Ohne Big Brother und Cloud, aber nicht ohne Probleme

Fallbeispiele zu Implikationen smarter Technik mit einfachen Sensoren im Zuhause

Andy Börner [1], Karola Köpferl [2], Tanja Lehmann [2], Alexa Becker [3], Arne Berger [3], Andreas Bischof [2] und Albrecht Kurze [1]

Abstract: Mit der Verbreitung von IoT-Geräten im Zuhause, mit einer Vielzahl von Sensoren, die Daten sammeln und speichern, entstehen Probleme, insbesondere für Privatheit. Diese lassen sich vermeintlich leicht lösen, wenn keine Produkte von großen Tech-Konzernen genutzt werden, um eine Speicherung und Analyse von Daten in der Cloud oder durch einen „Big Brother“ zu vermeiden. Wir zeigen anhand von drei Fallbeispielen aus der Literatur, dass es selbst bei einfachen Sensordaten hintergründig doch nicht so einfach ist. Abschließend beschreiben wir unseren Forschungsansatz „Privacy by Co-Design“ dazu.

Keywords: Smart Home, IoT, Internet of Things, Privacy, Sensors, Implications, ELSI

1 Einleitung

Mit dem Smart Home erreicht das Internet-der-Dinge (Internet of Things, IoT) auch einen höchst privaten Raum: die eigenen vier Wände [Te23]. Smarte Thermostate regeln die Temperatur in allen Räumen, eine smarte Kamera überwacht die Eingangstür und der smarte Kühlschrank kauft selbstständig frisches Essen ein. Aber auch vermeintlich einfache Sensoren, u. a. für Licht, Temperatur, Luftfeuchte und Luftqualität, helfen beispielsweise Schimmel zu vermeiden. Denn es gibt eine Vielzahl von sinnvollen Anwendungsfällen für solche einfachen Sensoren: Unterstützung beim Energiesparen oder als externe Metrik zur Verbesserung des persönlichen Wohlbefindens (z. B. mit CO_2-Ampel für Luftqualität). Dabei offenbart sich, dass das Geschäftsmodell der Unternehmen, welche derartige Geräte anbieten, meist nicht nur auf dem reinen Verkauf der Produkte basiert, sondern auch auf Sammlung und Auswertung der gemessenen und gespeicherten Daten [Wa23; We19]. Viele Nutzer:innen sehen dies in Bezug auf ihre Privatsphäre inzwischen kritisch, nutzen die

[1] Technische Universität Chemnitz, Professur Medieninformatik, Straße der Nationen 62, 09111 Chemnitz, Deutschland, andy.boerner@informatik.tu-chemnitz.de, https://orcid.org/0009-0004-3258-2903; albrecht.kurze@informatik.tu-chemnitz.de, https://orcid.org/0000-0002-3032-5725

[2] Technische Universität Chemnitz, Soziologie mit Schwerpunkt Technik, Thüringer Weg 9, 09126 Chemnitz, Deutschland, karola.koepferl@hsw.tu-chemnitz.de, https://orcid.org/0009-0001-5360-3927; tanja.lehmann@hsw.tu-chemnitz.de, https://orcid.org/0000-0003-1647-369X; andreas.bischof@hsw.tu-chemnitz.de, https://orcid.org/0000-0003-0437-9794

[3] Hochschule Anhalt, Fachbereich Informatik und Sprachen, Bernburger Straße 55, 06366 Köthen (Anhalt), Deutschland, alexa.becker@hs-anhalt.de, https://orcid.org/0000-0002-9761-3211; arne.berger@hs-anhalt.de, https://orcid.org/0000-0002-6398-839X

doi:10.18420/inf2024_65

Produkte jedoch, wenn der Gewinn an Bequemlichkeit groß genug ist [WNC16]. Dieser Zusammenhang wird als Privacy Paradox bezeichnet [GGV18].

Doch was ist, wenn man die Hersteller als vermeintlich übermächtige Dritte, als „Big Brother“ mit ihren Cloud-Lösungen, aus der eigenen Wohnung aussperren würde? Würden in dieser Form der digitalen Souveränität sich dann alle Bedenken und Probleme zur Privatsphäre von Smart Home Technik einfach auflösen?

Auf Basis von drei Fallbeispielen zeigen wir, dass es doch nicht so einfach ist. Wir schließen mit einem Blick auf unsere aktuelle Forschung und dem Ansatz Privacy by Co-Design.

2 Drei Fallbeispiele und Analyse

Im Folgenden stellen wir drei Beispiele, zum Einsatz einfacher Sensoren in Privathaushalten, ohne Hersteller und Cloud, die auf [Ku20; Ri18; Tr18] beruhen, sowie eine Analyse vor.

Beispiel 1: Wie in [Ku20; Ri18] beschrieben, hat die Ehefrau in einem Studienhaushalt bewusst die Daten eines Bewegungssensors an der Wohnungstür genutzt, um die Aussagen des Ehemannes zum Betreten bzw. Verlassen der Wohnung auf Plausibilität und damit auf ihren Wahrheitsgehalt zu überprüfen. Nach der Konfrontation des Mannes mit den Daten, welche zeigten, dass nach dem Betreten der Wohnung durch den Ehemann am frühen Nachmittag die Wohnungstür bis zum Kommen der Ehefrau am Abend nicht bewegt wurde, zeigte dieser sich sichtlich überrascht und unterstellte seiner Frau, ihn zu überwachen. Es wurde also das Wissen um den Sensor, den Zugriff auf die erzeugten Daten und die erlernte Fähigkeit diese zu interpretieren genutzt, um den Mann, ohne sein Wissen, zu überwachen.

Beispiel 2: Zu Einsatzmöglichkeiten einfacher Sensoren befragt, berichtet in [Ku20] eine Mutter über die Nutzung der Sensoren im Kinderzimmer ihres Sohnes mit dem Ziel, Kenntnis über verspätetes Nachhausekommen, die Nutzung von elektronischen Geräten sowie Schlaf- und Wachzeiten zu haben. Dazu sollten ein Bewegungssensor an der Tür, ein Lichtsensor im Zimmer zur Messung der Helligkeit von Zimmerleuchte, Leselampe und Bildschirmen, sowie ein Bewegungssensor am Bett die Daten liefern. Kinder haben selten ein Mitspracherecht, wenn es um den Kauf oder die Installation von Sensoren geht, und, wenn überhaupt, nur eingeschränkten Zugang zu gesammelten Daten. Selbst einfache Sensoren können so Eltern ermöglichen ihre Kinder im Zuhause umfassend zu kontrollieren, was von den Kindern kaum eingeschätzt und weder hinterfragt noch beeinflusst werden kann.

Beispiel 3: Im Rahmen der Studie „Wunderliche Sensoren“ [Tr18] sollten die Sensoren im Laufe der Zeit falsche, unlogische und verwirrende Daten aus dem Haushalt anzeigen. Ein Sensor wurde dabei an der Kühlschranktür befestigt. Die Mieterin und ihr Partner hatten sich vorher, unabhängig von der Studie, auf das Einhalten eines strikten Diätplanes geeinigt. Die Mieterin kontrollierte ihren Partner in ihrer Abwesenheit, ob dieser den Kühlschrank

öffnete. Bei erkanntem vermeintlichen Fehlverhalten wurde der Partner mit den Daten konfrontiert und an die Absprache erinnert, also mit Zielsetzung einer Verhaltensänderung.

Unwissenheit zum Vorhandensein der Technik und exklusiver Zugang zu den Daten: Einfache Sensoren lassen sich durch geringe Größe, drahtlose Konnektivität und Energiesparsamen Betrieb unauffällig und ohne Kabel platzieren. Somit kann eine Person aus dem Haushalt, meist mit überlegenen technischen Kenntnissen, eigenmächtig Sensoren installieren und das Wissen dazu für sich behalten. Im Beispiel 1 ist es die Frau, meist aber der Mann [Ta21]. Damit wird die dominante Position im Haushalt gefestigt und verstärkt. Gleiches gilt auch für das Machtgefälle zwischen Eltern und Kindern oder zu Mitbewohnern im Haushalt (Beispiele 2 und 3). Ein Zugriff auf Daten setzt voraus, dass man überhaupt weiß, dass es die Sensoren gibt, welche Daten diese erheben, wo diese gespeichert sind und dass man Zugangsdaten und -berechtigung hat. Dabei ist es letztlich egal, wo die Daten gespeichert werden, ob in der Cloud oder ausschließlich lokal.

(Un-)Fähigkeit zur Interpretation sowie Unter- und Überschätzung der Aussagekraft: Die Daten einfacher Sensoren sind abstrakt (z. B. Beschleunigungswerte, gezählte Bewegungsereignisse oder Helligkeit in Lux) und sprechen im Gegensatz zum Bild einer Kamera oder Audioaufzeichnungen nicht für sich selbst. Oft wird die Interpretation dieser Art von Daten erst durch den Einbezug von Kontext und situiertem Wissen [Ha88] ermöglicht. Diese Interpretation der abstrakten Sensordaten muss nicht objektiv korrekt sein, sondern nur plausibel genug für eine intersubjektive Wahrheit [Ku20]. Einfache Sensordaten lassen meist auch andere Interpretationen zu oder verführen sogar zu falschen Aussagen [Ku20]. Die Fähigkeit zur Interpretation der Sensordaten muss erlernt werden, ebenso wie die Erkenntnis, diesen Daten und Interpretationen nicht vorbehaltlos zu vertrauen, was den Zugriff auf die Daten voraussetzt.

Nutzung für eigene Zwecke: Die Fähigkeit, Sensordaten Sinn zu geben, erlaubt die Nutzung für eigene Zwecke. Oft sind diese Zwecke durchaus positiv, z. B. auf Komfort, Sicherheit und Effizienz ausgerichtet, was sich in den Erwartungen der Nutzenden [Te23], ihren tatsächlichen Nutzungen [Ku20] und den Versprechungen der Hersteller widerspiegelt. Trotzdem ergeben sich aber auch kritische Nutzungen: teils gezielt, teils auch eher versehentlich als Beiprodukt positiver Nutzungsziele [Be23], in den Beispielen 2 und 3 aus Fürsorge oder Sorge um Gesundheit. Die zuvor diskutierten Machtgefälle verstärken dabei die Grundlage für missbräuchliche Nutzung der Daten [Ri18] bis hin zu Überwachung. Die Beispiele zeigen anschaulich, dass dies im Kontext des Zuhauses laterale Überwachung ist, also auf gleicher Ebene zwischen Bewohnern stattfindet.

Die Analyse legt nahe, dass die bloße Verfügbarkeit von Sensordaten in Haushalten dazu führen kann, dass Individuen beginnen, diese Daten zu interpretieren und für eigene Zwecke zu nutzen – für positive wie auch problematische, was bestehende Machtungleichgewichte sichtbar macht oder verstärkt. Die analysierten Dynamiken sind nicht nur ein Nebenprodukt der Nutzung von Smart-Home-Technologien, sondern treten in solchen technologisch

erweiterten Umgebungen immanent auf – ohne externe Dritte als übermächtiger „Big Brother“ und ohne dass die Sensordaten überhaupt den Haushalt verlassen haben.

3 Forschungsansatz Privacy by Co-Design

Die Analyse verdeutlicht, dass selbst für einfache Sensoren keine einfachen Lösungen, sondern eher boshaft verzwickte Implikationen zu erwarten sind [KB21]. Die dargelegten Probleme lassen sich zwar analysieren, für Nutzer:innen sind sie jedoch schwer verständlich und meist noch schwerer adressierbar. Daher widmet sich das Projekt *Simplications* (BMBF, 2023–2026) gezielt diesen Punkten. Im Folgenden erklären wir dazu unseren partizipativen Forschungsansatz Privacy by Co-Design.

3.1 Sensorkit und Feldstudien

Bei den für unsere Feldstudien genutzten Sensorkits handelt es sich um ein in sich geschlossenes System mit einfachen Sensoren für Temperatur, Bewegung, Licht und Luftfeuchtigkeit auf Basis von [Be18; Ku22]. In Simplications erweiterten wir die Zusammenstellung um einen Luftqualitätssensor (Konzentration flüchtiger organischer Verbindungen und CO_2) sowie einen Lautstärkesensor. Die Sensoren sind per Bluetooth Low Energy bzw. WLAN mit einem Raspberry Pi verbunden, welcher die Messdaten der Sensoren aufzeichnet und in einer lokalen Datenbank speichert. Die Teilnehmer:innen der Studie können innerhalb ihres Haushalts auf die aufgezeichneten Daten mittels eines Tablets zugreifen und so eigenständig Visualisierungen der erfassten Sensordaten explorieren.

Die Sensorkits werden für einen Zeitraum von zehn bis 14 Tagen in acht Haushalten installiert. Am ersten Tag erfolgt die Übergabe des Sensorkits an die Teilnehmer:innen und die Einrichtung des Sensorkits in der Wohnung mit den Forscher:innen. Zudem werden ein Aufbauinterview durchgeführt und Feldnotizen angefertigt. In einem Aufgabenheft sind für jeden Tag Aufgaben vorgegeben, welche zum Erkunden der Daten und später auch zum Verändern der Position der Sensoren einladen. Am letzten Tag wird das Sensorkit wieder abgebaut und ein Abbauinterview durchgeführt. Etwa zehn Tage nach dem Abbau kommen die Teilnehmenden von zwei bzw. drei Haushalten zum Gruppenformat *Daten-Raten* [Ku20] zusammen. Darin werden ihnen anonymisierte Ausschnitte der gesammelten Sensordaten vorgelegt. Moderiert wird dann gemeinsam interpretiert, was die Daten zeigen, aus welchem Haushalt sie stammen und welche möglichen Implikationen sich daraus ergeben könnten.

3.2 Preliminary Findings

Im Frühjahr 2024 wurde eine erste Feldstudienphase durchgeführt, eine weitere ist im Herbst geplant. Die Auswertung der Interviews und Daten-Raten-Sitzungen ist noch nicht

abgeschlossen, erste Ergebnisse in Richtung der gezeigten Beispiele liegen jedoch bereits vor. So zeigt sich beispielsweise, dass technisch versierte Nutzer von Smart-Home-Geräten sich viele Gedanken über die technische Absicherung ihrer Daten machen, dabei jedoch oft den Blick für die Privatsphäre innerhalb des Haushaltes verlieren. Die Abkehr von großen Konzernen kann zwar die Überwachungsintensität durch diese Akteure reduzieren, jedoch die skizzierten Probleme innerhalb von Haushalten nicht vollständig beseitigen. Aus soziologischer Perspektive lässt sich argumentieren, dass Technologie, ähnlich der von Jürgen Habermas formulierten These der „Kolonialisierung der Lebenswelt“ [Ha95], Normen schafft, die durch technische Artefakte soziale Beziehungen der Individuen steuern. Die Individuen sind demnach an der Herstellung, dem Betrieb und der Nutzung der Artefakte beteiligt [He92].

3.3 Ausblick

Da wir auf lebensweltlich generiertes Wissen aus den Studien zusammen mit den zukünftigen Nutzer:innen angewiesen sind, wir dieses Wissen aber auch in deren Lebenswelt zurückspiegeln werden, nennen wir dies ***Privacy by Co-Design*** und fügen so den Ansätzen *Privacy by Design* und *Privacy by Default* das Element der Partizipation hinzu.

Implications for Use – Was lässt sich aus dem Entstehen der Privatsphäreimplikationen für die Nutzung smarter Technik lernen? Daraus werden Aufklärungs- und Bildungsmaterialien als Handreichungen zur eigenverantwortlichen Auswahl und Nutzung smarter Technik sowie zur Datenfreigabe und -weitergabe erarbeitet.

Implications for Design – Was lässt sich aus dem Entstehen der Privatsphäreimplikationen für die Entwicklung smarter Technik lernen? Daraus werden Hinweise an die Technikentwicklung abgeleitet, um vor allem die Datenerfassung und -interpretation von Anfang an privatsphärefreundlich zu gestalten.

4 Zusammenfassung

Ein einfacher Sensor, einseitiger Zugang zu Daten, das Interpretieren mit situiertem Wissen, bestehende Machtgefälle und eine Prise Neugier können eine Gefahr für die Privatsphäre darstellen, auch ohne Konzerne, „Big Brother“ oder Cloud. Wir zeigten dies mit drei Beispielen und ihrer Analyse. Das Projekt *Simplications* widmet sich der Findung relevanter Probleme durch Sensoren im Zuhause für die Privatsphäre, ausgehend von der Lebenswelt der Nutzenden, über die Analyse und Aufarbeitung entstehender Implikationen bis zu ihrer Adressierung. Wir werden mit der weiteren Auswertung unserer ersten Studie und der Durchführung einer zweiten zu konkreten Hilfestellungen zur privatsphärefreundlichen Nutzung von Smart Home Technik beitragen. Diese soll sich sowohl auf die Implications for Use als auch auf die Implications for Design beziehen.

Danksagungen

Diese Arbeit ist gefördert vom Bundesministerium für Bildung und Forschung (BMBF) FKZ 16KIS1868K.

Literaturverzeichnis

[Be18] Berger, A. et al.: Sensing Home: Designing an Open Tool That Lets People Collect and Interpret Simple Sensor Data from Their Homes. i-com 17 (2), Publisher: Oldenbourg Wissenschaftsverlag, 2018, ISSN: 2196-6826, DOI: 10.1515/icom-2018-0013, Stand: 07. 05. 2024.

[Be23] Berger, A. et al.: Accidentally Evil: On Questionable Values in Smart Home Co-Design. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. CHI 2023. CHI'23, ACM, New York, NY, USA, S. 3, 2023, Stand: 07. 05. 2024.

[GGV18] Gerber, N.; Gerber, P.; Volkamer, M.: Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior. Computers & Security 77, S. 226–261, 2018, ISSN: 01674048, DOI: 10.1016/j.cose.2018.04.002, Stand: 01. 03. 2024.

[Ha88] Haraway, D.: Situated Knowledge: The science Question in Feminism and the Privilege of Partial Perspective. Feminist Studies 14, S. 579–599, 1988, DOI: 10.2307/3178066, Stand: 07. 05. 2024.

[Ha95] Habermas, J.: Theorie des kommunikativen Handelns. Suhrkamp, Frankfurt am Main, 1995.

[He92] Hennen, L.: Technisierung des Alltags. VS Verlag für Sozialwissenschaften, Wiesbaden, 1992.

[KB21] Kurze, A.; Bischof, A.: Wicked Implications for Human Interaction with IoT Sensor Data. In: Workshop Human-Data Interaction through Design at Conference on Human Factors in Computing Systems (CHI '21). May 9, 2021. 2021, DOI: 10.48550/arXiv.2201.10470, Stand: 07. 05. 2024.

[Ku20] Kurze, A. et al.: Guess the Data: Data Work to Understand How People Make Sense of and Use Simple Sensor Data from Homes. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. ACM, Honolulu HI USA, S. 1–12, 2020, ISBN: 978-1-4503-6708-0, DOI: 10.1145/3313831.3376273, Stand: 07. 05. 2024.

[Ku22] Kurze, A.: Senseful Sensors: Learnings and Optimizations for IoT Sensors in HCI Research. In: 2022 IEEE 9th International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA). CIVEMSA. ISSN: 2377-9322, S. 1–6, 2022, DOI: 10.1109/CIVEMSA53371.2022.9853698, Stand: 07. 05. 2024.

[Ri18] Richter, J. et al.: Machtförmige Praktiken durch Sensordaten in Wohnungen. Mensch und Computer 2018 Tagungsband, 2018, DOI: 10.18420/muc2018-mci-0253, Stand: 07. 05. 2024.

[Ta21] Tanczer, L. M.: Das Internet Der Dinge: Die Auswirkungen »smarter« Geräte Auf Häusliche Gewalt. In (Prasad, N., Hrsg.): Geschlechtsspezifische Gewalt in Zeiten Der Digitalisierung. 1. Aufl., Formen Und Interventionsstrategien, transcript Verlag, S. 205–226, 2021, JSTOR: jj.11425490.13, Stand: 07. 05. 2024.

[Te23] Technikradar: TechnikRadar 2023: Was die Deutschen über Technik denken, acatech, Körber-Stiftung, Universität Stuttgart, 2023, URL: https://www.acatech.de/publikation/technikradar-2023/, Stand: 01. 03. 2024.

[Tr18] Traubinger, V.: Wunderliche Sensoren im Internet der Dinge. In. Mensch und Computer 2018 - Tagungsband. Gesellschaft für Informatik e.V., 10.18420/muc2018, 2018, DOI: 10.18420/muc2018-mci-0408, Stand: 07. 05. 2024.

[Wa23] Walker-Munro, B.: Hyper-Collection: A Possible New Paradigm in Modern Surveillance. Surveillance & Society 21 (2), S. 120–138, 2023, DOI: 10.24908/ss.v21i2.15770, Stand: 07. 05. 2024.

[We19] West, E.: Amazon: Surveillance as a Service. Surveillance & Society 17 (1/2), S. 27–33, 2019, ISSN: 1477-7487, DOI: 10.24908/ss.v17i1/2.13008, Stand: 07. 05. 2024.

[WNC16] Williams, M.; Nurse, J. R. C.; Creese, S.: The Perfect Storm: The Privacy Paradox and the Internet-of-Things. In: 2016 11th International Conference on Availability, Reliability and Security (ARES). IEEE, Salzburg, Austria, S. 644–652, 2016, ISBN: 978-1-5090-0990-9, DOI: 10.1109/ARES.2016.25, Stand: 07. 05. 2024.