Privacy-Fatique und (fehlende) Risikonarrative im Smart Home

Franziska Baum, Andreas Bischof, Tanja Lehmann

TECHNISCHE UNIVERSITÄT
IN DER KULTURHAUPTSTADT EUROPAS
CHEMNITZ

HOCHSCHULE ANHALT University of Applied Sciences

Verbraucherzentrale Sachsen

Bundesministerium für Forschung, Technologie und Raumfahrt

FKZ 16KIS1868K

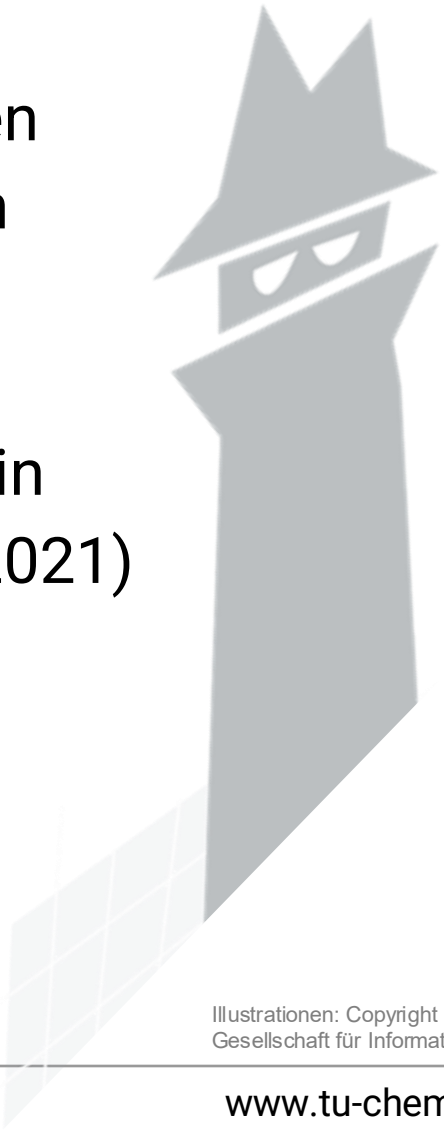
Agenda

1. Ausgangslage: Risikonarrative rund ums Smart Home
2. Forschungswerkzeug Sensorkit & Studiendesign
3. Typische Fallstrukturen
    a) Admins
    b) Standardnutzer
    c) Die gute Mutter
    d) Die Miele-Rentner
    e) Die passiven Nutzer*innen
4. Herausforderungen & Handlungsempfehlungen

Ausgangslage: Risikonarrartive rund ums Smart Home

1. Sicherheit und Komfort durchs Smart Home
   Risiken durch Abwesenheit minimieren, Zugang verstetigen und ermöglichen (Smart Locks) + individualisierter Nutzen
2. Privatheitsrisiken
   Cyberangriffe bzw. Zugriff von Außen
   Personalisierung = Datenprofile, z.B Wohnungsgrundriss in der Cloud, Rauchmelder als „emerging risks“ (Iten et al. 2021)

3. Risiken durch Anwendung im Haushalt
   intimate surveillance, datafied motherhood, bystanders, secondary users, Auswirkungen auf Nutzende selbst



Motivation und Studiendesign

- Technik im smarten / vernetzten Zuhause und Privatheitsrisiken
- Vermeintlich „einfache“ Sensoren

Image: Projekt_Kaffeebart on Pixabay

Problemstellung:

- Steigende Anzahl smarter Geräte im Smart Home, mit einfachen Sensoren (z. B. integriert im Kühlschrank, TV für Temperatur, Luftfeuchte, Stromverbrauch, …)
- Sammlung großer Mengen von Daten & Verwertung durch Plattformkonzerne durch Algorithmen (z. B. Morgner et al. 2017, Laput et al. 2017)

Zielsetzung:

- **Soziale Situiertheit und Privatheitsrisiken innerhalb des Haushalts**
- Sinngebungen anhand einfacher Sensordaten: Erkennung von Anwesenheit, typischer häuslicher Aktivitäten
  - durch Menschen mit Einbezug von Hintergrundwissen zum Kontext Zuhause (z. B. Tolmie et al. 2016, Kurze et al. 2020)
  - Missbrauch von Sensordaten von Bevormundung bis Überwachung möglich (z. B. Kurze et al. 2020, Berger et al. 2023)
- Implikationen der Nutzung: eigene Gefahren, die bislang nicht gut erforscht sind
- Problembewusstsein und Verständnis für **Risiken und Implikationen** für Privatheit innerhalb des Haushalts schärfen

Forschungswerkzeug Sensorkit

Forschungsfragen:

- Welche Akteurskonstellationen sind besonders kritisch?
- Welche Datennutzungen und Interpretationen sind kritisch?
- Implikationen für Nutzung: Welche Privatheitsrisiken lassen sich durch eine informierte Nutzung vermeiden oder minimieren?

Sensorkit: Datensammlung mit SensorTags
= klein, leicht, drahtlos, multifunktional, flexibel
erfassen: Licht, Bewegung, Temperatur, Luftfeuchte, Luftdruck, Lautstärke und Luftqualität

+ Dateninteraktion über **Visualisierungen**
(iPad mit Browser)

+ Datenreflektion über Material zur Dokumentation,
& **Gruppendiskussionen**

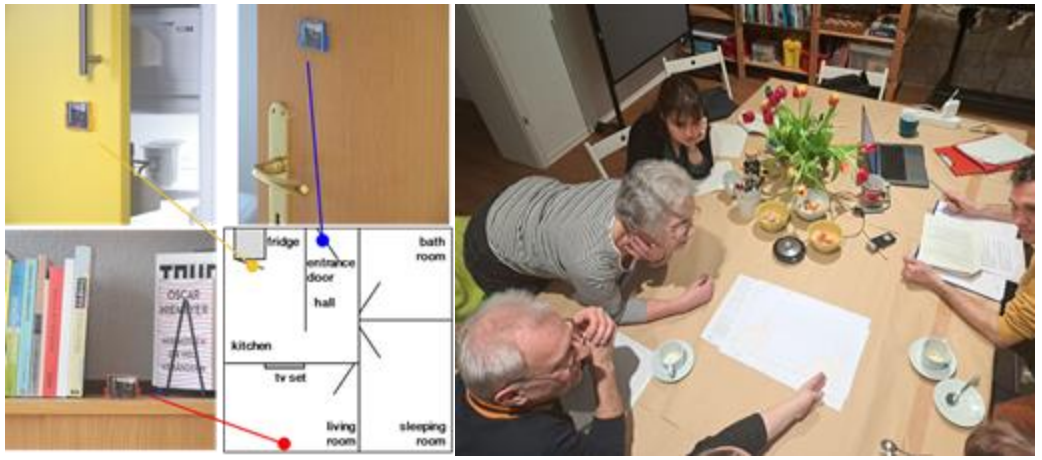
Daten-Browsing

Daten-dokumentation

Forschungswerkzeug Sensorkit

Studie

- zwei Feldphasen (2024 & 2025)
- 18 Haushalte x 10-14 Tage Laufzeit
- 36 Auf- und Abbauinterviews
- 6 Gruppendiskussionen „Datenraten“



Diversifiziertes Sample

- **Selbstselektion auf öffentliche Aufrufe**
- 1. Feldphase v.a. ältere Ehepaare im Ruhestand (60-70 J) & tech-affine Männer mittleren Alters (30-50 J)
- 2. Feldphase zusätzlich 2 Familien mit Kindern + Schichtarbeit (30-40 J), 2 Studierendenhaushalte (1 WG) (20-30 J), 1 alleinstehende Frau im Ruhestand
- typischerweise: “technische Drahtzieher” (BSI 2025) vs. sehr kritische Personen (“Das kommt mir nicht ins Haus”)

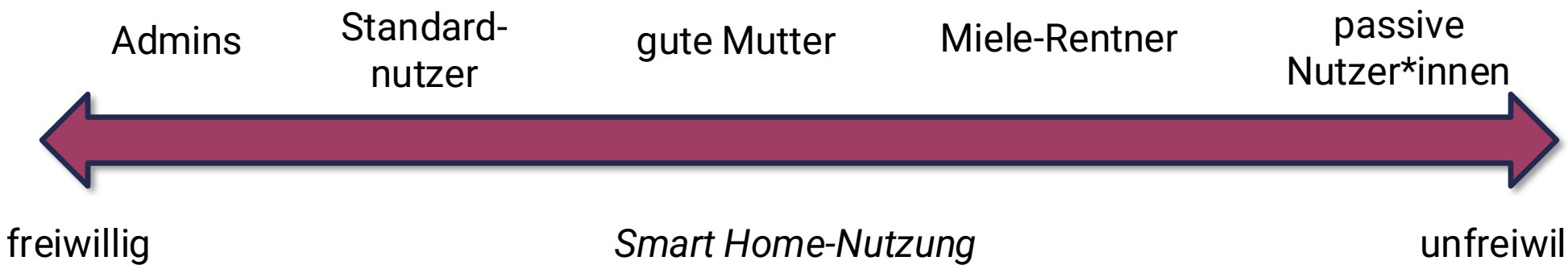
Typische Fallstrukturen

gebildet anhand folgender Kategorien:

- **Wohnsituation**: bspw. zur Miete / Eigentum
- **Wissen/Kompetenz:** über Smart Home-Technik
- **Kontrolle:** Kaufentscheidung, Zugriff auf Daten in Interface, weiterer Datenfluss?
- **Typische Nutzung des Sensorkits**: Wofür?, bspw. Schlaf überwachen

- **Risikobewusstsein**: Inwiefern vorhanden/ausgeprägt? Betroffenheit in der Vergangenheit
- **Aushandlungen (mit Mitbewohner:innen):** Welche expliziten Aushandlungen über Einsatz finden statt?
- **Blinde Flecken:** Welche Widersprüche oder Unwissenheit zeigt sich in der Nutzung?

Befund: "Unfreiwilliges Smart Home"; eine:r schafft an/willigt ein, andere sind betroffen



Typische Fallstrukturen

Technik-Verantwortliche (Admins)

Die Vorstellung von absoluter Sicherheit & Kontrolle, ”wenn man nur will”

Risikobewusstsein: Hat alles angeschafft und eingebaut, glaubt er hat alles im Griff (für immer), kein Risikobewusstsein, weil alles im eigenen Netz mit VPN läuft

Aushandlungen (mit Mitbewohnern): Partnerin wird schon gefragt, aber grundsätzlich “auf meinem Mist gewachsen” (T6m), WAF-Faktor=Reproarbeitserleichterung als Zustimmungsfaktor, Anstand und Gleichberechtigung sowie langjährige Beziehungsdynamiken = F2-T5m = achtet auf Wünsche, z.B, dass Partner:innen auch noch per Schalter bedienen können

Blinde Flecken: Eigene Machtposition, eigene Vergänglichkeit, eindeutige Spuren intime Überwachung

Typische Fallstrukturen

Der kommerzielle Nutzer

„*life assistance*“: Komfort sticht Problembewusstsein

Risikobewusstsein: Bewusstsein darüber, welche Bewegungsdaten ggf. nachvollziehbar sind; Werbung auf dem Smartphone wird als Hinweis gedeutet,

Aushandlungen (mit Mitbewohnern): Er entscheidet über Anschaffungen und überzeugt Familie etc. bzgl. Nutzen

Blinde Flecken: Überwachung und Macht durch Datenzugriff (Familie/Freunde/Partnerin), Ausblenden der kommerziellen Verwertung und Nutzung der Daten, obwohl dies über Drittanbieter erfolgt, Kontrolle des Gartens/Hund wichtiger als Rechte von Besuchern/Mitüberwachten, Nachvollziehbarkeit des gesamten aber auch des eigenen Tagesablaufs

Typische Fallstrukturen

Die “gute” Mutter
Laterale Überwachung im Kinderzimmer

Risikobewusstsein: kaum vorhanden, häufig kein Bewusstsein darüber, welche Bewegungsdaten etc. von ihr nachvollziehbar sind; Bedenken des Kindes wird nicht ernst genommen

Aushandlungen (mit Mitbewohnern): Sie entscheidet und hat scheinbar Hauptlast der Kinderbetreuung & Technikzugang

Blinde Flecken: Überwachung und Macht durch Daten, kommerzielle Verwertung und Nutzung der Daten, sofern dies über Drittanbieter erfolgt, Zugriff der Drittanbieter auf Kinderzimmerdaten; Nachvollziehbarkeit des gesamten aber auch des eigenen Tagesablaufs, Interpretierbarkeit der Daten ggf. immer auch als Nachweis gegen die Intention: Kind guckt jeden Tag fern vs. Immer nur eine Stunde, Negative Effekte der Selbstüberwachung

Typische Fallstrukturen

Die Miele-Rentner:

Accidental Smart Home durch Investment in hochwertige Geräte & Markentreue

Risikobewusstsein: fragt sich, was ihre Geräte versenden/weitergeben (Studienmotivation); unklare Verwertungsabsichten, TN ist Versprechen der Verkäufer & Hersteller ausgeliefert, dass ihre Daten sicher sind

Aushandlungen (mit Mitbewohnern): Ehemann kommt kaum vor (Reproduktionsarbeit), aber vertrauensvoller Zugang der Familie zu allen Anwendungen (Tochter ist bei Tür registriert) da gemeinsame Anschaffung

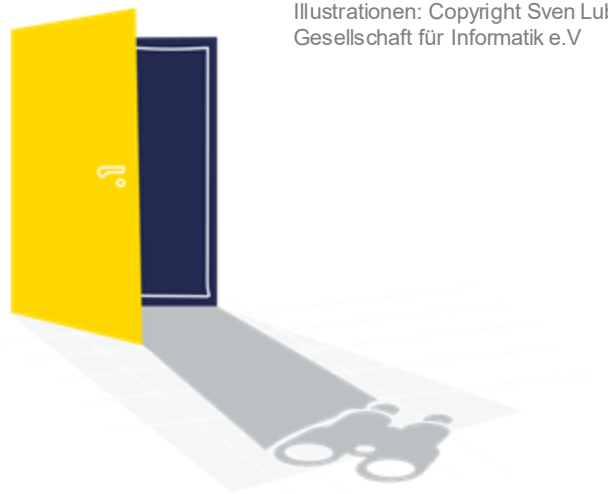
Blinde Flecken: Überwachbarkeit durch eigene Familie, konkrete kommerzielle Verwertung und Nutzung der Daten; Überwachung/Machtposition von Hausangestellten, z. B. der eigenen Haushaltshilfe

Typische Fallstrukturen

Die “passiven Nutzer”INNEN

Überlassen bis zur Überwachung

„das ist sein Projekt“



Risikobewusstsein: kaum vorhanden, siehe Aushandlung, häufig kein Bewusstsein darüber, welche Bewegungsdaten etc. von ihr nachvollziehbar sind.

Aushandlungen (mit Mitbewohnern): Partner sichert das Smart-Home nach außen ab, vertrauensvolle, oft jahrelange Partnerschaft mit klaren Zuständigkeiten

Blinde Flecken: Überwachbarkeit durch eigenen Partner, kommerzielle Verwertung und Nutzung der Daten, sofern dies über Drittanbieter erfolgt

3.) Herausforderungen & Handlungsempfehlungen

Zentraler Befund: Bedeutung des *unfreiwilligen* *Smart Homes*

- Frauen und Kinder als überwachte und “least capable user” aus Sicht der Admins und Installateure
- Überwachung durch Assistenzfunktionen („Smart Care“)
- Mieter:innen und unfreiwilliges Smart Home

Herausforderungen:

- allgemeine Fatique hinsichtlich Datenschutzverantwortung bzw. Umsetzung von Datenschutz als individuelle Aufgabe
- Fehlende Wahrnehmung von sich selbst als Betroffene & Problem

Handlungsempfehlungen

1.)Privatheitsrisiko beginnt schon bei fehlendem gleichberechtigtem Zugang: **Gewaltschutzansatz** in Governance, Beratung und Gestaltung von Smart Home-Nutzung integrieren (*Dual Use*).

2.) Gezielte **Informations- und Schulungsangebote** für unfreiwillige und vulnerable Nutzer*innen-Gruppen, insb. Frauen & Kinder zu ihren spezifischen Risiken im Smart Home notwendig

3.) Nutzung smarter Technologien als ***sozialer Aushandlungsprozess*** verstehen, der **informierte Einwilligung** und bewusste Partizipation aller Betroffenen erfordert.

Key Take Aways:

- Bedeutung des *unfreiwilligen Smart Homes* und deren Risiko
- Betroffene & Nutzungstypen mit unterschiedlichen Zugängen zu smarter Technik
- Blindspot Sicherheit: *Verstetigung von bestehenden Machtstrukturen* im Privathaushalt; Private Räume ≠ sichere Räume für alle
- *Aushandlungen und informierte Einwilligung* erforderlich

Vielen Dank!

Fragen? Kommentare? Anregungen?

Let's keep in touch:
franziska.baum@hsw.tu-chemnitz.de