktiken sichtbar zu machen, in denen Sensordaten zu sozialen Ressourcen werden, Wissen erzeugen, Entscheidungen legitimieren und Machtverhältnisse mitstrukturieren. Erst durch die Verbindung von kontinuierlicher Datenerhebung, individueller und kollektiver Interpretation sowie qualitativer Auswertung lassen sich die Dynamiken rekonstruieren, in denen aus einfachen Sensordaten soziale Wirklichkeit entsteht. Dieses Vorgehen bildet die Grundlage für die Darstellung der Ergebnisse im nächsten Kapitel, in dem Nutzung, Bedeutung und Konflikte rund um die Sensordaten analysiert werden.

Durch forschungspraktische und explorative Gründe weist die Studie mehrere Limitationen auf: Die Erhebung in 18 Haushalten im Raum Chemnitz bildet lokale soziokulturelle Strukturen ab und schränkt die Generalisierbarkeit ein. Zudem führt die Rekrutierung über soziale Medien zu einem selektiven Sample, wodurch bestimmte Gruppen (z. B. nicht deutschsprachige oder konflikthafte Haushalte) unterrepräsentiert sind. Das Studiendesign erzeugt außerdem Interventionseffekte, da das *Sensorkit* zur Reflexion anregt und damit Daten aktiv mitgestaltet werden; dies entspricht zwar dem *Co-Design*-Ansatz, kann aber auch unbeabsichtigte Effekte haben, etwa die Anregung neuer Überwachungspraktiken. Teilnehmende interpretierten die Sensoren teils als Grundlage für Produktentwicklungen statt als Reflexionsinstrument. Zusätzlich ist die Vergleichbarkeit mit proprietären und *Open Source* basierten *Smart-Home*-Systemen bewusst eingeschränkt, da reale Nutzungsdaten schwer zugänglich und anders verwendet werden. Trotz dieser Einschränkungen bietet der Ansatz wertvolle Einblicke in soziale Praktiken, Verantwortlichkeiten und Normalitätskonstruktionen in vernetzten Haushalten mit Fokus auf sozial verankerte Sinnstrukturen statt universeller Verallgemeinerung.

4. Aus Sensordaten werden soziale Wirklichkeiten

Unsere Studie zeigt, wie vermeintlich einfache Sensordaten interpretiert, mit Routinen verknüpft und zur Begründung von Entscheidungen herangezogen werden. Auf diese Weise entstehen aus Messwerten soziale Bedeutungen, die Konflikte, Machtverschiebungen und Verantwortlichkeiten erzeugen. Wie das geschieht, zeigen wir im Folgenden entlang vier zentraler Dimensionen dieser Interpretations- und Aushandlungsprozesse: Interpretierbarkeit, Datenpraktiken als Machtpraktiken, Akteurskonstellationen sowie mentale Modelle und *Awareness* (Sensibilisierung). Wir nutzen vornehmlich Beispiele aus einer von sechs Gruppendiskussionen zur Veranschaulichung⁵.

4.1 Interpretierbarkeit: Aus Daten werden Geschichten

Die Studie zeigt, dass die Teilnehmenden aus vermeintlich einfachen Sensorwerten vielfältige Rückschlüsse über Alltag, Routinen und Interaktionen sowohl in ihrem als auch in anderen Haushalten ziehen können. Sie zeigt nicht nur, dass die Teilnehmer:innen anhand von Daten, die z. B. Türöffnungen anzeigen, oder Änderungen von Temperatur und Luftfeuchtigkeit, prinzipiell in der Lage sind, diese mit zeitlichen Mustern und bekannten Gewohnheiten zu verknüpfen. Unsere Ergebnisse zeigen auch, dass Daten aus dem Zuhause immer mit alltagsweltlichen Kategorien wie Anwesenheit, Schlaf- und Arbeitsrhythmen oder Besuchssituationen korreliert werden. Die Sensordaten werden durch die Teilnehmenden standardmäßig *nicht* als technische Werte, sondern als Ausdruck von alltagspraktischen Vollzügen interpretiert. Das wird besonders deutlich, wenn Abweichungen von erwarteten Mustern nicht als technische Artefakte oder Messfehler interpretiert werden, sondern als Indikatoren für unerwartetes, erklärungsbedürftiges Verhalten. Die Teilnehmer:innen haben stets den Messwerten geglaubt. So fragt z. B. eine Teilnehmerin den Partner scherzhaft, ob er sich wohl rausgeschlichen habe, denn nur so wäre die nächtliche Bewegung in der Küche zu erklären. Eine wesentliche privatheitsrelevante Implikation von Sensordaten aus dem Zuhause entsteht demnach durch ihre Interpretierbarkeit auf Basis von eigenem alltagsweltlichem Wissen, und einer Normalitätser-

5 In den Gruppendiskussionen im *Guess-the-Data*-Verfahren wissen die Teilnehmenden nicht, aus welchem Haushalt die Daten stammen. Sie raten und plausibilisieren daher, ob bzw. in welchem Kontext die vorliegenden Daten entstanden sein könnten.

wartung, dass angezeigte Daten direkter Ausdruck von zuvor vorgängigem Verhalten sind.

4.2 Datenpraktiken als Machtpraktiken

In diesem Zusammenhang liegt es nahe, dass Daten im Haushalt eine geradezu autoritative Rolle einnehmen: Sie stützen Vermutungen, schaffen Legitimation für Handlungen und Bewertungen, aber schaffen auch Konfrontationen zwischen Haushaltsmitgliedern. Sensordaten können im Haushalt als Instrumente von Kontrolle und Normdurchsetzung eingesetzt werden. Dies zeigte sich in einem Haushalt beim Lüften und der Kühl-schranköffnung. So unterließen es mehrere Teilnehmerinnen, an den Kühl-schrank zu gehen, oder waren sich bewusst, dass nun sichtbar ist, wie kurz der Spaziergang mit dem Hund ausfällt oder wie gelüftet wurde. Im Studienkontext erfolgte eine Kontrolle von Verhalten nie mit schädigender Absicht. Dennoch zeigte sich auch in unserer Feldforschung, dass der Zugriff auf Daten bzw. Datenausschnitte laterale Überwachung innerhalb sozialer Nahbeziehungen, konkret zwischen Partner:innen, Eltern und Kindern und in Wohngemeinschaften, ermöglicht hat. Ein Kind explizierte dies und bewertete die Erhebungsphase als dauerhafte Überwachung durch die Mutter im Privatraum Kinderzimmer. *Smart-Home*-Daten dienen nicht nur der Beobachtung der Umwelt oder der Selbstbeobachtung, sondern auch der Beobachtung Dritter, etwa, wenn damit die nächtliche Geräuschkulisse im Hausflur eines Mietshauses erfasst wurde. Dass dies nicht unproblematisch ist, wurde darüber sichtbar, dass ein Teilnehmer sich aktiv darum bemühte, dies so klandestin wie möglich zu gestalten.

Innerhalb von Haushalten und in den Gruppendiskussionen wurden die Sensordaten regelmäßig als Grundlage für Verbesserungs- und Normierungspraktiken genutzt, z. B. in Bezug auf Heizen, Lüften oder Energieverbrauch. In den Gruppendiskussionen zeigt sich, wie sehr die Bewertungen dieser Aspekte normativ aufgeladen sind und Vorstellungen von Verantwortung, Fürsorge oder Nachhaltigkeit transportieren. So expliziert eine Teilnehmerin, sie hoffe, die Werte stammten nicht aus ihrem Haushalt, da ihr die Werte der schlechten Luftqualität peinlich wären. Heiz- und Lüftungsverhalten wurde regelmäßig als falsch beschrieben, wobei falsches Lüften und Heizen bspw. zu Schimmel führen könnten.

Diese Dimension der Implikationen zeigt, dass hinsichtlich Privatheit im *Smart Home* neue Herausforderungen entstehen. Es kann nicht nur darum

gehen, wie das vernetzte Zuhause *nach außen* abgesichert ist. Vielmehr muss neben dem kollektiven Erfordernis von Datenschutz (Véliz 2021) auch beachtet werden, wie Privatheit *innerhalb* von Familien- bzw. Haushaltsgefügen ausgestaltet wird. Privatheit gerät so als relationales, situiertes Geschehen – nicht als Individualpräferenz bzw. individuelle Abwehraufgabe in den Blick. Im Haushaltskontext gilt zu fragen: Wer darf Daten einsehen, wer interpretiert sie, wessen Deutungen gelten als maßgeblich und wessen Komfort wird berücksichtigt? Datenpraktiken können bestehende Machtasymmetrien verstärken, insbesondere wenn einzelne dauerhaft die Rolle der Beobachtenden übernehmen, während andere zu Objekten der Interpretation werden.

4.3 Akteurskonstellationen

Der Haushalt selbst darf nicht als abgeschlossene Einheit mit den immer gleichen Personen verstanden werden. Das vernetzte Zuhause beobachtet und speichert nicht nur die Daten von Personen, die sich für die Installation entschieden haben und sich der Implikationen der Nutzung (vermeintlich) bewusst sind. Neben den direkt beteiligten Haushaltsmitgliedern sind in unserer Studie eine Reihe von sekundären Nutzer:innen betroffen gewesen, u. a. waren Besucher:innen, Dienstleister:innen oder Handwerker:innen zeitweise in den Daten präsent. So rekonstruiert ein Paar in der ‚Daten-Raten‘ Sitzung genau, wann der Besuch gekommen ist, was er gemacht hat und wann dieser wieder gegangen ist. In diesem Kontext wird besonders deutlich, dass Privatheit im *Smart Home* nicht allein durch individuelle Zustimmung bzw. Ablehnung der Anschaffenden gewährleistet werden kann. Zudem wurden mehrfach Datenpraktiken über einzelne Haushalte hinaus berichtet. Häufig installierte ein:e technisch versierte Nutzer:in älteren Angehörigen *Smart-Home*-Geräte und wurde so zu einer Art Administrator aus der Ferne. Neben handlungspraktischen Implikationen, dass der Administrator bei Problemen eingreifen muss, ergaben sich daraus auch privatsphärerelevante Aushandlungen, wie z. B. um *smarte* Schließsysteme und die Frage, ob der Schwiegersohn dann einfach unangekündigt in der Wohnung stehen könne. Dabei wird die mögliche laterale Überwachung durch solche zugriffsberechtigten Haushaltsmitglieder zugunsten des Aspekts der Sicherheit im Notfall tendenziell ausgeblendet.

4.4 Mentale Modelle und Awareness

Unsere Studie zeigt, dass nicht-audiovisuelle Sensoren vor und während der Studie häufig als unproblematisch wahrgenommen werden. Dies zeigt zum Beispiel der Umgang mit der Messung der durchschnittlichen Lautstärke. Diese wird von den Teilnehmer:innen im Vergleich zur Sprachaufzeichnung als unproblematisch gerahmt. Paradox erscheint, dass es in den Haushalten, in denen die primären und sekundären Teilnehmenden Sorge vor Sprachaufzeichnungen im Studienkontext hatten, dennoch auch der Sprachassistent Amazon Alexa genutzt wurde, da dieser Teil der eigens geschaffenen häuslichen Komfortinfrastruktur war. Temperatur, Luftfeuchtigkeit oder Lautstärke erscheinen zunächst als harmlos, da sie keinen direkten Personenbezug aufweisen. Die Annahme der Harmlosigkeit von Umweltmessungen führt dazu, dass die Aussagekraft der Daten, die gerade aus der Überlagerung der einzelnen Messwerte entsteht, unterschätzt wird.

Ein avisiertes Ziel der Studie war, dass die Teilnehmer:innen durch die praktische Auseinandersetzung mit den eigenen Messwerten ein Bewusstsein dafür entwickeln, welche Rückschlüsse auf Anwesenheit, Routinen oder Aktivitäten möglich sind. Durch die Kombination aus individueller Exploration, strukturierten Aufgaben und kollektiver Interpretation in der Gruppendiskussion ‚Daten-Raten‘ wurde den Teilnehmenden deutlich, dass dieselben Werte unterschiedliche Bedeutungen annehmen können. Besonders anschaulich wird das in wiederkehrenden Diskussionen zur Rolle von Luftfeuchtigkeit und richtigem Lüften – und wie ein Vermieter im Vergleich zu einem Mieter diese Daten lesen würde. So zeigte sich im ‚Daten-Raten‘ bereits, dass die Teilnehmenden die Daten einer Person als Hinweis werten, dass bei den vorliegenden niedrigen Temperaturen bzw. Dauerlüften Schimmel vorprogrammiert sei. An dieser Stelle wurden die Implikationen von *Smart-Home*-Daten, insbesondere vor dem Hintergrund von durch Vermieter installierte Systeme, für die Teilnehmer:innen besonders nachvollziehbar.⁶

5. Implikationen für Gestaltung und Nutzung von Smart-Home-Daten

Die empirischen Befunde zeigen, dass Privatheitskonflikte im *Smart Home* nicht allein durch die eingesetzte Technik, sondern durch die konkrete

6 In der Erhebungsphase begann eine öffentliche Diskussion um den Einsatz von Sensorik in „smarten Rauchmeldern“ durch Vermieter (Wolfangel 2024).

Nutzung, institutionelle Rahmenbedingungen und gestalterische Entscheidungen entstehen. Daraus ergeben sich praktische Implikationen für Design, Nutzung, Transfer und Intervention sowie für die politische Rahmung und Regulierung.

5.1 Implikationen für die Gestaltung technischer Systeme

Smart-Home-Technologien können Privatheit nur dann wirksam gewährleisten, wenn ihre Gestaltung die sozialen Konstellationen innerhalb eines Haushalts berücksichtigt. Das betrifft vor allem die Ausgestaltung von Zugriffsrechten. Sowohl Nutzungsbedingungen, die Optionen zur Einwilligung in diese als auch Schnittstellen und Apps zur Steuerung differenzieren bislang nicht oder nicht ausreichend zwischen unterschiedlichen Nutzer:innen und deren Privatheitsbedürfnissen. Es gibt zur Steuerung von Geräten in der Regel ein Benutzerkonto. Das Vorhandensein weiterer Personen, die ebenfalls zustimmen müssten, wird technisch nicht beachtet. Dies gilt es genau andersherum zu gestalten. Unterschiedliche Rollen wie Erwachsene, Kinder oder temporäre Haushaltsmitglieder und Besucher:innen müssten in den *Interfaces* und Einstellungsmöglichkeiten berücksichtigt werden. Die Erfassung der Daten muss insgesamt nach außen sichtbar werden, insbesondere für Personen, die sich nicht intensiv mit dem konkreten *Smart-Home*-System beschäftigen und über ihre Datenerfassung informiert sind. Zudem ließe sich bei der Datenerfassung eine Zweckbindung bzw. zeitliche Beschränkung der Datenerhebungen durch Gesetze oder Richtlinien zur Technikgestaltung einführen.

Hierbei kommt es wesentlich darauf an, ob das System auf *Open-Source*-Anwendungen basiert, oder kommerzielle Produkte zum Einsatz kommen. Generell sollten *Default*-Einstellungen die minimale Datenerfassung und lokale Speicherung priorisieren. Bei den meisten *Open-Source*-Systemen ist dies bereits der Fall bzw. oberste Priorität der primären Nutzenden. Dennoch sollten auch in diesen Fällen Möglichkeiten bereitstehen, um gerade sekundären Nutzer:innen mehr Handlungsspielräume zu eröffnen, ohne dass dafür ein Einstieg in die Programmebene der Systeme notwendig ist.

Funktionen wie ein temporäres Anhalten bzw. Stummschalten, eine einfache Möglichkeit zur Löschung von bestimmten Zeitabschnitten, eine einfache *exit-option* sowie Migration und Export von Daten eröffnen Handlungsspielräume, ohne die Nutzung zu unterbinden (Kurze u. a. 2025).

Gerade um sekundären Nutzer:innen den Zugang zu erleichtern, sollten Möglichkeiten zur Annotation, Kommentierung und Kontextualisierung bestehen, damit Nutzer:innen eigene Erklärungen, Irritationen oder alternative Deutungen einbringen und sichtbar machen können (Kurze/Reuter 2024; Reuter 2025; Reuter/Kurze 2025).

Festgelegte Transparenzmechanismen sollten für Dritte verständlich darstellen, welche Daten entstehen, wo sie verarbeitet werden und wer Zugriff darauf hat und welche Interpretationen und Rückschlüsse ggf. daraus möglich sind. Zugleich müssen *Interfaces* und Visualisierungen handhabbar sein und Aushandlungsprozesse erleichtern. Irritationen können produktiv gemacht und bestehende Machtasymmetrien als Ergebnis von Aushandlungen sichtbar werden, anstatt sie zu verschleiern. Erst wenn die technische Gestaltung sozial anschlussfähig ist, können die Schutzwirkungen der Systeme im Alltag realisiert werden.

5.2 Implikationen für die Nutzung

Privatheit wird nicht allein durch vernetzte Systeme, sondern wesentlich durch deren Nutzung und fehlende Aushandlungsprozesse innerhalb des Haushalts gefährdet. Entscheidungen über Sensorplatzierung, Datensichtbarkeit und -interpretation sollten offen kommuniziert, diskutiert und gemeinsam getroffen werden, sodass alle betroffenen Personen einbezogen sind. Praktische Checklisten oder Pfaddiagramme können dabei helfen, zentrale Fragen vor der Installation eines Sensors zu klären, zum Beispiel: Welche Daten werden wirklich benötigt? Wer ist davon betroffen? Welche Alternativen gibt es? Solche Reflexionen verwandeln technische in soziale Entscheidungen und fördern ein Bewusstsein für die Auswirkungen der Datenerhebung auf alle Beteiligten. Die Gruppendiskussionen bezeugen, dass der eigentliche Wunsch hinter dem Einsatz von *Smart Home* nicht selten der Wunsch nach einfachen Abschaltmechanismen, bspw. für Strom und Herd im Notfall, ist. Zudem verdeutlichen die Ergebnisse die Grenzen individueller Verantwortung und technischer Kompetenz für *Smart-Home*-Systeme. In Mehrpersonenhaushalten, bei *Cloud*-Diensten oder bei ungleichen Zugangsmöglichkeiten reicht individuelles Wissen allein nicht aus, um alle Risiken zu überblicken. So wird bspw. immer wieder von technisch versierten und fürs *Smart-Home*-System verantwortlichen Personen betont, dass sie die alleinigen Administrator:innen sind, die das System nach außen vollständig absichern. Doch auch in solchen Konstellationen gehen Risiken

einher. So erwähnte ein Teilnehmer in der Diskussion, das z. B. seine Ehefrau keinen Zugriff auf die Steuerung der Heizungsanlage hätte. Effektiver Schutz der individuellen Privatheit auch und gerade im eigenen Zuhause erfordert daher, dass Nutzung in technische, rechtliche und institutionelle Rahmenbedingungen eingebettet wird und die Aushandlung im Haushalt durch unterstützende Formate und geeignete Gestaltung begleitet wird.

5.3 Implikationen für weitere Forschung und Wissenstransfer

Die privatheitsrelevante Wirkung einfacher Sensordaten wird besonders dann erfahrbar, wenn alltagsnahe Formate und Methoden eingesetzt werden. Daten-Vignetten, Simulationen, *Workshops* und Elemente aus *Design Fiction* konfrontieren die Teilnehmenden mit irritierenden oder widersprüchlichen Szenarien und machen die Inferenzpotenziale der Daten nachvollziehbar. Als besonders effektiv hat sich der *Zugang zu den eigenen Daten* gezeigt. Personen, die sonst vor allem in einer sekundären Position sind, wird durch den Zugriff die eigene Abbildbarkeit bewusst, und es regt zur Reflexion an. Aber auch administrativ agierende primäre Nutzende überdachten ihre Position. Beispielsweise wurde im Studienkontext in einem Haushalt davon Abstand genommen, einen Amazon-Echo-Lautsprecher – wie ursprünglich geplant – im Schlafzimmer zu installieren. Da Selbsterfahrungsformate extrem aufwendig sind, hat sich auch das Format von Daten-Raten-*Workshops* als effektiv erwiesen, in denen fremde anonymisierte Datenausschnitte auf Basis kurzer Impulse gemeinsam interpretiert werden. Abstrakte Risiken werden dadurch in konkrete Alltagsszenarien übersetzt und Diskussionen über Angemessenheit, Fehlinterpretation sowie Daten als soziale und machtvoll Ressource ermöglicht. Verbraucherzentralen und andere Bildungsträger können diesbezüglich eine Multiplikator:innen-Rolle übernehmen, indem sie wissenschaftliche Befunde in alltagstaugliche Bildungsressourcen übersetzen und Nutzer:innen aktiv in Deutung und Reflexion einbeziehen. Formate, die den Zugang bzw. die Einsicht in die eigenen Daten durch andere simulieren, können eine ähnliche Auseinandersetzung ermöglichen (*Serious Games*).

Privacy-by-Co-Design erweist sich insgesamt als wertvolles und zentrales Konzept, da Partizipation zusätzliche Aspekte sichtbar macht, die allein durch antizipierende Planung von Produkten oder Fallstricken nicht erkennbar sind. Dies sind nicht antizipierte Bedrohungspotenziale, alltagspraktische Zumutungen und die Bedienbarkeit von Datenschutzmaßnah-

men im Umfeld von *Smart-Home*-Systemen. Im Studienkontext hat sich hier der Zugang zu den Daten als solcher Aspekt erwiesen. Die dabei erzeugte methodische Irritation ist kein Störfaktor, sondern ein Werkzeug, um implizite Annahmen über Technik, Normalität und Kontrolle offenzulegen und reflexive Distanz bei den Teilnehmenden zu fördern. Neben den Teilnehmenden sind auch die Gestalter:innen von *Smart-Home*-Technik eine Zielgruppe des Forschungsansatzes: Zwar kann in der Entwicklungspraxis nicht für jede neue *Smart-Home*-Anwendung so eine Feldstudie vorgelagert werden, aber eine grundlegende Sensibilisierung der Entwickler:innen für *Smart-Home*-Privatheit als soziale Aushandlung auf Haushaltsebene hat sich sowohl als Leerstelle als auch machbar erwiesen. Eine aus dem Projekt entwickelte Workshopmethode dazu berichten Becker u. a. (2026).

5.4 Implikationen für die politische Regulierung und Steuerung

Unsere Forschung zeigt, dass Privatheit für alle betroffenen Personen im *Smart Home* nicht allein durch individuelles Verhalten oder technische Gestaltung abgesichert werden kann, sondern eine normative und regulatorische Rahmung erforderlich erscheint. Zentral ist dabei das Transparenz-Erfordernis: *Smart-Home*-Systeme müssen klar aufzeigen, welche Daten sie erfassen, wie diese verarbeitet und aggregiert werden können und nicht zuletzt, wer Zugriff darauf hat. Ebenso wesentlich sind wirksame *Default*-Vorgaben. Sensoren sollten standardmäßig nur notwendige Daten erfassen, lokal speichern und leicht von außen deaktivierbar sein. Die Datenhaltung sollte standardisiert zeitlich sowie zweckgebunden begrenzt werden. Darüber hinaus müssen die unterschiedlichen Haushaltsrollen berücksichtigt werden. Erwachsene, Kinder und Dritte sollten klar definierte Zugriffsrechte erhalten, und Entscheidungen über die Nutzung oder Freigabe von Daten sollten gemeinschaftlich im Haushalt abgestimmt werden, um Informationsasymmetrien zu vermeiden. Dies kann bspw. über Vorgaben zu Nutzungs-IDs und Zustimmungserfordernissen unterstützt werden. Diese Vorgaben müssen insgesamt in technische und organisatorische Anforderungen übersetzt werden, etwa durch lokale Speicheroptionen, standardisierte Visualisierungen von Datenflüssen, verständliche Rollenmodelle sowie systematische Bildungs- und Reflexionsangebote. Auf diese Weise kann Privatheit nicht als statische Norm verstanden werden, sondern als dynamisches, relationales Gut, das situativ stabilisiert werden muss. Diese

Diskurs-, und Interpretationsprozesse in technische Abläufe zu übersetzen, so dass die Technik bei der Inbetriebnahme viele der oben erwähnten Aspekte in die Konfiguration übernehmen, ist das nächste Forschungsziel aus dem Projektkontext.

6. Fazit

Der Beitrag zeigt, dass vermeintlich einfache Sensordaten im häuslichen Umfeld komplexe Privatheitsimplikationen erzeugen, weil sie im Kontext sozialer Beziehungen interpretiert werden und als Ressource für Wissen, Kontrolle und Normdurchsetzung dienen. Sensoren, die Temperatur, Bewegung, Licht oder Luftfeuchtigkeit messen, erscheinen zunächst unproblematisch, entfalten ihre Bedeutung jedoch in Verbindung mit alltäglichen Routinen, Rollenverteilungen und der Organisation von Haushalten. Sensordaten werden nicht nur erfasst, sondern in Geschichten über An- und Abwesenheit, Verhalten und Abweichungen übersetzt und sind in soziale Aushandlungsprozesse eingebettet. Sie legitimieren Wertungen, stabilisieren normative Erwartungen und strukturieren Machtverhältnisse im Haushalt mit.

Die Daten und Visualisierungen fungieren nicht als technisch erfasste Informationen, sondern als Belege für bestehende Wert- und Normvorstellungen und werden mit autoritativer Aussagekraft, im Sinne von objektiven Fakten, eingesetzt, um Positionen Gewicht zu verleihen. Dies zeigt sich insbesondere hinsichtlich der Fragen von richtigem und falschem Lüften, zum Umgang mit Eigentum bzw. Mietsachen oder bei Fragen der Lärmbelästigung.

Durch die Verbindung von Feldforschung, partizipativen *Workshops* und reflexiver Analyse wird sichtbar, wie einfache Sensordaten komplexe soziale Dynamiken, Informationsasymmetrien und normative Aushandlungsprozesse auslösen. Sensordaten werden zudem leichtfertig als Mittel lateraler Überwachung genutzt. Sie erlauben die Beobachtung anderer Haushaltsmitglieder, werden für die Bewertung von deren Verhalten eingesetzt. Privatheit erweist sich in diesem Kontext nicht als individuelles Recht, sondern als relationales und situatives Gut, das in Aushandlungsprozessen, Konflikten und impliziten Hierarchien im Haushalt – und teils darüber hinaus – entsteht. Neben Haushaltsmitgliedern betrifft die Datenerhebung Besucher:innen, Handwerker:innen, und Pflegedienste. Schon auf Ebene der Studie war diese Zustimmung durch alle Betroffenen – trotz schrift-

licher und mündlicher Aufklärung und Ausgabe entsprechender Einwilligungsbögen – nicht immer gegeben. In der empirischen Welt außerhalb der Studie ist dies noch seltener der Fall.

Die Studie verdeutlicht, dass Problembewusstsein und Sensibilität gerade für nicht-audiovisuelle Sensorik schwach ausgeprägt sind. Temperatur-, Luftfeuchtigkeits- oder Geräuschdaten werden häufig als harmlos eingeschätzt, obwohl sie in Kombination mit Alltagswissen hochgradig aussagekräftig sind. Erst partizipative, datenbasierte Konfrontationen mit den eigenen Daten machten Risiken, Fehlinterpretationen und Konfliktpotenziale sichtbar. *Awareness* entsteht somit nicht primär durch Information, sondern durch Erfahrung und kollektive Reflexion.

Aus praktischer Perspektive ergibt sich, dass Privatheit im *Smart Home* nur durch das Zusammenspiel von Gestaltung, Nutzung und Bildung gesichert werden kann. Technische Systeme müssen Rollen- und Rechtekonzepte, Transparenzmechanismen und datensparsame Voreinstellungen bieten. Nutzung muss als sozialer Prozess verstanden werden, der Kommunikation, Aushandlung und gemeinsame Regeln einschließt. Bildung und Transfer befähigen Nutzer:innen, Daten zu interpretieren, Fehlinterpretationen zu erkennen und normative Implikationen zu reflektieren. Schutz entsteht demnach durch die Kombination von Technik, Praxis und Kompetenzinfrastruktur.

Regulatorische und pädagogische Ansätze schließen sich dabei nicht aus, sondern ergänzen sich. Vorgaben für Hersteller und Plattformen sichern Mindeststandards, während Aufklärung und Reflexion der Nutzer:innen die sozialen Dynamiken adressieren. Laterale Überwachung, normative Kontrolle und konfliktreiche Deutungen entstehen nicht primär durch Marktversagen, sondern durch alltägliche Nutzungskonstellationen. Nutzer:innen sind zugleich Adressat:innen und aktive Akteur:innen bei der Herstellung oder Unterminierung von Privatheit.

In der doppelten Bedeutung der ‚Nutzer:innen‘, einerseits als technische Bedienende und andererseits als soziale Akteur:innen, zeigt sich eine grundlegende Ambivalenz. Schutz erfordert sowohl Regulierung der Anbieter als auch Aufklärung derjenigen, die Technik einsetzen. Partizipative Aufklärung, datenbasierte Irritation und reflexive Nutzung sind kein Ersatz für Regulierung, sondern eine notwendige Ergänzung, um Privatheit im vernetzten Zuhause als relationales, situiertes und gestaltbares Gut zu stabilisieren.

Literatur

- Adryan, Boris (2015): Connected product labelling github.io URL: <https://badryan.github.io/2015/09/30/connected-product-labelling.html> (besucht am 02.06.2019)
- Becker, Alexa; Schäfer, Mirko; Kurze, Albrecht; Bischof, Andreas; Baum, Franziska; Pierce, James und Berger, Arne (2026): Design Strategies for Mitigating Tensions in Using Simple Smart Home Sensors. In: ACM (Hrsg.): *Proceedings of Designing Interactive Systems Conference (DIS) 2026, Singapore*. New York, NY: ACM, S. 722–733. <https://doi.org/10.1145/3800645.381298>
- Berger, Arne; Kurze, Albrecht; Totzauer, Sören; Storz, Michael; Lefevre, Kevin; Bischof, Andreas und Freiermuth, Mira (2018): Sensing Home: Designing an Open Tool That Lets People Collect and Interpret Simple Sensor Data from Their Homes. *i-com*, 17(2), S. 153–167.
- Bühr, Peter (2017): Report: A Trustmark for IoT. thingscon.com. URL: <https://www.thingscon.com/report-a-trustmark-for-iot/> (besucht am 24.06.2018)
- Caven, Peter; Zhang, Zitao; Abbott, Jacob; Ma, Xinyao und Camp, Ljean (2024): Comparing the Use and Usefulness of Four IoT Security Labels. In: ACM (Hrsg.): *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, CHI '24, Honolulu, HI*. New York, NY: ACM, S. 1–31. <https://dl.acm.org/doi/10.1145/3613904.3642951>
- Deschamps-Sonsino, Alexandra (2018): *Smarter Homes: How Technology Will Change Your Home Life*. Berkeley, CA: Apress.
- Dereymaeker, Julie; Schokkenbroek, Janneke M.; Martens, Marijn und De Wolf, Ralf (2024): Smarter homes, smarter surveillance? Exploring intimate surveillance practices in modern day households. *New Media & Society*, 27(11), S. 6119–6138. <https://doi.org/10.1177/14614448241263757>
- Fischer, Joel E.; Crabtree, Andy; Rodden, Tom; Colley, James A.; Costanza, Enrico; Jewell, Michael O. und Ramchurn, Sarvapali D. (2016): „Just Whack It on Until It Gets Hot“: Working with IoT Data in the Home. In: ACM (Hrsg.): *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, CHI'16, San Jose*. New York, NY: ACM, S. 5933–5944. <https://dl.acm.org/doi/10.1145/2858036.2858518>
- Garg, Vaibhav (2021): A Lemon by Any Other Label: In: Mori, Paolo, Lenzini, Gabriele und Furnell, Steven (Hrsg.): *Proceedings of the 7th International Conference on Information Systems Security and Privacy, ICISSP, Paolo Mori*, Vol. 1. Setúbal: Science and Technology Publications, S. 558–565. <https://doi.org/10.5220/0010295205580565>
- Hahn, Sara; Al-Amrani, Nusaibah; Allagah, Sara; Huang, He Rong; Kircher, Eva; Rehs, Cornelia; Vogt, Joachim; Marky, Karola und Gerber, Nina (2024): How to Respect Bystanders' Privacy in Smart Homes - A Co-Creation Study. In: *Proceedings of the 13th Nordic Conference on Human-Computer Interaction, NordiCHI'24, Upsala*, Artikel Nr. 7. New York, NY: ACM, S. 1–19. <https://doi.org/10.1145/3679318.3685340>

- Jin, Haojian; Guo, Boyuan; Roychoudhury, Rituparna; Yao, Yaxing; Kumar, Swarn; Agarwal, Yuvraj und Hong, Jason I. (2022): Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes. In: ACM (Hrsg.): *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, CHI'22, New Orleans, LA*, Artikel Nr. 449. New York, NY: ACM, S. 1–19. <https://doi.org/10.1145/3491102.3517602>
- Köpferl, Karola; Lehmann, Tanja; Börner, Andy; Becker, Alexa; Berger, Arne; Bischof, Andreas und Kurze, Albrecht (2024): Ich sehe das, was Du nicht siehst: Spuren einfacher Sensordaten im smarten Zuhause erleben und reflektieren. In: Gesellschaft für Informatik e.V., (Hrsg.): *Mensch und Computer 2024 – Workshopband, Karlsruhe*. Bonn: Gesellschaft für Informatik e.V. <https://doi.org/10.18420/muc2024-mci-ws17-153>
- Kruse, Jan (2015): *Qualitative Interviewforschung: ein integrativer Ansatz*, (Grundlagentexte Methoden). 2., überarbeitete und ergänzte Auflage. Weinheim Basel: Beltz Juventa.
- Kurze, Albrecht; Bischof, Andreas; Totzauer, Sören; Storz, Michael; Eibl, Maximilian; Brereton, Margot und Berger, Arne (2020): Guess the Data: Data Work to Understand How People Make Sense of and Use Simple Sensor Data from Homes. In: ACM (Hrsg.): *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, CHI'20, Honolulu, HI*. New York, NY: ACM, S. 1–12. <https://doi.org/10.1145/3313831.33762>
- Kurze, Albrecht und Bischof, Andreas (9. Mai 2021): Wicked Implications for Human Interaction with IoT Sensor Data. Workshop Human-Data Interaction through Design at Conference on Human Factors in Computing Systems (CHI21), Yokohama. <https://dl.acm.org/doi/pdf/10.1145/3613905>
- Kurze, Albrecht (2022): Senseful Sensors: Learnings and Optimizations for IoT Sensors in HCI Research In: IEEE (Hrsg.): *2022 IEEE 9th International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*, Chemnitz. Setúbal: Science and Technology Publications. <https://doi.org/10.1109/CIVEMSA53371.2022.9853698>
- Kurze, Albrecht und Reuter, Christin (2024): Understanding and addressing user needs for annotation of simple sensor data: Bridging the gap between human sensemaking and machine interpretation. In: Gesellschaft für Informatik e.V. (Hrsg.): *Proceedings of INFORMATIK 2024, Wiesbaden*. Bonn: Gesellschaft für Informatik e.V., S. 465–472. https://doi.org/10.18420/inf2024_34
- Kurze, Albrecht; Bischof, Andreas und Berger, Arne (2025): Smart, simple, sincere - Why and how we might rethink connected things in our smart homes. In: Stiftung ThingsCon (Hrsg.): *ThingsCon Report: The State of Responsible Technology 2025*. Amsterdam: ThingsCon, S. 24–30. <https://doi.org/10.5281/zenodo.16498330>
- Kurze, Albrecht; Becker, Alexa; Bergk, Jana und Reuter, Christin (2026): (De)Coding Lay Users' Annotations of Time-series Sensor Data from the Home. In: ACM (Hrsg.): *Extended Abstracts of the 2026 CHI Conference on Human Factors in Computing Systems, CHI EA '26, Barcelona*. New York, NY: ACM, S. 1-7. <https://dl.acm.org/doi/10.1145/3772363.3798962>

- Laput, Gierad; Zhang, Yang und Harrison, Chris (2017): Synthetic Sensors: Towards General-Purpose Sensing. In: ACM (Hrsg.): *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, CHI '17, Denver, CO*. New York, NY: ACM, S. 3986–3999. <http://dx.doi.org/10.1145/3025453.3025773>
- Leitão, Roxanne (2019): Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. In: *Proceedings of the 2019 on Designing Interactive Systems Conference. DIS' 19, San Diego*. New York, NY: ACM, S. 527–539. <https://doi.org/10.1145/3322276.3322366>
- Lopez-Neira, Isabel; Patel, Trupt; Parkin, Simon; Danezis, George und Tanczer, Leonie (2019): 'Internet of Things': How Abuse is Getting Smarter. In: *Safe – The Domestic Abuse Quarterly*, (63), S. 22–26. <http://dx.doi.org/10.2139/ssrn.3350615>
- Lupton, Deborah (2016): *The quantified self: A sociology of self-tracking*. Cambridge, Malden, MA: Polity.
- Marky, Karola; Voit, Alexandra; Stöver, Alina; Kunze, Kai; Schröder, Svenja und Mühlhäuser, Max (2020): „I don't know how to protect myself“: Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In: ACM (Hrsg.): *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society. Nordic Chi'20, Talin*, Artikel Nr. 4. New York, NY: ACM, S. 1–11. <https://doi.org/10.1145/3419249.3420164>
- Marky, Karola; Prange, Sarah; Mühlhäuser, Max und Alt, Florian (2021): Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. In: ACM (Hrsg.): *20th International Conference on Mobile and Ubiquitous Multimedia. Association for Computing Machinery, Lueven*. New York, NY: ACM, S. 108–122. <https://doi.org/10.1145/3490632.3490664>
- Mascheroni, Giovanna (2020): Datafied childhoods: Contextualising datafication in everyday life. *Current Sociology*, 68(6), S. 798–781. <https://doi.org/10.1177/001139211880753>
- Morgner, Philipp; Müller, Christian; Ring, Matthias; Eskofier, Björn; Riess, Christian; Armknecht, Frederik und Benenson, Zinaida (2017): Privacy Implications of Room Climate Data. Computer Security. In: Foley, Simon; Gollmann, Dieter und Snekkenes, Einar (Hrsg.): *Proceedings of Computer Security, ESORICS 2017, Oslo*. Cham: Springer, S. 324–343. https://doi.org/10.1007/978-3-319-66399-9_18
- Mucha, Henrik; Barros, Ana; Benjamin, Jesse; Benz Müller, Christoph; Bischof, Andreas; Buchmüller, Sandra; Carvalho, Alexandra; Dhungel, Anna-Katharina; Draude, Claude; Fleck, Marc-Julian; Jarke, Julian; Klein, Stefanie; Kortekaas, Caroline; Kurze, Albrecht; Linke, Diane; Maas, Franzisca; Marsden, Nicola; Melo, Ricardo; Michel, Susanne und Berger, Arne (2022): Collaborative Speculations on Future Themes for Participatory Design in Germany. *i-com*, 21(2), S. 283–298. <https://doi.org/10.1515/icom-2021-0030>
- Ramokapane, Kopo M.; Sameen, Maria und Dkaidek, Zaina (2024): Inclusive Internet of Things Privacy Labels. *IEEE Security & Privacy*, 22(5), S. 32–39. <https://doi.org/10.1109/MSEC.2024.3417819>

- Reinhardt, Delphine und Railean, Alexandr (2020): OnLITE: On-line Label for IoT Transparency Enhancement. In: Asplund, Mikael und Nadjm-Tehrani, Simin (Hrsg.): *Proceedings of the 25th Nordic Conference on Secure IT Systems (NordSec), 2020: Secure IT Systems*. Cham: Springer Nature, S. 229–245. https://doi.org/10.1007/978-3-030-70852-8_14
- Reuter, Christin (2025): Eine Nutzerfreundliche Annotationslösung für Einfache Sensordaten im Zuhause. 18. *Internationales Symposium für Informationswissenschaft (ISI 2025)*, Chemnitz. <https://doi.org/10.5281/zenodo.15511487>
- Reuter, Christin und Kurze, Albrecht (2025): AnnoTool: A User-Friendly Annotation Tool for Simple Sensor Data in the Home. In: Gesellschaft für Informatik e.V. (Hrsg.): *Mensch und Computer 2025 – Workshopband, Dresden*. Bonn: Gesellschaft für Informatik e.V. <https://doi.org/10.18420/muc2025-mci-wip-284>
- Richter, Johanna; Bischof, Andreas; Kurze, Albrecht; Totzauer, Sören; Freiermuth, Mira; Storz, Michael; Lefevre, Kevin und Berger, Arne (2018): Machtförmige Praktiken durch Sensordaten in Wohnungen. In: Gesellschaft für Informatik e.V. (Hrsg.): *Mensch und Computer 2018 – Tagungsband, Dresden*. Bonn: Gesellschaft für Informatik e.V. <https://doi.org/10.18420/muc2018-mci-0253>
- Rogers, Michaela M.; Fisher, Coleen; Ali, Parveen; Allmark, Peter und Fontes, Lisa (2023): Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review. *Trauma, Violence, & Abuse*, 24(4), S. 2210–2226. <https://doi.org/10.1177/15248380221090218>
- Saqib, Eimaan; He, Shijing; Choy, Junghyun; Abu-Salma, Ruba; Such, Jose; Bernd, Julia und Javed, Mobin (2025): Bystander Privacy in Smart Homes: A Systematic Review of Concerns and Solutions. *ACM Transactions on Computer-Human Interaction*, 32(5), S. 1–43. <https://doi.org/10.1145/3731755>
- Schulz, Annika Sabrina; Müller, Johanna und Beruscha, Frank (2023): Experience by Cohabitation: Living in a Smart Home Initiated by Your Partner. In: Abdelnour Nocera, Jose; Kristín Lárusdóttir, Marta; Petrie, Helen; Piccinno, Antonio und Winckler, Marco (Hrsg.): *Human-Computer Interaction – INTERACT 2023 (Lecture Notes in Computer Science, Bd. 14144)*. Cham: Springer Nature, S. 304–323. https://doi.org/10.1007/978-3-031-42286-7_17
- Stark, Luke und Levy, Karen (2018): The Surveillant Consumer. *Media, Culture & Society*, 40(8), S. 1202–1220. <https://doi.org/10.1177/0163443718781985>
- Tanczer, Leonie Maria (2021): Das Internet der Dinge: Die Auswirkungen »smarter« Geräte auf häusliche Gewalt. In: bff: Bundesverband Frauenberatungsstellen und Frauennotrufe; Prasad, N. (Hrsg.): *Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung. Formen und Interventionsstrategien (Gender Studies)*. Bielefeld: transcript, S. 205–226. <https://doi.org/10.14361/9783839452813>
- Tolmie, Peter; Crabtree, Andy; Rodden, Tom; Colley, James und Luger, Ewa (2016): “This has to be the cats”: Personal Data Legibility in Networked Sensing Systems. In: ACM (Hrsg.): *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing, CSCW’16, Vienna*. New York, NY: ACM, S. 491–502. <https://dl.acm.org/doi/10.1145/2818048.2819992>
- Véliz, Carissa (2021): *Privacy is power: why and how you should take back control of your data*. London: Corgi Books.

- Wang, Ge; Zhao, Jun; Van Kleek, Max; Pea, Roy und Shadbolt, Nigel (2025): FamiData Hub: A Speculative Design Exploration with Families on Smart Home Datafication. In: ACM (Hrsg.): *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems. Chi'25, Yokohama*. New York, NY: ACM, Artikel Nr. 940, S. 1–17. <https://dl.acm.org/doi/10.1145/3706598.3713494>
- Wolfangel, Eva (2024): Rauchmelder bei Vonovia: Der Spion an meiner Decke. In: *Zeit Online vom 24.10.2024*. Zeit.de URL: <https://www.zeit.de/digital/datenschutz/2024-10/rauchmelder-vonovia-mieter-datenschutz-smart> (besucht am 12.03.2026)
- Yao, Yaxing; Basdeo, Justin Reed; Kaushik, Smirity und Wang, Yang (2019): Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In ACM (Hrsg.): *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, CHI'19, Glasgow*, Artikel Nr. 198. New York, NY: ACM, S. 1–12. <https://doi.org/10.1145/3290605.3300428>
- Zufferey, No  ; Salehzadeh Niksirat, Kavous; Humbert, Mathias und Huguenin, K  vin (2024): Our Data, Our Solutions: A Participatory Approach for Enhancing Privacy in Wearable Activity Tracker Third-Party Apps. *Proceedings on Privacy Enhancing Technologies*, 2024(4), S. 734–754. <https://doi.org/10.56553/popets-2024-0139>