Human-Centered Privacy in Intelligent Environments

Dissertation

an der Fakultät für Mathematik, Informatik und Statistik
der Ludwig-Maximilians-Universität München

vorgelegt von

Maximiliane Windl

M.Sc. Media Informatics

München, den 1. Juli 2025

Erstgutachter:	Prof. Dr. Albrecht Schmidt
Zweitgutachter:	Prof. Dr. Florian Schaub
Drittgutachter:	Prof. Dr. M. Angela Sasse

Tag der mündlichen Prüfung: 21. Oktober 2025

Abstract

Advancements in technology have transformed our everyday environments into intelligent, sensor-rich spaces. While technologies such as smart home devices, augmented reality, and radio frequency sensing bring various benefits and make life more convenient and enjoyable, they also expose users to significant privacy risks. However, users often lack awareness and understanding of how their data is collected, processed, stored, and shared. At the same time, they lack mechanisms that help manage privacy effectively. Technology designers and researchers have the opportunity to support users by creating privacy-friendly devices and mechanisms. However, they must carefully balance privacy considerations with maintaining rich features and ensuring engagement in users' primary tasks. Overly strict privacy measures can deter adoption, especially since many users consider privacy management a low priority. It is rarely a primary goal but rather a secondary concern that arises alongside the main use case.

This thesis outlines a vision of privacy mechanisms that seamlessly integrate into users' daily routines and effectively empower them to claim autonomy and exercise agency over their privacy. To realize this vision, we require (1) a thorough understanding of users' privacy concerns and the factors shaping their perceptions of privacy risks to (2) design effective interventions to mitigate these concerns. Consequently, this thesis outlines a vision of a privacy-preserving future among advanced, sensor-rich technologies. In this thesis, we first investigate how users perceive and interact with privacy risks in intelligent environments. Second, we design and evaluate innovative, human-centered solutions to address these concerns.

The first part of this dissertation examines privacy concerns in intelligent environments. We conducted surveys, interviews, and focus groups to understand how users perceive privacy risks and navigate data practices. In detail, we explored concerns in smart homes, focusing on bystanders' perspectives on mobile and smart home technologies and users' understanding of interconnected interactions involving mobile phones and smart devices. We further examined people's experiences with privacy violations in the physical world and investigated people's understanding and concerns about emerging technologies, such as advanced domestic robots and radio frequency sensing. These systematic investigations offer new insights into people's privacy concerns and establish a foundation for designing effective, user-centered solutions.

The second part of this thesis develops and evaluates innovative privacy solutions and interventions, focusing on empowering users to claim autonomy and exercise agency over their privacy. We proposed two conceptual frameworks: one for designing effective consent mechanisms for spontaneous interactions in augmented reality and one for addressing privacy violations in the physical world. We further proposed communication patterns enabling domestic robots to convey their privacy-relevant states to users effectively. We then created interactive privacy labels that inform users about the privacy implications of smart home devices and support control and use-case-based interactions. Finally, through three studies, we explored tangible privacy interfaces for smart homes, resulting in a cross-ecosystem privacy hub. We evaluated this hub in an in-the-wild study, delivering unique insights into lived experiences with a tangible privacy control system.

Based on our findings from the first part of this dissertation, I propose a conceptual model for privacy concerns in intelligent environments, outlining how personal, technological, and situational factors impact privacy concerns. Next, condensing the insights from the dissertation's second half, I present a research playbook for human-centered privacy mechanisms in intelligent environments. The framework integrates theoretical insights and practical findings to guide the design of future privacy-preserving technologies. I designed the framework as a resource for researchers and designers aiming to create systems that align privacy practices with user needs.

Overall, this thesis contributes (1) a comprehensive understanding of people's privacy concerns and mental models in intelligent environments, (2) innovative systems, tools, and comprehensive concepts to enhance privacy awareness and control, (3) a conceptual model for privacy concerns in intelligent environments, (4) a research playbook to elicit effective human-centered privacy mechanisms for intelligent environments, and (5) reflections on methods in privacy research and the future of privacy in intelligent environments. I envision human-centered privacy solutions that reduce the burden on individuals while making privacy management seamless and engaging. By developing a deep understanding of people's privacy concerns and creating several privacy mechanisms and frameworks, this thesis lays the groundwork for a future where privacy and innovation coexist.

Zusammenfassung

Unser Alltag hat sich durch technologischen Fortschritt zunehmend in intelligente, sensorreiche Umgebungen verwandelt. Smart-Home-Geräte und Technologien wie Augmented Reality und radiofrequenzbasierte Sensoren haben zahlreiche Anwendungen und versprechen, das Leben komfortabler und angenehmer zu machen. Gleichzeitig setzen diese Technologien Nutzerinnen und Nutzer erheblichen Datenschutzrisiken aus. Häufig fehlt es jedoch an Bewusstsein und Verständnis dafür, wie persönliche Daten erfasst, verarbeitet, gespeichert und weitergegeben werden. Zudem mangelt es an wirksamen Mechanismen zur Kontrolle über die eigenen Daten und die eigene Privatsphäre. Hier liegt eine zentrale Herausforderung für die Gestaltung datenschutzfreundlicher Technologien, die Funktionalität, einfache Benutzbarkeit und Datenschutz in Einklang bringen. Zu strenge Datenschutzmaßnahmen können die Akzeptanz mindern – insbesondere, da viele Menschen den Schutz ihrer Privatsphäre nicht als vorrangiges Ziel, sondern eher als eine begleitende Aufgabe erachten.

Diese Dissertation verfolgt das Ziel, Datenschutzmechanismen menschenzentriert zu entwickeln, die sich nahtlos in den Alltag integrieren und es Nutzenden ermöglichen, Selbstbestimmung und Autonomie über ihre Privatsphäre zu gewinnen, ohne dadurch das Benutzererlebnis zu schmälern. Grundlage dafür sind (1) ein vertieftes Verständnis der zugrunde liegenden Datenschutzbedenken sowie der Faktoren, die die Risikowahrnehmung beeinflussen, und (2) darauf aufbauende, gezielte Interventionen, um diese Bedenken auszuräumen. Die Arbeit eröffnet damit eine fundierte und empirisch abgesicherte Perspektive auf eine datenschutzfreundliche Zukunft im Zeitalter ubiquitärer digitaler Technologien.

Im ersten Teil der Dissertation werden Datenschutzbedenken in intelligenten Umgebungen untersucht. Anhand von Umfragen, Interviews und Fokusgruppen analysiere ich, wie Menschen Risiken wahrnehmen und wie sie mit der Erhebung, Verarbeitung und Weitergabe ihrer Daten umgehen. Im Fokus stehen dabei unter anderem Bedenken im Kontext von Smart Homes aus der Perspektive sekundärer Nutzender. Insbesondere untersuchen wir das Verständnis für vernetzte Interaktionen zwischen Smartphones und smarten Geräten. Darüber hinaus betrachten wir auch Erfahrungen mit Datenschutzverletzungen im analogen Alltag sowie Wahrnehmungen gegenüber neuartigen Technologien wie innovativen Haushaltsrobotern und radiofrequenzbasierten Sensoren. Diese Analysen liefern wertvolle Einblicke in die Bedenken und Bedürfnisse von Nutzenden und bilden die Grundlage für die Entwicklung wirksamer datenschutzfreundlicher Lösungen.

Im zweiten Teil der Arbeit werden neuartige Datenschutzmechanismen entwickelt und empirisch evaluiert, die Menschen zu mehr Kontrolle über ihre Daten befähigen. Dabei stelle ich zwei konzeptuelle Rahmenwerke vor: Das erste befasst sich mit der Gestaltung wirksamer Einwilligungsmechanismen für spontane Interaktionen in Augmented Reality. Das zweite befasst sich mit dem Umgang mit Datenschutzverletzungen im physischen Raum. Darüber hinaus entwickeln wir Kommunikationsmuster, mit denen Haushaltsroboter ihre datenschutzrelevanten Zustände transparent vermitteln können. Darauf aufbauend entstehen interaktive

Privacy Labels, die über die Datenschutzimplikationen von Smart-Home-Geräten informieren und eine fallbezogene und feingranulare Kontrolle ermöglichen. Ergänzend werden in drei Studien greifbare Interaktionsmechanismen für die Einstellung von Datenschutzparametern untersucht. Diese wurden anschließend zu einem plattformübergreifenden System, dem *PrivacyHub,* weiterentwickelt.

Auf Basis der Erkenntnisse aus dem ersten Teil entwickle ich ein konzeptuelles Modell, das zeigt, wie persönliche, technologische und situative Faktoren die Risikowahrnehmung in intelligenten Umgebungen beeinflussen. Im zweiten Teil fasse ich die gewonnenen Erkenntnisse in einem praxisorientierten Leitfaden für nutzerzentrierte Datenschutzmechanismen in intelligenten Umgebungen zusammen. Dieser richtet sich an Forschende sowie an Entwicklerinnen und Designer, die datenschutzfreundliche Systeme entwickeln möchten, die sich konsequent an den Bedürfnissen der Nutzenden orientieren.

Insgesamt leistet die Dissertation einen Beitrag, indem sie (1) ein umfassendes Verständnis von Datenschutzbedenken und mentalen Modellen in intelligenten Umgebungen vermittelt, (2) innovative Konzepte und Werkzeuge zur Förderung von Datenschutzbewusstsein und Kontrolle entwickelt, (3) ein konzeptuelles Modell zur Erklärung von Risikowahrnehmung vorstellt, (4) ein Rahmenwerk für effektive, nutzerzentrierte Schutzmechanismen bereitstellt und (5) methodische Reflexionen zur Datenschutzforschung sowie Ausblicke auf künftige Herausforderungen bietet. Die Arbeit zeigt auf, wie benutzerfreundliche Datenschutzlösungen gestaltet sein können, die sich nahtlos in den Alltag integrieren lassen und das Management von Privatsphäre intuitiv und wirkungsvoll machen. So legt diese Dissertation den Grundstein für einen Ansatz, der Datenschutz, technologische Innovation und Benutzbarkeit in Einklang bringt.

Acknowledgements

First and foremost, I would like to thank my advisor, **Albrecht Schmidt**. Thank you for your trust and constant support, for showing me that hard work pays off, teaching me the value of volunteering, and introducing me to the wonderful HCI community. My sincere thanks also go to **Florian Schaub** and **Angela Sasse** for serving on my thesis committee and for the insightful discussions during my defense. A very special thank you to **Niels Henze**, without whom I would have never started this amazing journey. Another vital person is **Sebastian S. Feger**. Thank you for being a great mentor, the master of discussions and hardware prototyping, but most importantly, a great friend. To **Florian Alt**, thank you for the many conversations about privacy and career advice at the coffee machine. And to **Lorrie Cranor**, thank you for welcoming me at CyLab and teaching me so much about research. I learned an incredible amount during my stay.

The best part of my journey was the many amazing people I met — people I am lucky to now call some of my closest friends. To my dearest office boys, **the Foffice Crew**: I could not decide whom to name first, so I am naming you all at once. **Jan Leusmann**, my favorite coffee nerd with the best dance moves. Thank you for being my friend from the very first moment we met. For the club nights, late-night talks, hikes through Bavarian and Hawaiian mountains, cooking sessions, and everything big and small in between. I am forever grateful to have you in my life. **Julian Rasch**, thank you for being the greatest appreciator of nature, for pointing out every tiny flower and the biggest mountains, for showing me the best places to eat, and for your thoughtful advice and kindness. **Luke Haliburton**, you are the funniest, kindest, lobster-loving Canadian mountain goat I have ever met. Thank you for cheering me up when things went wrong, for teaching me about Canadian folk music, and for all the laughs. **Thomas Kosch**, we were destined to become best friends: Two metalheads lost in academia. Thank you for your endless advice, the beers, the concerts, and the air-guitar solos. Thank you for becoming my honorary brother. I look forward to still headbanging with you 50 years from now. **Steeven Villa**, thank you for crying with me at Iron Maiden, for your warmth and intelligence, and for every deep conversation about science and life. **Sophia Sakel**, my amazing bag-slapping office mate. Thank you for the daily support, for cheering me up, and for joining me at the gym. I am so glad you chose the empty seat in my office. **Teodora Mitrevska**, for being the funniest person I know. Thanks for "sending it" every day and for making my life brighter — you were truly the missing crystal in my life. **Verena Winterhalter**, for your cakes that turned rainy Mondays into sunny Saturdays, for our great time in Seattle, and for teaching me about tea, books, and the little things that make life better. **Clara Sayffaerth**, my favorite emo music and metalcore concert partner, who always has the craziest and most entertaining stories for almost every occasion. **Sarah Völkel**, for being a role model in every way: organized, clever, accomplished, and still incredibly fun. **Francesco Chiossi**, for being the most supportive soul in the office, for your amazing pineapple pasta, and for activating lightspeed mode for happy hour. **Matthias Schmidmaier**, for being the most modern traditional Bavarian friend and for brunches that became full-day events. **Kathrin Schnizer**, for always being kind, open, and putting everyone in a good mood. **Jakob Karolus**, my first office mate and friend. Thank you for all the laughs, music exchanges, stargazing, and the best road trip. **Fiona Draxler**, for showing that one can be clever, organized, and still the life of every party. **Philipp Thalhammer**, for building the best dashboard ever and for squeezing the Squishy. **Carl Oechsner**, for hosting the most legendary WG parties and introducing me to Rüscherl. **Jesse Grootjen**, for being my best Dutch friend and sharing countless teas, coffees, and ski trips. **Henrike Weingärtner**, for interactive captions, Christmas parties, and fun lunch talks. **Yannick Weiss**, for starting this journey with me and for our bakery walks. **Florian Lang**, for being the most German person I know, with the driest humor. **Florian Bemmann**, for submitting our paper a million times and winning an award for it. **Bettina Eska**, for being one of my first friends in the office, a great roommate on trips, and for the most amazing road trip. **Linda Hirsch**, for being my first lunch roulette partner and introducing me to PhD life. **Thomas Weber**, for always being the person to ask about virtually anything and for being an amazing developer. **Nađa Terzimehić**, for the best Bosnian food and for still joining our lab gatherings. **Ceenu George**, for our great collaboration on VR security indicators. **Sarah Delgado Rodriguez**, for being my first privacy buddy and fellow tangible privacy researcher. **Rifat Amin**, for your biryani and ever-friendly presence. **Pascal Knierim**, for great skiing talks and delicious SOUPS. **Katharina Barlage**, for joining us in Munich and not letting me scare you off. **Matthias Hoppe**, for talks about Japan, sumo, and snakes. **Sarah Prange**, for teaching me so much about privacy research early on. **Oliver Hein**, for fun party nights and for being the best publications co-chair. **Khanh Huynh**, **Lukas Mecke**, **Xuedong Zhang**, **Dennis Dietz**, **Lisa Townsend**, **Doruntina Murtezaj**, **Felix Dietz**, and **Viktorija Paneva**, for great research talks and lunch breaks. **Changkun Ou**, **Jingyi Li**, **Sarah Aragon-Hahner**, and **Robin Welsch** — you may have left our lab but never our hearts. **Lewis Chuang**, for your advice and patience at the beginning of my PhD, when I knew nothing. **Andreas Butz**, for inspiring talks about mountains and running and for being a subtle motivator to be more active. **Heinrich Hussmann**, for your early encouragement and genuine excitement for my successes and for being the best tour guide in Venice.

To the many HCI friends from other labs, you make every event even more fun, especially **Anna-Marie Ortloff**, **Florian Müller**, **Passant Elagroudy**, **Anastasiya Zakreuskaya**, **Christopher Katins**, **Christopher Lazik**, **Karo Marky**, **Daniel Buschek**, and **Bastian Pfleging**.

To the amazing people at CyLab who made my stay unforgettable: **Elijah Bouma-Sims**, **Clement Fung**, **Eric Zang**, **McKenna McCall**, **Alejandro Cuevas**, **Trevor Kann**, **Keane Lucas**, **Taro Tsuchiya**, **Brian Singer**, **Omer Akgul**, **Andrea Gallardo**, **Lily Klucinec**, **Alexandra Li**, **Alexandra Nisenoff**, and **Ellie Young**.

Thank you also to the many wonderful people I worked with in various volunteering roles at conferences, especially **Julia Dunbar**, **Ciabhan Connelly**, and **Mikołaj Woźniak** for being the best SV Co-Chairs.

To the students and interns I was fortunate to supervise, especially **Petra**, **Elisa**, **Magdalena**, **David**, **Anna**, **Lina**, and **Ramisa**. Thank you for your curiosity, effort, and inspiration.

A big thank you to **Anja**, for dealing with all of us daily without losing your sanity, and for your life advice. To **Rainer**, for always having the answers: #askRainer. To **Boris**, for guiding the path along unexpected ways and the cat lighter. To **Christa**, **Salsabeel**, **Emma**, and **Franziska**, thank you for all your help with countless little things along the way.

Beyond HCI, I owe so much to the people in my life. **Katja**, my best friend since forever. Thank you for your unwavering support, for understanding when deadlines consumed my time, for the concerts, the trips, the laughter, and for simply being you. Thank you also to **Verena**, **Kirby**, **Lydia and Wolfgang**, **Maike and Hans**, **Andreas**, **Daniel**, **Markus**, and **Karo**.

To my partner, **Sven**. Thank you for your unconditional support, gentle advice, and for cheering me up in hard times. Thank you for all the beautiful adventures: in the tallest mountains, the warmest beaches, the loudest concerts, the most thrilling theme parks, and the quiet moments in between.

Finally, to my amazing family. I could never have done this without you. Thank you for cheering for me and supporting me no matter what. To **Monika** and **Bernhard**, for encouraging me to start this journey and believing in me. Thank you for all the love, support, and the wonderful trips that helped me recharge. To **Helmut** and **Bettina**, for sharing my enthusiasm for HCI and for the many inspiring, funny, and thoughtful conversations that I deeply treasure. Thank you for all the amazing food. To the best sister ever, **Patricia**, thank you for always being there for the big and small problems and for laughing through it all with me. To **Basti**, for your steady calm, thoughtful perspective, and the grounded advice I can always count on. To my wonderful grandparents, **Irmgard** and **Heinz**, **Martha** and **Helmut**. Finally, to **Dagmar**, **Jürgen**, **Pauline**, **Franziska**, **Wolfgang**, and **Max**. Thank you for being my family.

TABLE OF CONTENTS

Publications

This is a cumulative dissertation consisting of research that has been published in established, peer-reviewed venues. These publications comprise the main body of this dissertation. I use the format "[Core$i$]" when referring to these publications.

Additionally, I include four publications to complement the core contributions which I refer to as "[Pub$i$]." Specifically, [Pub1] and [Pub2] contribute to the background section through a privacy control framework and a literature review, and [Pub3] as well as [Pub4] contribute to my methodological reflections in the discussion.

[Core4] received an *Honorable Mention Award* at the 2025 USENIX Security Symposium, [Core3] received the *IAPP Privacy Award* at the 2024 SOUPS Symposium on Usable Privacy and Security, and [Pub3] was awarded with an *Honorable Mention Award* at the 2022 CHI Conference on Human Factors in Computing Systems.

All publications were joint efforts with fellow researchers and students. As such, I use the scientific term "we" when referring to my prior research and only use "I" when specifically discussing thoughts and considerations original to this thesis.

Core Publications

[Core1] Windl, Maximiliane and Mayer, Sven. 'The Skewed Privacy Concerns of Bystanders in Smart Environments.' In: *Proc. ACM Hum.-Comput. Interact.* 6.MHCI (2022). DOI: 10.1145/3546719.

[Core2] Windl, Maximiliane, Schlegel, Magdalena, and Mayer, Sven. 'Exploring Users' Mental Models and Privacy Concerns During Interconnected Interactions.' In: *Proc. ACM Hum.-Comput. Interact.* 8.MHCI (2024). DOI: 10.1145/3676504.

[Core3] Windl, Maximiliane, Leusmann, Jan, Schmidt, Albrecht, Feger, Sebastian S., and Mayer, Sven. 'Privacy Communication Patterns for Domestic Robots.' In: *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. Philadelphia, PA: USENIX Association, 2024, pp. 121–138.

[Core4] Windl, Maximiliane, Akgul, Omer, Malkin, Nathan, and Cranor, Lorrie Faith. 'Privacy Solution or Menace? Investigating Perceptions of Radio Frequency Sensing.' In: *34th USENIX Security Symposium (USENIX Security 25)*. USENIX Association, 2025.

[Core5] Windl, Maximiliane, Winterhalter, Verena, Schmidt, Albrecht, and Mayer, Sven. 'Understanding and Mitigating Technology-Facilitated Privacy Violations in the Physical World.' In: *Proceedings of the 2023 CHI Conference on Human Factors in Com-*

puting Systems. CHI '23. Hamburg, Germany: Association for Computing Machinery, 2023. DOI: 10.1145/3544548.3580909.

[Core6] Windl, Maximiliane, Laboda, Petra Zsofia, and Mayer, Sven. 'Designing Effective Consent Mechanisms for Spontaneous Interactions in Augmented Reality.' In: *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. CHI '25. Japan: Association for Computing Machinery, 2025. DOI: 10.1145/3706598.3713519.

[Core7] Windl, Maximiliane and Feger, Sebastian S. 'Designing Interactive Privacy Labels for Advanced Smart Home Device Configuration Options.' In: *Proceedings of the 2024 ACM Designing Interactive Systems Conference*. DIS '24. Copenhagen, Denmark: Association for Computing Machinery, 2024, pp. 3372–3388. DOI: 10.1145/3643834.3661527.

[Core8] Windl, Maximiliane, Schmidt, Albrecht, and Feger, Sebastian S. 'Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes.' In: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. CHI '23. Hamburg, Germany: Association for Computing Machinery, 2023. DOI: 10.1145/3544548.3581167.

[Core9] Windl, Maximiliane, Hiesinger, Alexander, Welsch, Robin, Schmidt, Albrecht, and Feger, Sebastian S. 'SaferHome: Interactive Physical and Digital Smart Home Dashboards for Communicating Privacy Assessments to Owners and Bystanders.' In: *Proc. ACM Hum.-Comput. Interact.* 6.ISS (2022). DOI: 10.1145/3567739.

[Core10] Windl, Maximiliane, Thalhammer, Philipp, Müller, David, Schmidt, Albrecht, and Feger, Sebastian S. 'PrivacyHub: A Functional Tangible and Digital Ecosystem for Interoperable Smart Home Privacy Awareness and Control.' In: *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. CHI '25. Japan: Association for Computing Machinery, 2025. DOI: 10.1145/3706598.3713517.

Complementing Publications

[Pub1] Feger, Sebastian S., Windl, Maximiliane, Grootjen, Jesse, and Schmidt, Albrecht. 'ConnectivityControl: Providing Smart Home Users with Real Privacy Configuration Options.' In: *End-User Development*. Ed. by Lucio Davide Spano, Albrecht Schmidt, Carmen Santoro, and Simone Stumpf. Cham: Springer Nature Switzerland, 2023, pp. 180–188. DOI: 10.1007/978-3-031-34433-6_11.

[Pub2] Delgado Rodriguez, Sarah, Windl, Maximiliane, Alt, Florian, and Marky, Karola. 'The TaPSI Research Framework - A Systematization of Knowledge on Tangible Privacy and Security Interfaces.' In: *Proceedings of the 2025 CHI Conference on Human*

Factors in Computing Systems. CHI '25. Association for Computing Machinery, 2025. DOI: 10.1145/3706598.3713968.

[Pub3] Windl, Maximiliane, Henze, Niels, Schmidt, Albrecht, and Feger, Sebastian S. 'Automating Contextual Privacy Policies: Design and Evaluation of a Production Tool for Digital Consumer Privacy Awareness.' In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. CHI '22. New Orleans, LA, USA: Association for Computing Machinery, 2022. DOI: 10.1145/3491102.3517688.

[Pub4] Windl, Maximiliane, Amberg, Roman, and Kosch, Thomas. 'The Illusion of Privacy: Investigating User Misperceptions in Browser Tracking Protection.' In: *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. CHI '25. Japan: Association for Computing Machinery, 2025. DOI: 10.1145/3706598.3713912.

1 INTRODUCTION

Preserving users' privacy online has long been a key concern. Since the early days of the internet, researchers and lawmakers have recognized the need to protect privacy when sensitive user data is stored and processed [31]. As a result, research has focused on understanding potential privacy risks [51], the concerns these risks cause [120], and strategies for mitigating them [108]. Yet, recently, the boundaries between the digital and physical worlds have blurred as technology becomes embedded in nearly every aspect of our daily lives. In fact, due to advancements in technology, daily life has been transformed into a sensor-rich intelligent environment: when asking a smart speaker to dim the lights and adjust the thermostat, when a caregiver relies on a fall detection system to monitor an elderly family member, or when a fitness tracker continuously analyzes heart rates and sleep patterns to provide health insights. While such technology offers great convenience and enhances security, it also introduces significant privacy risks, as it relies on collecting and processing large amounts of user data. People already struggle to grasp the implications of their online behavior and its privacy risks [50]. With emerging technologies whose full functionality and capabilities may be even less transparent, these concerns could become even more pronounced. This raises the question: How can we empower users to protect their privacy in a world where intelligent, connected technology constantly surrounds us?

It is immediately clear that established online privacy solutions do not translate well to the physical world. Even in online settings, research has long criticized the ineffectiveness of methods like privacy policies and cookie banners, citing their complex legal language [110] and excessive length [91]. This issue gets aggravated in intelligent environments, where many devices lack screens to display privacy information, forcing users to rely on secondary devices to understand privacy implications.

Moreover, in a connected world, the person whose data is collected is often not the device owner but a *bystander*; someone exposed to the technology without being its primary user [146]. These bystanders may not even be aware that data is being collected, making it difficult for them to inform themselves about their rights and choices [74]. Another challenge is that users already avoid engaging with privacy information when signing up for accounts or making online purchases. In environments where interactions last only split seconds, such as checking a smartwatch's heart rate or viewing sensitive documents on smart glasses, the time required to engage with privacy information could easily exceed the interaction duration itself. According to research on privacy calculus, people weigh the effort of protecting their privacy against the perceived benefits [32]. This underscores the need for privacy mechanisms that are seamlessly embedded in interaction flows, minimizing effort while empowering users.

In summary, preserving privacy in a connected, intelligent environment is challenging because (1) people may struggle to fully understand emerging technologies and their associated risks, and (2) the unique characteristics of intelligent environments, such as the lack of screens, constant exposure, and varying user roles, demand novel privacy mechanisms. These two factors motivate my vision:

> **Vision:** To design seamless and engaging human-centered privacy mechanisms for interconnected, intelligent environments that integrate into daily routines and effectively empower users to claim autonomy, exercise agency, and manage access to their data, enabling meaningful, real-world privacy control.

In this thesis, I work toward this vision through two research questions. First, to develop effective countermeasures, we must understand which technologies and situations trigger privacy concerns. Thus, I pose the first research question: **RQ1:** *What privacy concerns do people have in intelligent, sensor-rich environments?* Once we have identified the situations requiring privacy mechanisms, we aim to design solutions that support users without adding additional burden. Hence, I ask in my second research question: **RQ2:** *How can privacy concerns in intelligent environments be effectively mitigated?*

To address the first research question, we conducted a series of investigations to understand people's privacy concerns with technology, ranging from established to emerging technologies. First, we examined whether familiarity and the distinction between established and emerging technologies influence privacy concerns [Core1]. Through an online survey, we presented participants with video scenarios featuring either a smartphone or a smart home device from a bystander perspective in different social settings. We found that people are significantly less concerned about smartphones than smart home devices, despite their similar capabilities. However, context and sensor type led to pronounced differences in privacy concerns. Investigating these concerns separately does not fully reflect reality, as smartphones and smart home devices are often interconnected; for example, when using a smartphone to stream music to a smart speaker. Therefore, we next explored users' mental models and privacy concerns in interconnected interactions through an online survey [Core2]. We found that while privacy concerns increase with the number of interconnected devices, users struggle to understand complex privacy processes and correctly attribute privacy-protection responsibilities. Motivated by the prospect of smart home devices gaining more interactive and mobile capabilities in the near future, we then examined privacy concerns related to domestic robots [Core3]. Through an online survey, we found that increased capabilities led to heightened and entirely new privacy concerns, such as a robot searching through private documents or interrupting sensitive situations. Finally, in [Core4], we investigated concerns surrounding emerging, non-transparent technologies, focusing on Radio Frequency (RF) sensing. While it is often marketed as a privacy-preserving alternative to cameras due to the lack of visual data, RF sensing actually introduces similar and even additional privacy risks. Through interviews and a large-scale online survey, we found that most were initially unaware of the full capabilities but expressed context-dependent concerns upon learning more. People, for example, preferred RF sensors in private locations but cameras when imagining their neighbor using the technology and in security-relevant situations. Overall, these studies provided a solid understanding of users' diverse privacy needs in intelligent environments and formed the basis for developing effective mitigation mechanisms.

To address the second research question, we conducted several studies aimed at developing frameworks, strategies, and concrete mechanisms to mitigate the privacy concerns and risks identified in the first research question. We first developed a framework to address privacy violations in the physical world, consisting of four tools that guide designers in creating effective mechanisms based on situational characteristics [Core5]. Similarly, we designed a framework for effective privacy consent in spontaneous, quick, and ubiquitous interactions, such as those involving smart glasses [Core6]. Building on this, we explored how domestic robots, given their interactivity and human-like capabilities, can communicate their privacy-relevant states to users [Core3]. We investigated different communication patterns and identified those perceived as most effective. As concrete mechanisms, we advanced the concept of privacy nutrition labels [39] by proposing interactive privacy labels for smart homes. These labels not only inform users about a device's privacy-relevant state but also dynamically adapt to reflect advanced configuration options [Core7]. Finally, through three projects, we explored the potential of tangible privacy interfaces for smart homes. First, we examined the general potential of tangible privacy controls, investigating manual and automated privacy mechanisms as well as physical privacy dashboards for privacy awareness [Core8]. We found that tangible mechanisms enhance awareness and control, independent of users' technological knowledge, ultimately fostering inclusive privacy. Building on these insights, we developed a digital-physical smart home ecosystem for security and privacy awareness [Core9], featuring a physical dashboard with colored LEDs to signal security and privacy vulnerabilities. Lastly, we created a fully functional smart home dashboard for privacy awareness and control [Core10], incorporating device proxies, floor plan, and data stream visualizations. The proxies allow users to adjust a device's connectivity state, while the visualizations enhance awareness of device presence and data transactions. Our findings indicate that the ecosystem effectively increased privacy awareness and control. Together, these mitigation measures offer a path forward toward a more privacy-preserving future in intelligent environments.

Overall, this thesis contributes the following to HCI and a privacy-preserving future: (1) a comprehensive understanding of the privacy risks and people's associated privacy concerns in intelligent environments, (2) innovative systems, and comprehensive concepts and frameworks to enhance privacy awareness and control, (3) a conceptual model of how personal, technological, and situational factors interplay to impact privacy concerns, (4) a research playbook to elicit human-centered privacy mitigation approaches in intelligent environments, and (5) a reflection on methods in privacy research and the future of privacy in intelligent environments. In all, this thesis lays the groundwork for a privacy-preserving future within intelligent environments.

1.1 Research Approach and Methods

We employed a wide range of methods across our studies, including online surveys, interviews with experts and laypeople, and in-the-wild studies. Whenever feasible, we used a mixed-methods approach, combining quantitative and qualitative data to contextualize effects and to explain the reasons behind patterns uncovered through log data or scales.

A central focus of my research was investigating people's privacy concerns (**RQ1**). These concerns are inherently subjective, shaped by individual experiences and backgrounds [137], and highly dependent on context [96]. As such, they are difficult to measure objectively, and researchers must often rely on self-reported data collected through questionnaires or interviews. This challenge was especially present when exploring emerging technologies and speculative futures, such as advanced domestic robots or RF-based sensing systems, that have not yet been widely adopted. In these cases, we primarily used online surveys. To support participants in engaging with unfamiliar scenarios, we incorporated visual materials such as images and videos, instead of relying solely on textual descriptions.

We mostly developed prototypes and conducted in-the-wild studies for **RQ2**, which focused on evaluating privacy mitigation mechanisms. Such studies are desirable when feasible, as they offer higher ecological validity by allowing participants to integrate the technology into their daily routines [67]. These deployments yielded valuable insights that would have been difficult to obtain through lab-based studies. Their durations ranged from one [Core10] to six weeks [Core8], as is common in HCI research.

Across all studies, we followed established ethical standards and obtained approval from our institutional review board. We also ensured that all participant data was processed and stored in compliance with the General Data Protection Regulation (GDPR) and local data protection regulations.

Interviews: We conducted interviews as one of the primary study methods in [Core4, Core5, Core6, Core7] and used introductory and exit interviews in [Core9, Core10, Pub3, Pub4]. When interviews served as a main method, we aimed to gather in-depth insights, as they allowed for follow-up questions, which is an advantage over open-ended survey responses. The introductory and exit interviews primarily contextualized quantitative findings obtained through questionnaires and log data. We recorded and transcribed all interviews and analyzed them using iterative coding and thematic analysis as described by Blandford et al. [16] or affinity diagramming [53].

Online Surveys: We conducted qualitative [Core5], quantitative [Core3, Pub3], and mixed-method online surveys [Core1, Core2, Core4, Core3, Core7]. With the exception of [Pub3], where we used a combination of convenience and snowball sampling, we recruited the participants on Prolific to ensure a more diverse sample than reachable using only the university's mailing list. Online surveys enabled us to explore futures that have not yet materialized, such as capable domestic robots [Core3] and RF sensing [Core4]. Additionally, we used online surveys to capture lived experiences with technology [Core5, Core1, Core2] and to evaluate digital prototypes with larger participant samples [Pub3, Core7].

In-the-wild Studies: We conducted in-the-wild studies in [Core9, Pub3, Core10] to evaluate self-developed prototypical systems. While these studies offer less control than lab studies, they provide higher ecological validity and allow us to capture lived experiences and more realistic behavior over an extended period, something lab studies usually cannot achieve.

Questionnaires: We used questionnaires in all publications. When available, we used validated questionnaires, such as the Internet Users' Information Privacy Concerns (IUIPC) [85] to assess people's general privacy perception or the Affinity for Technology Interaction (ATI) [44] to investigate people's affinity for technology. For specific questions, we also created our own items. While doing so, we followed best practices for scale design and mostly used 100-point Visual Analog Scales (VASs) without ticks to prevent responses from converging around the ticks [90]. Further, VAS lead to higher data quality, more precise responses [45], and since they collect continuous data, allow for more statistical tests [111].

Log Data: We collected log data, automatically captured without requiring explicit user input, in [Core7, Core9, Core10] to analyze how participants interacted with our self-developed prototypical systems. Rather than relying solely on questionnaires, log data allowed us to investigate user behavior more objectively and avoid recall bias, which can occur in self-reported methods such as questionnaires or interviews.

Design Activities: We conducted co-design activities in [Core5, Core3, Core6] to help participants visualize abstract ideas and articulate their visions more easily. In all these studies, we asked participants to sketch their privacy mitigation mechanisms while thinking aloud. We then systematically analyzed the sketches by coding and categorizing their elements, identifying recurring patterns, and cross-referencing them with participants' comments to understand their design choices.

Prototypes: We developed hardware prototypes in [Core9, Core10, Pub1] and software prototypes in [Pub3, Core7]. In [Core9, Pub3, Core10], the prototypes were a primary contribution of the publication. To support future research, we open-sourced the code and materials, allowing others to build upon and extend our systems. Overall, the prototypes provided deep insights into user interactions while generating generalizable knowledge that extends beyond the usefulness of the prototypes themselves.

1.2 Research Context

I conducted most of the research presented in this dissertation at the Chair for Human-Centered Ubiquitous Media and the Media Informatics Group at LMU Munich over approximately four and a half years. My primary advisor is Prof. Albrecht Schmidt, the head of the chair. Additionally, I conducted the research for [Core4] at Carnegie Mellon University during my three-month research stay under the supervision of Prof. Lorrie Cranor. Finally, I collaborated with team members and researchers from other institutions on studies and co-authored publications, which I outline in Table 1.1.

All publications were associated with the Munich Center for Machine Learning (MCML), a research center dedicated to advancing machine learning through fundamental research, interdisciplinary applications, and academic-industry collaboration. Within the research group *Humane AI*, we focus on human-computer interaction and human-centered AI topics.

1.3 Papers and Contributions

Table 1.1 outlines the methods and contributions according to Wobbrock and Kientz [141] for all core contributions.

Table 1.1: Methods and contributions for each of the contributing publications.

Paper	Methods	Contributions [141]
[Core1]	Mixed-method online survey ($N = 170$)	*Empirical:* Understanding of bystanders' privacy concerns related to smartphones and smart devices
[Core2]	Mixed-method online survey ($N = 120$)	*Empirical:* Understanding of users' mental models during interconnected interactions
[Core3]	Mixed-method online survey ($N = 90$), focus groups ($N = 22$), quantitative large-scale online survey ($N = 1720$)	*Theoretical & Empirical:* Set of privacy communication patterns for domestic robots and insights from online surveys and focus groups
[Core4]	Interviews ($N = 14$) and mixed-method large-scale online survey ($N = 510$)	*Empirical:* Understanding of people's privacy concerns regarding RF sensing
[Core5]	Qualitative online survey ($N = 89$) and expert interviews ($N = 10$)	*Theoretical:* Design framework for effective privacy consent in the physical world
[Core6]	Focus groups ($N = 17$), expert interviews and co-design activities ($N = 11$)	*Theoretical:* Design framework for effective privacy consent for spontaneous interactions in AR
[Core7]	Expert interviews ($N = 10$) and two online surveys ($N = 160$) and ($N = 120$)	*Artifact & Empirical:* Interactive privacy labels and findings from expert interviews and two online surveys
[Core8]	Focus group ($N = 8$), conference workshop ($N = 8$), and six-week in-the-wild study with households ($N = 6$)	*Empirical:* Insights into how tangible privacy mechanisms scale across devices and fit user needs in smart homes
[Core9]	In-the-wild study with households ($N = 8$)	*Artifact & Empirical:* SaferHome, an interactive digital-physical privacy framework and findings from an in-the-wild study using the framework
[Core10]	In-the-wild study with households ($N = 6$)	*Artifact & Empirical:* A cross-ecosystem smart home hub and findings from its one-week deployment

2

BACKGROUND AND RELATED WORK

> *"There is not a lot of death and gore in privacy law. If this is the standard to recognize a problem, then few privacy problems will be recognized."*
>
> **– Daniel J. Solove.**
> ***'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*.**
> **2007.**

The common claim of "having nothing to hide" reduces privacy to the concealing of wrongdoing [126]. Yet, privacy issues are multi-faceted and often emerge not from isolated disclosures but from complex systems of data processing that draw inferences, aggregate information, and repurpose data beyond its original context. Solove [126] further argues that a lack of privacy can lead to chilling effects, discouraging socially valuable behaviors like political discourse. Thus, privacy is not merely a subjective concern but a societal value. This is also signified by the fact that the United Nations declares privacy a fundamental human right in Article 12 [136]. Yet, they do not further define what the term privacy entails. This lack of clarity reflects the complexity of privacy as a multidimensional concept spanning legal, social, cultural, economic, and political domains [70]. Academic definitions vary, framing privacy as freedom from intrusion, control over personal data, or assurance against unauthorized disclosure [8, 55, 139]. In the context of information privacy, Westin [140] describes it as "the ability of an individual to control the terms under which their personal information is acquired and used." Solove [127] further argues that a universal definition is elusive due to the concept's diversity. Instead, he proposes understanding privacy through the issues that arise in context, offering a four-dimensional taxonomy of privacy violations: (1) information collection, (2) information processing, (3) information dissemination, and (4) intrusion. Nissenbaum's framework of contextual integrity redefines privacy in the digital age. Rather than opposing information sharing outright, it argues that privacy concerns stem from violations of context-specific norms [97]. This perspective challenges traditional public–private boundaries, emphasizing that information flows should align with social expectations within specific settings, such as workplaces or healthcare [96].

While a large body of prior work has focused on online privacy [51, 108, 120], the established concerns and mitigation strategies may not directly apply to intelligent environments. People may struggle to fully understand emerging technologies and the associated risks. Moreover, the unique characteristics of intelligent environments, such as the lack of screens, continuous exposure, and varying user roles, may call for novel privacy mechanisms, highlighting a research gap that this dissertation aims to address. To lay the foundation for our investigation, I first present prior work on privacy concerns (**RQ1**) in intelligent environments, followed by a summary of work on mitigation approaches (**RQ2**).

Definition — Human-Centered Privacy

Human-Centered Privacy emphasizes individual needs, capabilities, and contexts. It promotes designing mechanisms that respect user autonomy, enable meaningful control, and integrate privacy into daily life in usable, seamless, and inclusive ways.

2.1 Understanding Privacy in Intelligent Environments

This section presents prior research relevant to my first research question (**RQ1**). Specifically, I discuss the privacy risks that arise in sensor-rich environments, the concerns these risks trigger, and the contextual factors that influence those concerns. I discuss these issues in the context of smart homes, domestic robots, AR, and RF sensing.

2.1.1 Smart Homes

I first discuss privacy in smart homes, where devices are increasingly embedded into everyday routines and environments.

Privacy Risks

Smart home devices are placed in the most intimate spaces of daily life, such as bedrooms and bathrooms, where users expect a high level of privacy [14, 74, 152]. However, their placement and constant data collection introduce significant privacy risks. Prior research has shown that data collected by these devices can be exploited to reveal sensitive insights, including behavioral patterns, such as daily routines and periods of absence [9], and even the number of occupants in a household, their sleeping habits, and eating routines [93]. For instance, encrypted network traffic from sleep monitors has been shown to correlate with users' sleeping times [9]. Video surveillance systems are particularly vulnerable, with studies demonstrating attacks that inject forged video streams, execute denial-of-service attacks [99], or expose sensitive footage [102]. Geneiatakis et al. [48] used off-the-shelf devices to show how hackers could eavesdrop to deduce the smart hub's operating system, IP address, and unique ID or even impersonate legitimate users. These findings underscore the importance of protecting user privacy in smart homes, as data can reveal intimate aspects of daily life.

Privacy Concerns

While users often struggle to articulate the exact risks and technical vulnerabilities of smart home devices [49, 86], they nonetheless express privacy concerns [73]. These concerns include fears of data being transmitted without consent, persistent monitoring via always-listening smart speakers, targeted advertising, third-party data sharing, and a general lack of transparency [73, 74]. Surveys of adopters and non-adopters show that such concerns significantly influence smart speaker adoption. Non-adopters often cite distrust in manufacturers and data misuse [73], while adopters tend to justify use through trust in manufacturers [74, 142, 152]. Users' privacy concerns vary significantly depending on the type of sensors. Cameras and microphones are the most concerning [23, 25, 146], while non-visual sensors, such as temperature or motion detectors are seen as less intrusive [152]. Users are also particularly uneasy about specific types of data, especially those that reveal demographics (e.g., age, gender), communication content, daily routines, and lifestyle patterns [14]. However, they are generally more comfortable with data flows essential to the device's primary function [14]. This preference reflects a broader pattern: many users are willing to trade privacy for perceived benefits or convenience [95, 134], particularly in health-related contexts where older adults prioritize autonomy [134].

Contextual and social factors also shape privacy concerns. Device location within the home is a significant factor; devices in private areas, such as bedrooms or bathrooms, elicit stronger concerns than those in more public spaces, like kitchens [23, 146]. Similarly, the social relationship between individuals plays a critical role. Devices owned by trusted individuals are generally seen as less threatening [146], though greater familiarity can also increase perceived sensitivity due to easier interpretation of the data [142]: some users do not consider certain data sensitive until it is interpreted by someone familiar [72]. Privacy expectations extend beyond primary users as visitors and bystanders in smart home environments also hold privacy expectations [88, 146]. Bystanders, those who are not the primary users but are indirectly exposed to smart devices, are a particularly vulnerable group. They often lack the ability to consent, control, or even recognize their exposure [74, 77, 88, 146]. Their concerns include being recorded without notice, discrimination based on captured behavior, and mistrust in device manufacturers [87]. Power dynamics in multi-user settings, such as homes with guests or shared control scenarios, further complicate privacy. Studies show that visitors often share privacy preferences with homeowners but lack the means to express or act on them [47, 89].

2.1.2 Domestic Robots

As mobile and interactive extensions of the smart home, domestic robots introduce new privacy challenges beyond those posed by stationary devices like smart speakers.

Privacy Risks

Domestic robots can have advanced locomotion and interaction capabilities that allow them to access virtually all areas of a private home. As a result, their presence can impact not only informational privacy but also physical, psychological, and social dimensions of privacy [83]. Many domestic robots are equipped with mobile cameras, enabling them to capture images of users in intimate spaces such as bedrooms and bathrooms, collect detailed spatial data, or eavesdrop on conversations without users' awareness [19, 35, 119]. Furthermore, their ability to engage in verbal interaction, often combined with a humanoid or lifelike appearance, can prompt users to voluntarily disclose sensitive information [83, 133]. Due to their advanced mobility, interactive capabilities, and often humanoid appearance that fosters user trust, domestic robots introduce entirely new privacy challenges.

Privacy Concerns

While earlier work has highlighted the risks stemming from domestic robots' mobility and physical presence [20], users express stronger concerns about institutional privacy aspects, such as how their data is collected, stored, and used by manufacturers, often underestimating potential threats to their physical privacy [84]. Nevertheless, some users do express unease about the potential for robots to be exploited for harmful purposes like stalking or hacking [84]. In an interview study by Lee et al. [76], participants stated that they did not mind being recorded by the robot, provided they were aware of when it was happening. However, they voiced concerns about accidental recordings that might occur as the robot navigates or interacts with others. Participants generally agreed that they wanted to be informed about such accidental data collection. The study also revealed that users tended to underestimate what the robot could perceive, often assuming, based on its humanoid appearance, that its vision was limited like that of a human and incapable of seeing behind itself. This underscores the importance of clearly communicating the robot's actual sensing abilities to users [76].

2.1.3 Augmented Reality

AR glasses are always-on systems that combine sensors like cameras and microphones in a single device, heightening concerns about continuous and often opaque data collection.

Privacy Risks

Prior research highlights that continuous recordings enabled by AR glasses pose significant privacy and surveillance challenges [70, 114, 115]. These concerns are particularly critical because the devices have microphones and cameras that remain "always on" and are directed at people without requiring explicit user actions. Such recordings frequently extend beyond the primary user, capturing the surrounding environment and bystanders and raising concerns about unintentional data collection [30, 115]. By linking visual data with time and location, individuals' preferences and habits can be inferred [15]. Additionally, psychological and physiological information derived from biometric data may be used to predict behavioral patterns [70]. When combined with biometric cues, interpreting facial expressions, gestures, and voice can further reveal emotional states, thoughts, and feelings [15, 70]. These studies show how AR glasses pose completely new privacy challenges due to their unobtrusive, constant presence and collection of rich user data.

Privacy Concerns

Gallardo et al. [46] found that users generally accept tracking location, body temperature, heart rate, and movement related to AR glasses. This acceptance likely stems from the familiarity of such data collection through devices like smartphones and smartwatches. In contrast, participants expressed strong discomfort with more invasive data collection, such as private conversations, personal activities, brain wave recordings paired with visual data, and scenarios where employers monitor employees. The study also explored attitudes toward secondary uses of collected data. Participants were skeptical toward entities such as AR companies, employers, healthcare providers, insurance companies, and advertisers. However, prior research also suggests that AR technologies are perceived more positively when they provide assistive functions, particularly for individuals with visual impairments [6, 103]. People are also more open to AR usage by close contacts [34] and expect clear communication of intent from strangers who use AR glasses [28]. Additionally, people accepted AR usage more in public environments [34, 46]. According to Chung et al. [28], this may be because users associate public settings, like classrooms or meetings, with established social norms and thus expect lower risks of privacy violations.

2.1.4 Radio Frequency Sensing

RF sensing enables rich tracking and recognition capabilities. At the same time, it can operate through walls and remain undetectable to users, making it particularly invasive from a privacy perspective.

Privacy Risks

RF sensing enables a wide range of advanced capabilities that raise both opportunities and concerns. By analyzing reflected RF signals, RF sensors can infer rich information, including emotions [151], biometric characteristics [36], and physical activities [112]. Unlike visible-light cameras, RF sensors are not sensitive to lighting conditions and can operate through non-metallic objects and walls [3, 13, 27, 153], making them versatile for use in both public and private environments [150]. In security contexts, RF sensing enables comprehensive surveillance, such as tracking multiple individuals [2, 17, 27, 124], identifying room occupancy [3], recognizing detailed hand and finger movements [104, 129], and even detecting keystrokes [7]. Biometric inference further allows for identifying individuals based on body size and shape [41]. Recent advances have even demonstrated the ability to reconstruct sound through barriers [100]. These capabilities position RF sensing systems for security-relevant use cases, such as intruder detection, also distinguishing their activity from that of non-intruders, such as pets or authorized personnel like security guards [24]. RF sensing also offers significant potential for healthcare applications. It has been used to monitor daily activities (e.g., walking, and sitting) [138], track vital signs like heart rate and breathing [4, 118, 149], and analyze sleep behavior [57]. Some systems can simultaneously monitor multiple individuals, even distinguishing between people sharing a bed [148]. RF sensing has also been used to infer emotional states through heartbeat and pose recognition [106, 151], and to detect conditions such as Parkinson's disease [143]. These rich capabilities, combined with RF sensing's ability to track through solid barriers, underscore the technology's potential for novel privacy intrusions.

Privacy Concerns

Research explicitly investigating how people perceive RF sensing is scarce. Singh et al. [125] explored whether privacy concerns are primarily influenced by the human interpretability of sensor data. Focusing on mmWave sensors, an example of devices that generate data not directly interpretable by humans, they compared these to cameras and Wi-Fi routers in an online survey with 160 participants. The results suggest that when dealing with non-human-interpretable data, concerns are more strongly shaped by the potential inferences that can be made rather than by interpretability itself. However, their study does not address broader perceptions of RF sensing technology beyond the issue of data interpretability.

Summary: Understanding Privacy in Intelligent Environments

Established smart home devices and emerging technologies, such as domestic robots, AR, and RF, are transforming our daily lives into intelligent environments. These devices are equipped with various sensors and capabilities that continuously record and process potentially sensitive user information, exposing users to a range of privacy risks. These risks cause multiple privacy concerns that may hinder device adoption. However, such concerns are not uniform; they depend heavily on contextual factors, social roles, and individual experiences. This means that no single privacy mitigation strategy will suffice; solutions must be adaptable to individual preferences and contexts. Developing a deep understanding of users' privacy concerns toward emerging technology is therefore crucial for our vision of human-centered privacy mechanisms.

2.2 Mitigating Privacy Concerns

Recognizing the importance of data protection, the European Union introduced the GDPR in April 2016. Its main goal is to harmonize data protection laws across the European Union and ensure transparent, fair, and secure data processing by organizations [109]. No comparable overarching privacy law exists in the United States. Instead, they follow a sectoral and state-level approach to regulation. For example, the Health Insurance Portability and Accountability Act (HIPAA) [56] governs the handling of health-related data, and California enacted the California Consumer Privacy Act (CCPA) [18], a law that ensures consumer privacy rights. While not legally binding, United States regulations are influenced by the Federal Trade Commission's Fair Information Practice Principles (FIPs) [43], which outline core ideas such as notice, choice, access, security, and enforcement. A disadvantage of the sector-specific approach in the United States is that privacy in emerging domains often remains unregulated until new legislation is enacted. In contrast, the GDPR applies broadly, extending to new domains. However, the GDPR has also struggled to fulfill its promise of extensive privacy protection, as companies continue exploiting loopholes, due to weak enforcement and penalties too minor to act as effective deterrents

Yet, due to such regulations, companies are required to safeguard privacy in their products and integrate privacy-preserving measures. Spiekermann and Cranor [128] discussed two general approaches to mitigate privacy violations: privacy-by-policy and privacy-by-architecture. Privacy-by-architecture focuses on preventing privacy violations by minimizing data collection and anonymizing data, and privacy-by-policy relies on notice and choice principles, such as consent forms and settings. They argue that even though the former provides stronger protection, many businesses rely on the latter as it caters better to data-driven business models. In 2009, Cavoukian [22] coined the term privacy by design, which refers to the integration of privacy protections into products and systems from the outset [22]. She outlines seven foundational principles, including proactive prevention of privacy risks, privacy as the default setting, end-to-end security, and user-centric privacy mechanisms. As many businesses still refrain from incorporating privacy in their products from the beginning, prior research has investigated Privacy-Enhancing Technologies (PETs) to help users cater to their privacy needs. The need for human-centered privacy solutions is also highlighted by prior work emphasizing that users fail to protect their privacy because privacy protection is currently deemed too complicated or requires too much effort. As a result, many users resort to simple protective behaviors, such as unplugging devices [64]. Yet, this is also counterproductive as it renders the whole device useless, whereas most concerns only apply to specific sensors or capabilities. In the following, I will discuss system-level solutions, user-facing mechanisms, and tangible privacy mechanisms suggested by prior work.

2.2.1 System-Level Mechanisms

This section presents technical mitigation strategies that do not require active user involvement.

Smart Homes

In the context of IoT, researchers introduced traffic shaping to mitigate privacy risks in device traffic [10] and proposed auto-configuring smart devices with automatic updates to help users maintain secure settings [78]. To address the limitations of static privacy policies in dynamic smart home environments, they suggested frameworks that adjust privacy levels based on contextual parameters by obscuring data access [94]. Other approaches define privacy zones and generate adaptive policies [12], or implement context-based permission systems tailored to IoT environments [63]. Personalized privacy assistants aim to learn users' preferences over time, automatically adjust settings, and make privacy decisions on their behalf [21]. For perceptual technologies, such as systems using cameras and sensors to observe users and their environments, researchers developed Darkly, a protection layer that limits third-party access through access control, algorithmic transformation, and optional user audits [61].

Augmented Reality

In the context of AR, prior research has proposed frameworks for access control—that is, restricting access to sensors under certain circumstances. PrivacyManager, for example, is an access control framework for developers and system administrators, designed to manage access across entire domains, such as hospitals. A similar concept is the privacy passport, which automatically communicates with predefined policies to deactivate sensors, such as turning off a camera in a changing room [116]. Another approach disconnects the collection of camera frames on the device from internet communication and blocks the upload of sensitive data to the network [58, 62]. Shifting focus from users to bystanders, researchers have proposed systems that obscure bystanders identified through eye and voice tracking [29] or allow users to train the system to recognize familiar faces and blur unfamiliar ones [147].

RF Sensing

To mitigate the privacy risks associated with RF technology, researchers developed a system that distorts signals potentially leaking private information while allowing legitimate sensors to function as intended [105]. Other approaches include physically encrypting Wi-Fi channels to prevent unauthorized eavesdropping while retaining sensing capabilities [81], applying fine-grained perturbations to disable certain RF functionalities while preserving others [79], and erasing behavioral data from RF signals while maintaining the system's ability to authenticate users [80]. Finally, researchers have also proposed RF sensing shields that block sensing outside a defined perimeter [100, 144], and techniques that inject decoy activities to confuse sensing systems [121].

2.2.2 User Facing Mechanisms

This section presents user-facing mechanisms that require active user involvement.

Smart Homes

In the context of smart homes, prior research introduced interactive privacy and security labels inspired by nutrition labels to enhance transparency at the point of purchase [40]. Follow-up work refined these into layered labels that combine essential printed content with more detailed online information, contributing to the development of the Cyber Trust Mark regulatory framework [38, 42]. Other studies compared privacy awareness mechanisms, such as ambient lights, smart speakers, and data dashboards, and found that their effectiveness varies by context [131]. For example, participants described ambient lights as discreet and dashboards as offering detailed control and insights. Co-design sessions showed that users generally favor keeping data local, disconnecting devices from the internet, enabling authentication for multi-user scenarios, and managing access through distinct modes [145]. Further work addressed bystanders' concerns by outlining both cooperative mechanisms (e.g., negotiating preferences, requesting control) and bystander-centric solutions (e.g., enhancing awareness, limiting data collection) [146]. Research on smart home interfaces found social robots promising as controllers, despite usability challenges [82]. Finally, in the context of smart toys, prior work recommended clear recording indicators and features that allow children to review captured audio [92].

Domestic Robots

Regarding domestic robots, experts argued that privacy feedback should go beyond one-time notices and instead be provided continuously [66, 83]. Prior work further suggested strategies such as enabling shutdowns, restricting movement, anonymizing data, and designing physical features (e.g., expressive eyes or ears) to visually indicate active sensing [83].

Augmented Reality

AR systems increasingly offer user-facing privacy controls. One system blocks data capture in sensitive spaces (e.g., bathrooms) by filtering images based on user-defined preferences [130]. Other approaches provide an interface for reviewing and controlling outgoing visual data [58], or allow users to apply privacy profiles and enable bystanders to opt out of real-time AR monitoring via gestures that trigger facial blurring [122]. Patterned fabric has been used to conceal sensitive objects, replacing them with virtual content adapted to their shape [59]. Another framework enables real-time masking of sensitive information using visual markers like hand-drawn rectangles [107]. Finally, studies explored opt-in and opt-out mechanisms based on gestures or wearable tags [68, 123].

2.2.3 Tangible Privacy Mechanisms

Prior research highlights the potential of tangible mechanisms to make complex and abstract privacy concepts more accessible and engaging. In [Pub2], we presented a systematic literature review on Tangible Privacy and Security Interfaces (TaPSI). We identified key opportunities and challenges of TaPSI and introduced the TaPSI research framework to guide future work in this area. Ahmad et al. [5], who coined the term "tangible privacy," defined its core principles as (1) providing physical mechanisms to control data collection and (2) offering unambiguous feedback on what data is being collected. He advocates for tangible mechanisms due to their high comprehensibility, the trust they foster, and their inclusiveness, particularly for users with limited technological expertise. Because of these qualities, participants strongly preferred tangible controls in sensitive spaces such as bathrooms [23]. Tangible privacy mechanisms have primarily been explored at the sensor level. Examples include a wearable microphone jammer [26], a physical cover for smart speakers [132], and an automated webcam shutter [37]. Some systems extend beyond individual devices, offering privacy control at a broader system level. For instance, *PriKey* [113] allows users to deactivate sensors at the room level via a tangible key, and in [Pub1], we proposed a tangible framework enabling device functionality across different connectivity modes (online, local, offline), allowing users to make deliberate trade-offs between privacy and functionality. Despite these promising developments, existing research has concentrated mainly on sensor-level controls, with limited attention to system-level solutions. Additionally, most prototypes remain conceptual or low-fidelity and have not been evaluated in real-world settings.

Summary: Mitigating Privacy Concerns in Intelligent Environments

Although technical measures can effectively protect privacy, they often operate invisibly, which limits user awareness and control and might fail to account for diverse or evolving privacy preferences. In contrast, user-facing mechanisms can foster trust and transparency by supporting individual privacy decisions. However, effective privacy mechanisms for emerging technologies in intelligent environments, such as RF sensing and autonomous domestic robots, remain scarce. While tangible approaches have been proposed to enhance user control and awareness in smart homes, most remain at the prototype stage and lack evaluation in everyday contexts.

2.3 Summary

Prior work has shown that people's privacy concerns are highly context-dependent and shaped by situational factors. However, existing research has left important gaps regarding how these concerns manifest for emerging technologies and how to design effective, human-centered privacy mechanisms. In the next chapter, I will present how we addressed these gaps. We conducted a series of studies to develop a deep understanding of users' mental models and concerns regarding emerging technologies [Core1, Core2, Core3, Core4, Core5]. Building on these insights, we investigated privacy challenges from multiple angles. Recognizing that tangible mechanisms show promise in smart homes but remain largely unevaluated in real-world settings, we explored their everyday potential [Core8, Core9, Core10]. Beyond tangibility, we developed theoretical foundations for designing privacy mechanisms in physical environments [Core5] and in AR [Core6], created communication patterns to improve transparency in domestic robots [Core3], and introduced an interactive privacy label to support awareness, informed decision-making, and user education in smart homes [Core7].

3 HUMAN-CENTERED PRIVACY IN INTELLIGENT ENVIRONMENTS

This chapter outlines the core publications of this dissertation. It is structured by the two research questions, with the first focusing on understanding users' privacy concerns in intelligent environments (**RQ1**) and the second focusing on mitigating these concerns (**RQ2**). For each publication, I discuss the motiviation, methodological approach, and main findings. [Core3] is discussed in both sections as it tackles people's concerns about domestic robots before developing mitigation strategies. For a better overview, Table 1.1 summarizes the methods and contributions of each paper. Finally, as all contributions were collaborative efforts, Table 4.1 outlines the individual contributions of each author.

3.1 Understanding People's Privacy Concerns in Intelligent Environments

We introduce four publications [Core1, Core2, Core3, Core4] in this section that investigate people's privacy concerns from different angles. By exploring the factors that shape people's privacy concerns and understanding their mental models of privacy-relevant processes, these works address **RQ1** and the associated sub-research questions.

RQ1: *What privacy concerns do people have in intelligent, sensor-rich environments?*

3.1.1 Differing Perception of Smart Home vs. Personal Computing Devices

This section is based on the following publication [Core1].

Windl, Maximiliane and Mayer, Sven. 'The Skewed Privacy Concerns of Bystanders in Smart Environments.' In: *Proc. ACM Hum.-Comput. Interact.* 6.MHCI [September 2022]. DOI: 10.1145/3546719

A seemingly illogical discrepancy exists between the perception of smart home devices and personal computing devices, such as smartphones. Related to smart home devices, people express privacy concerns and engage in protective behaviors, such as turning off or unplugging devices. Yet, we do not observe similar behaviors related to personal computing devices, e.g., laptops or smartphones, even though both device types have similar capabilities. Motivated by this, we investigated how the device type affects bystanders' privacy concerns. We focused on bystanders as they have been recognized as especially protection-worthy due to their limited control options [87, 146]. Moreover, there is limited research on bystanders' privacy concerns toward smart personal computing devices. The following research question drove our investigation:

RQ1a: *How do bystanders perceive smart home devices compared to personal computing devices?*

Framed by five hypotheses derived from prior work, we conducted an online survey. We recruited participants via Prolific ($N = 135$) and our university's mailing list ($N = 35$) to obtain a more diverse sample. To help participants immerse themselves in the described situations, we created videos, which we also share for reuse in future research: https://maximiliane-windl.com/skewed-bystanders/. We investigated ten devices, five personal computing devices (e.g., smartphone, smartwatch, laptop) and five smart home devices (e.g., smart speaker, smart display, smart doorbell), using a within-subjects design, so each participant saw all videos. Building on prior work that shows social context influences privacy concerns, we also varied five social relationships (i.e., friend, family, colleague, homestay, hotel) as a between-subjects factor. After each video, participants answered questions about device ownership, familiarity, perceived privacy concern, and, in a final block, general privacy concerns across different sensors (e.g., camera, motion sensors) and locations (e.g., bedroom, garage). We found that bystanders perceive smart home devices as significantly more concerning than personal computing devices. Stronger social relationships reduced some of these concerns. We also identified factors influencing the severity of privacy concerns: cameras and microphones were seen as particularly concerning, concerns increased with the perceived intimacy of the location, and decreased with greater familiarity through device ownership. Based on our findings, we call for informing bystanders about the presence of smart devices across social contexts; Ideally, before entering intimate spaces, such as at the entrance.

3.1.2 Understanding Concerns in Interconnected Interactions

Our first investigation delivered valuable insights. Yet, considering smart home and personal computing devices as separate entities does not necessarily reflect reality: Users frequently use the devices together, for example, when streaming music from the smartphone to a smart speaker, when streaming a movie to a smart TV, or when connecting the smartphone to the car's infotainment system. Hence, in this work, we investigated people's privacy concerns and mental models during interconnected interactions involving smartphones and smart home devices through the following research question:

RQ1b: *What are users' mental models and privacy concerns related to interconnected interactions?*

This section is based on the following publication [Core2].

Windl, Maximiliane et al. 'Exploring Users' Mental Models and Privacy Concerns During Interconnected Interactions.' In: *Proc. ACM Hum.-Comput. Interact.* 8.MHCI [September 2024]. DOI: 10.1145/3676504

We again conducted an online survey on Prolific ($N = 120$), framed by five hypotheses derived from prior findings. Anticipating that laypersons might struggle to grasp the concept of interconnected device interactions, we first conducted eight expert interviews with HCI researchers to create six concrete interconnected scenarios. One example is streaming a movie from a smartphone to a smart TV. To support participant immersion, we created images to accompany the textual scenario descriptions. Learning from our first study that longer surveys can cause fatigue, we used a between-subjects design, meaning we confronted each participant with only one scenario. Participants answered questions in two rounds: In the first, they rated their familiarity with the scenario and their general privacy concern. In the second, we explored their mental models more deeply by asking what privacy risks they feared, where in the scenario these risks occurred, how they occurred, and who they believed was responsible for protecting their data. We found that most users do not fully understand the privacy-relevant processes in interconnected scenarios. However, their concerns increased when more data actors were involved. Based on these findings, we conclude that current methods of informing users about privacy implications are inadequate. Users need better support to make informed privacy decisions. As one possible solution, we suggest restricting data processing to the app layer and improving encryption of device traffic to shift data protection responsibility away from users. We encourage future research to reproduce and extend our results. For this purpose, we made our data and analysis script available on the Open Science Framework (OSF): https://osf.io/6dmgb/.

3.1.3 Understanding Concerns toward Emerging Technology

Moving beyond current capabilities and toward emerging technologies, we explored people's privacy concerns related to advanced smart home assistants, specifically, domestic robots. We investigated how increased locomotion and interaction capabilities influence privacy concerns through the following research question:

RQ1c: *How do privacy concerns change with intelligent systems' increasing levels of locomotion and interaction capabilities?*

This section is based on the following publication [Core3].

Windl, Maximiliane et al. 'Privacy Communication Patterns for Domestic Robots.' In: *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. Philadelphia, PA: USENIX Association, August 2024, pp. 121–138

We again used an online survey conducted via Prolific ($N = 90$). To minimize bias, we used consistent textual descriptions across conditions, varying only the locomotion and interaction capabilities. We deliberately avoided illustrations to prevent associations with specific devices or manufacturers. We defined three levels of interaction and four levels of locomotion, collaboratively developed with four experts in privacy and robotics. This resulted in 12 smart assistants, ranging from passive and stationary to fully interactive with world-level mobility. Using a within-subjects design, each participant evaluated all 12 assistants. For each assistant, participants rated their privacy concern and provided a brief explanation. Our results showed that higher interaction and locomotion capabilities were associated with increased privacy concerns. Participants often expressed fears that such assistants could follow them, open doors or drawers, and ultimately eliminate any sense of private space. We conclude that these heightened concerns highlight the need for domestic robots to clearly communicate their privacy-relevant states to users.

3.1.4 Understanding Concerns toward Emerging and Invisible Technology

Technology is becoming not only more advanced but also increasingly invisible in its operation. RF sensing is one such emerging technology: it interprets RF waves to understand and monitor the environment. RF sensors are gaining traction as powerful alternatives to traditional single-sensor systems like motion detectors, and especially to camera-based systems, offering similar functionality at lower cost. Because they do not rely on visual data, RF sensors are often presented as a privacy-preserving alternative. However, this claim can be misleading: RF sensors can infer the same information as cameras, and in some cases, even more. Their ability to operate through most physical obstacles makes them difficult to detect, leaving people unaware that they may be monitored. This project addressed the following research question:

RQ1d: *How do people perceive the capabilities and privacy risks of RF sensing, and how do they differ from cameras?*

This section is based on the following publication [Core4].

Windl, Maximiliane et al. 'Privacy Solution or Menace? Investigating Perceptions of Radio Frequency Sensing.' In: *34th USENIX Security Symposium (USENIX Security 25)*. USENIX Association, August 2025

We conducted two studies to investigate public perceptions of RF sensing technology. First, we conducted 14 semi-structured interviews with laypersons recruited via Prolific to explore general knowledge, awareness, and perceptions. As we expected that most participants would be unfamiliar with RF sensing, we provided a carefully crafted and neutral explanation that described the technology's functionality without mentioning privacy risks. After the explanation, we discussed different scenarios to understand how context affects perceptions, participants' reactions to RF sensors compared to cameras, and the impact of protective measures. The scenarios represented four realistic deployments of RF sensors across public/private and beneficial/non-beneficial contexts. We found that most participants were initially unaware of the technology and its privacy implications but expressed nuanced concerns once informed. The interviews also yielded initial insights into contextual factors shaping those concerns. Building on this, we conducted a large-scale online vignette survey ($N = 510$) with a representative US sample on Prolific. Using a between-subjects design, we varied contextual factors, use case, perspective, and location across 17 vignettes, such that each participant saw one scenario. Participants evaluated each scenario twice: once with a camera and once with an RF sensor, in random order. Afterwards, we assessed how different protective measures influenced their perceptions. While participants generally expressed privacy concerns, they tended to prefer RF sensors over cameras in private settings. However, people tended to prefer cameras outside their homes, in security use cases, or when deployed by neighbors. Finally, we found that protective measures can improve comfort, though their effectiveness depends on the specific use case and perspective. Based on our findings, we advocate for greater public education about RF sensing and call for updated legal frameworks to protect privacy as the technology becomes increasingly widespread.

3.1.5 Summary

We conducted four studies to investigate people's privacy concerns in intelligent environments. Our investigations covered current smart home and emerging, invisibly operating technologies. Across our studies, we identified a consistent pattern: people's privacy concerns are shaped by how well they understand the technology and various contextual parameters. First, people express stronger concerns toward smart home devices than personal computing devices, even when their sensing capabilities are similar. The closer the relationship to the device owner is, the less intimate the device location is, and the higher the familiarity with the device, the lower the privacy concerns. Second, we found that concerns intensify when devices interact across ecosystems, yet users often lack a clear understanding of the data flows involved, highlighting a gap in mental models. Third, increased autonomy in emerging technologies, such as domestic robots with full movement and interaction capabilities, leads to higher perceived privacy invasiveness due to fears of losing control over personal space. Finally, invisibly operating and poorly understood technologies, like RF sensing, evoke concern only after people learn about their capabilities, demonstrating the crucial role of awareness and education. Altogether, our findings suggest that understanding, familiarity, perceived control, and contextual sensitivity are key factors for mitigating privacy concerns in intelligent environments. We identify a need for privacy-centered design, improved user communication, and regulatory frameworks tailored to emerging and interconnected sensing technologies. These findings lay the groundwork for the second part of the dissertation, in which we develop effective mitigation mechanisms.

3.2 Mitigating People's Privacy Concerns in Intelligent Environments

In this section, we discuss seven publications [Core3, Core5, Core6, Core7, Core8, Core9, Core10] that address the previously mentioned privacy concerns. These works examine approaches to enhancing awareness and control, with a particular focus on tangible privacy solutions. Together, they contribute to answering **RQ2** and its related sub-questions.

RQ2: *How can privacy concerns in intelligent environments be effectively mitigated?*

3.2.1 A Framework for Privacy Mitigation Approaches in the Physical World

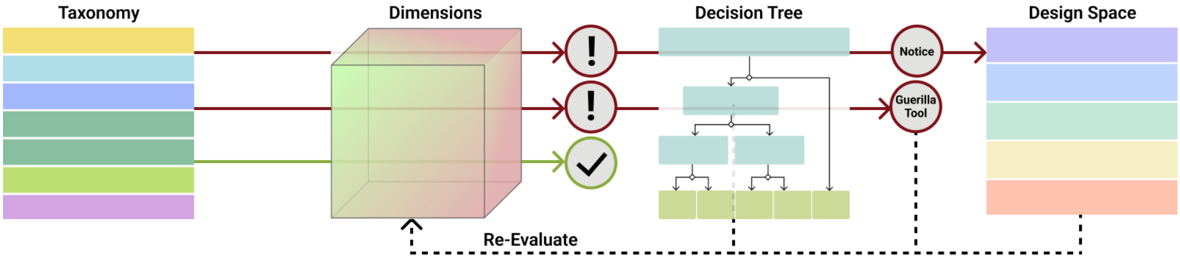

Figure 3.1: A conceptual framework for effectively mitigating privacy violations in the physical world. Figure adapted from [Core5].

This section is based on the following publication [Core5].

Windl, Maximiliane et al. 'Understanding and Mitigating Technology-Facilitated Privacy Violations in the Physical World.' In: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. CHI '23. Hamburg, Germany: Association for Computing Machinery, 2023. DOI: 10.1145/3544548.3580909

While mitigating privacy risks in the online world has been thoroughly explored, efforts to mitigate privacy violations in the physical world are scattered and focused on specific domains, such as smart homes [38, 131, 145]. Consequently, we lack an encompassing understanding of how to protect people's privacy in intelligent environments. In this project, we tackled the following research question:

RQ2a: *How can we structure a conceptual framework to understand and mitigate privacy violations in intelligent environments?*

We created a process to elicit effective privacy mechanisms using an online survey and expert interviews. We first conducted an online survey on Prolific ($N = 100$) to understand where people experience privacy violations through technology in the physical world. Based on these experiences, we constructed a scenario taxonomy. We then conducted interviews with ten privacy experts from industry and academia. We validated the taxonomy by asking the experts to create four scenarios using the taxonomy they deemed especially privacy-violating. In a second step, we asked them to sketch effective mitigation strategies while thinking aloud. Out of the sketches and discussions, we derived three additional tools: (2) the dimensions of privacy violations that help judge if a situation should be considered a violation, (3) a decision tree to decide on the most suitable mechanism based on context factors, and (4) a design space to create privacy notices, see Figure 3.1. Together, our tools form a conceptual framework, helping designers and researchers effectively mitigate privacy violations in the physical world.

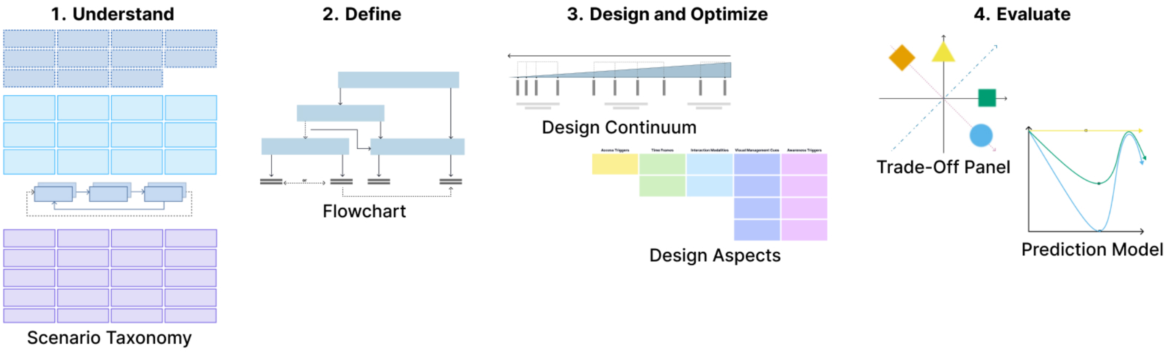

Figure 3.2: Conceptual framework for effective privacy consent for spontaneous technology interactions aligned with the 4 steps of the user-centered design process. Figure adapted from [Core6].

3.2.2 A Framework for Effective Consent in Augmented Reality

This section is based on the following publication [Core6].

Windl, Maximiliane et al. 'Designing Effective Consent Mechanisms for Spontaneous Interactions in Augmented Reality.' In: *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. CHI '25. Japan: Association for Computing Machinery, 2025. DOI: `10.1145/3706598.3713519`

Today, interacting with technology involves deliberate actions: logging into a website to shop or picking up a phone to make a call. In contrast, with the widespread adoption of technologies like AR glasses, interactions will become near-instantaneous and largely subconscious. These spontaneous interactions will occur frequently and without conscious decision-making, while the devices continuously collect and process private information. Whether reading a confidential document or having a sensitive conversation, users will be exposed to constant data collection. Current privacy communication, typically via text-based methods like privacy policies or cookie banners, is already ineffective. In a future where interactions last only split seconds, engaging with such notices would take longer than the interaction itself, making the traditional "notice and choice" model obsolete. This project explored how effective privacy consent can be achieved in such spontaneous technology interactions. We addressed the following research question:

RQ2b: *How can privacy consent mechanisms be designed to be effective and suitable for spontaneous, seamless interactions in everyday AR environments?*

We first conducted two focus groups ($N = 17$) to explore when and how spontaneous technology interactions in AR environments involve private information. Participants engaged in speculative discussions, imagining a future where AR glasses are widely adopted, and designed AR interaction scenarios across various life contexts. From these discussions, we developed a scenario taxonomy of privacy-relevant AR interactions. Next, we conducted semi-structured interviews with 11 privacy and AR experts from industry and academia to identify ways to effectively mitigate the identified privacy risks. To validate the taxonomy, we asked experts to use it to create two privacy-relevant scenarios and to sketch suitable consent mechanisms while thinking aloud. From these interviews, we derived three additional conceptual tools: a flowchart to decide on the best mechanism based on the contextual constraints of a situation; a design continuum and design aspects chart to design the concrete mechanism, and a trade-off and prediction chart to evaluate the mechanisms, i.e., their impact on user effort, control, and comfort. Together with the scenario taxonomy, these tools form a conceptual framework (see Figure 3.2) to support developers and designers in creating effective consent mechanisms for spontaneous AR interactions.

3.2.3 Privacy Communication Patterns for Domestic Robots

This section is based on the following publication [Core3].

Windl, Maximiliane et al. 'Privacy Communication Patterns for Domestic Robots.' In: *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. Philadelphia, PA: USENIX Association, August 2024, pp. 121–138

Apart from these privacy frameworks, we also developed actionable design patterns. In this paper, for example, which I already discussed previously related to **RQ1**, we derived a need for novel communication patterns for domestic robots to communicate their privacy-relevant state to users. Motivated by domestic robots' increased capabilities that raise novel concerns but also offer completely new ways to communicate privacy states, we developed and evaluated different privacy communication patterns. Concretely, we answered the following research question:

RQ2c: *Which communication patterns should domestic robots use to convey their privacy-relevant functionalities?*

We conducted three focus groups ($n = 22$) to derive communication patterns. To scope this initial investigation, we focused on patterns related to cameras, microphones, and network connectivity; capabilities that were most frequently mentioned in the paper's first study. We began by thoroughly introducing domestic robots and their current and expected future capabilities. We then divided participants into smaller groups and asked them to design communication patterns, emphasizing creatively using the robot's novel interactive features and locomotion capabilities. Through this process, we collected 86 distinct communication patterns. We classified these patterns into two main types: awareness patterns, which communicate the status of a capability to users without altering its function, and intervention patterns, which physically prevent a capability (e.g., a microphone or camera) from operating. To evaluate the effectiveness of these patterns, we conducted a large-scale online survey with 1720 participants. We assessed how each pattern performed across several key dimensions: trust, privacy, understandability, notification quality, and general user preference. The findings revealed that most patterns performed similarly across these dimensions. This suggests that there is no single best solution; rather, the suitability of a communication pattern depends on the specific context and requirements of the situation. To support future researchers and developers in exploring and selecting appropriate patterns, we developed an interactive web application: https://robot-patterns-finder.web.app/. Our final set of communication patterns will guide future research and practitioners in ensuring a privacy-preserving future among domestic robots.

3.2.4 Interactive Privacy Labels

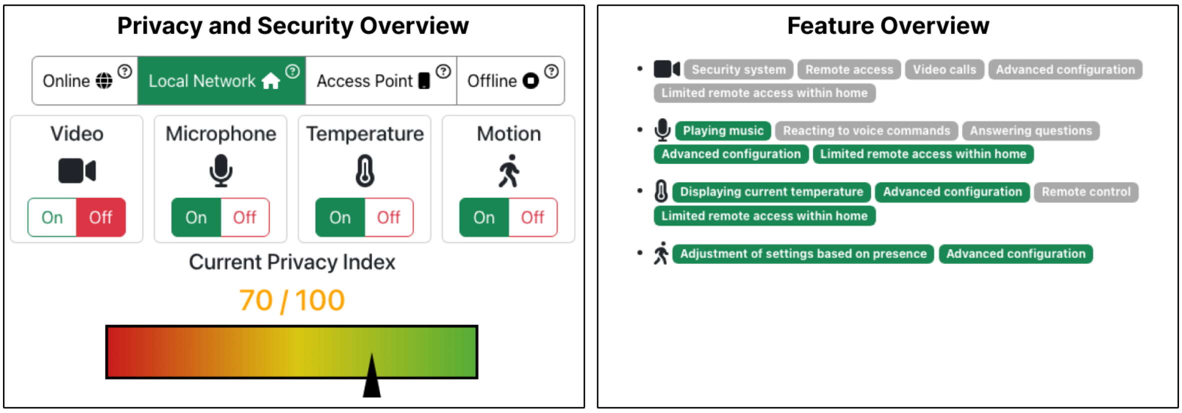

Figure 3.3: The interactive smart device privacy label. The left shows the control panel that enables users to change the connectivity mode and the state of individual sensors. It also shows the privacy index that reflects the privacy exposure based on the current configuration. The right panel dynamically shows the available features based on the current configuration. Image adapted from [Core7].

This section is based on the following publication [Core7].

Windl, Maximiliane and Feger, Sebastian S. 'Designing Interactive Privacy Labels for Advanced Smart Home Device Configuration Options.' In: *Proceedings of the 2024 ACM Designing Interactive Systems Conference*. DIS '24. Copenhagen, Denmark: Association for Computing Machinery, 2024, pp. 3372–3388. DOI: `10.1145/3643834.3661527`

Privacy labels, modeled after nutrition labels, have been proposed to inform consumers about the privacy implications of smart products at the time of purchase [38]. These labels have even influenced regulatory frameworks [42, 33]. However, current implementations remain static and fail to reflect device configuration options or how these settings affect privacy risks and device functionality. This contrasts with recent research on communicating and controlling individual sensor states [25, 37, 132]. To address this gap, we explored the following research question:

RQ2d: *How can interactive privacy labels effectively reflect advanced smart device configuration options?*

We began by designing smart home privacy labels that reflect device configuration options, building on findings from prior work [38, 40]. We created two versions: a static, printable label and an interactive digital label accessible via QR code. The digital label lets users explore and adjust device and sensor settings directly, see Figure 3.3. To evaluate and refine these labels, we first conducted an interview study with ten privacy experts. Next, we ran an online survey on Prolific with 160 participants to assess the labels' interpretability and usability. Finally, we conducted a second online survey with 120 participants to examine whether the interactive label effectively educates users about sensor configuration options. Our findings show that static labels are inadequate for conveying configuration options. In contrast, most participants were able to correctly configure the interactive label and often selected more privacy-preserving settings than required by the tasks. Participants also reported that the interactive label provided important information and helped them access sensor details more quickly and accurately.

3.2.5 Tangible Privacy Mechanisms

In [Core8, Core9, Core10], we investigated the potential of tangible privacy mechanisms for smart homes. We started with a general exploration of sensor-level and ecosystem-level tangible mechanisms [Core8], developed and tested a privacy-awareness-focused tangible smart home dashboard [Core9], and finally combined all previous findings to develop and evaluate a fully functional smart home control and awareness dashboard [Core9]. These investigations offer novel insights into the potential of tangible mechanisms for smart home privacy awareness and control.

Exploring Tangibility for Smart Homes

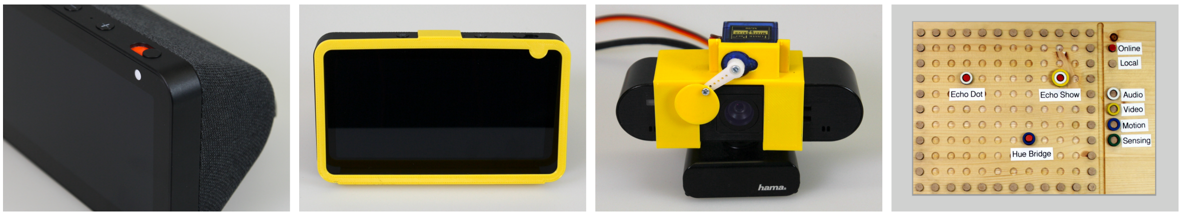

Figure 3.4: Overview of tangible privacy artifacts. From left to right, they show (1) an integrated tangible camera shutter of an Echo Show, (2) a 3D printed Snap-on-Privacy (SNOP) artifact to cover the Echo Show's camera, (3) an automated 3D printed SNOP artifact on a webcam, and (4) a tangible, static smart home dashboard. Image adapted from [Core8].

This section is based on the following publication [Core8].

Windl, Maximiliane et al. 'Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes.' In: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. CHI '23. Hamburg, Germany: Association for Computing Machinery, 2023. DOI: 10.1145/3544548.3581167

Prior work highlighted the strong potential of tangible mechanisms to foster user trust. These mechanisms provide immediate, intuitive feedback that clearly indicates they are functioning as intended. This is particularly valuable for users with lower technological affinity [5]. However, how these mechanisms can be effectively applied in smart homes remains unclear.

RQ2e: *How can user-centered tangible privacy mechanisms provide effective and trustworthy control over different sensors in smart home environments?*

We explored the potential of tangible privacy-preserving mechanisms for future smart homes through three studies. First, we developed manual and automated speculative artifacts for sensor-level control (see Figure 3.1) and evaluated them in a focus group ($N = 8$). Participants valued tangible control over individual sensors but wanted a central control unit. They also highlighted tensions between their need for privacy and the convenience smart devices offer. To broaden these insights, we conducted a second study: a workshop on tangible privacy at an HCI conference ($N = 8$). Participants discussed analog strategies to prevent digital threats and focused on designing mechanisms that raise awareness rather than provide direct control. In the third study, informed by the previous findings, we developed and deployed a tangible, static privacy dashboard (see Figure 3.1) in a six-week in-the-wild study across six households. This study examined how household members and visitors interacted with the dashboard and revealed real-world dynamics of privacy negotiation. We found that the dashboards effectively raised awareness among residents and guests and frequently initiated conversations about smart home privacy. However, while visitors often reported discomfort, they rarely requested that devices be turned off, either because they did not perceive their data as sensitive or wished to avoid social conflict. Overall, our findings show that while some users expect future tangible tools to offer automated interventions, many view them as prompts for personal interaction, negotiation, and conflict resolution. This reinforces the need to design future systems that support both awareness and control, rather than focusing exclusively on one dimension.

A Tangible Dashboard for Smart Homes Awareness

> This section is based on the following publication [Core9].
>
> Windl, Maximiliane et al. 'SaferHome: Interactive Physical and Digital Smart Home Dashboards for Communicating Privacy Assessments to Owners and Bystanders.' In: *Proc. ACM Hum.-Comput. Interact.* 6.ISS [November 2022]. DOI: `10.1145/3567739`

This project had two main goals: (1) to compare the value of a tangible dashboard versus a purely digital one, and (2) to examine the impact of floor plan visualizations in helping device users and bystanders understand the number and placement of smart devices in the home. Additionally, the system incorporated color-coded warnings to notify users of privacy and security issues associated with their devices. Specifically, we investigated the following research question:

RQ2f: *How does a tangible smart home dashboard that maps floor plans impact privacy awareness?*

We compared the benefits of floor plan visualizations to a traditional list view. As we also wanted to assess the role of tangibility, we created two versions of a floor plan–based dashboard: one digital and one physical. Both versions allowed users to recreate their household floor plans and place representations of their smart devices within their homes, either via an online web application or a physical dashboard built from 256 connectors, wall tiles, and functional device proxies. Each device proxy indicated its type through an exchangeable icon plate and included a yellow LED that lit up when new privacy or security vulnerability reports became available. In the digital version, devices changed their background color to yellow to signal the same. We conducted a two-week in-the-wild study with eight households and 16 participants to evaluate these dashboards. In the first week, all households used the digital list view as a baseline. In the second week, half of the households used the digital floor plan, and the other half used the physical version. For all dashboards, we provided real, curated privacy and security vulnerability reports drawn from public databases and reviewed by a computer security consultant. While all three visualizations were rated similarly in terms of usability, functionality, and perceived helpfulness, participants, especially those using the physical dashboard, reported that the constant visual presence of their smart home setup prompted frequent reflection on the devices they had installed and their placement. However, participants also expressed a clear desire for more control. They wanted the ability to limit remote data exchange and to adjust settings according to their current privacy preferences. These findings directly informed the prototype development presented in [Core10].

A Tangible Dashboard for Smart Home Awareness and Control

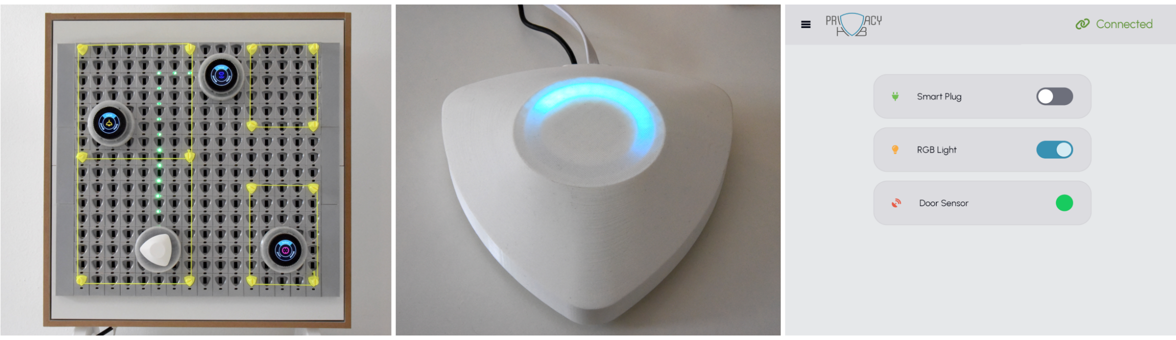

Figure 3.5: The PrivacyHub ecosystem. From left to right, the figure shows (1) the tangible control and awareness dashboard, (2) the hub serving as the central control unit of the system, and (3) the web application for remote control and awareness. Figure taken from [Core10].

In this project, we combined insights from the previous studies to develop a fully functional, tangible smart home ecosystem. Specifically: (1) we designed a tangible interface to foster trust and understanding among users with lower technological affinity and to enhance recall and awareness through physical visibility; (2) we integrated a dashboard with a floor plan visualization to help users comprehend their smart home setup and increase situational awareness; and (3) we incorporated both awareness and control features to address the diverse needs of users. This project addressed the following and final research question:

RQ2g: *What impact does a fully functional smart home privacy awareness and control dashboard have on smart home users?*

This section is based on the following publication [Core10].

Windl, Maximiliane et al. 'PrivacyHub: A Functional Tangible and Digital Ecosystem for Interoperable Smart Home Privacy Awareness and Control.' In: *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. CHI '25. Japan: Association for Computing Machinery, 2025. DOI: 10.1145/3706598.3713517

Our smart home ecosystem consists of three core components, see Figure 3.5: a physical dashboard that maps household floor plans and displays device locations using tangible proxies; a smart home hub that serves as the central control unit; and a digital web application that enables remote access. The system allows users to manage privacy by changing the connectivity settings of individual devices, either physically, by rotating the proxy's ring on the dashboard, or digitally, via the responsive web app. Users can choose between three connectivity modes: local, online, and online-shared, the latter enabling integration with third-party platforms like Amazon Alexa. These connectivity states were adapted from our work in [Pub1]. The dashboard visualizes data flows whenever a device's connectivity is adjusted to support privacy awareness. The web app also features a history page that allows users to review previous settings. To foster transparency and future development, we open-sourced all 3D models and code on GitHub: https://github.com/mimuc/PrivacyHub. Using questionnaires, system logs, and interviews, we evaluated the system in a one-week in-the-wild study with six households and 13 participants. All participants appreciated the system for its ability to increase control and awareness. They reported heightened attention to privacy risks, made more privacy-conscious decisions, and developed a better understanding of how their smart devices handle data. While some participants favored the convenience of digital interactions, most preferred the tangible dashboard as they considered it more direct and trustworthy. Many also noted that its visibility prompted ongoing awareness, not only for themselves, but also for household visitors and bystanders. Finally, participants highlighted that the system's directness and constant availability helped integrate privacy management into daily routines, shifting it from a burdensome chore to a natural part of everyday life.

3.2.6 Summary

This section explored effective mitigation approaches from multiple perspectives, including theoretical frameworks, system contributions, and empirical findings. Our theoretical contributions can guide researchers and developers by outlining the steps needed to design, select, and evaluate privacy mechanisms. Our set of communication patterns lays the groundwork for future efforts to effectively communicate privacy-relevant states, supporting a privacy-preserving future with autonomous assistants. We also contribute a concrete solution in the form of an interactive privacy label. Our studies show that it enhances privacy awareness, supports more informed decision-making, and educates users about device configuration and data practices. Finally, we offer in-depth insights into tangible privacy mechanisms. Across three studies, we demonstrate how tangibility makes privacy more accessible and actionable. We show that tangible tools increase trust and understanding, not only for primary users, but also for bystanders, highlighting the broader potential of physical interfaces in privacy-aware intelligent environments.

4 DISCUSSION

This dissertation aimed to establish human-centered mechanisms that empower people to reclaim autonomy over their privacy in intelligent environments. My first research question focused on understanding people's privacy concerns. Across four studies, we investigated how people perceive different technologies, from current smart home devices and smartphones to emerging and autonomous systems. Building on these insights, we conducted seven more investigations to design and evaluate effective privacy mechanisms. This included the development of conceptual frameworks and functional prototypes. In the following, I will synthesize these findings by presenting a conceptual model of privacy concerns in intelligent environments. Based on this model, I will derive a research playbook for developing privacy mechanisms. Finally, drawing on the diverse methodological approaches used throughout this work, I will reflect on their suitability for privacy research and the future of privacy in intelligent environments.

4.1 A Model for Privacy Concerns in Intelligent Environments

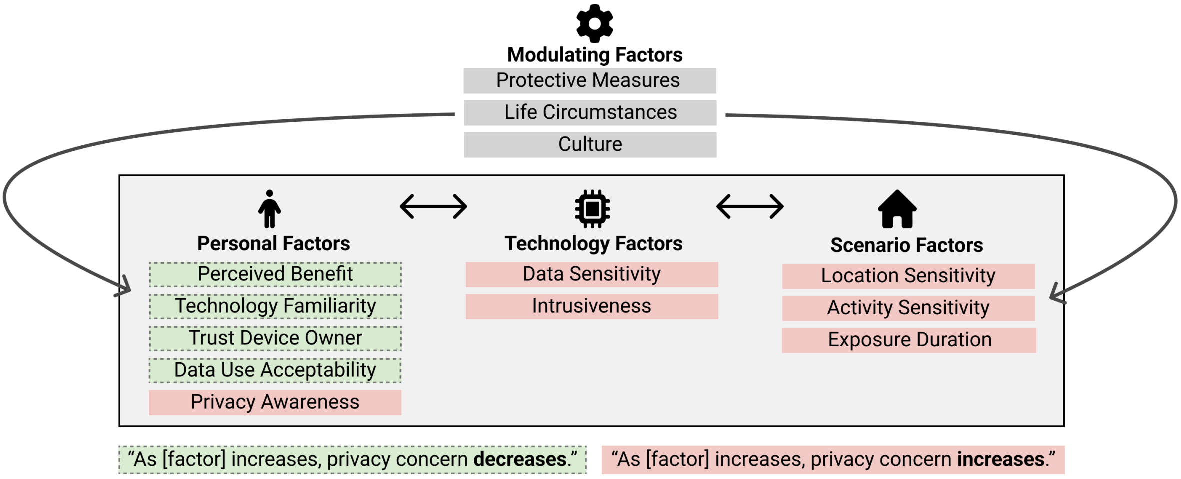

Figure 4.1: A conceptual model outlining how various contextual and personal factors impact privacy concerns in intelligent environments. Green factors indicate that the privacy concern decreases as the factor increases, and red factors indicate that the concern increases as the factor increases.

In our first research question (**RQ1**), we asked: What privacy concerns do people have in intelligent, sensor-rich environments? Overall, we found that concerns are shaped by a combination of personal, situational, and technological factors, for example, a person's familiarity with the technology, the type of data being collected, and the location of the sensing system. Surprisingly, we did not observe the stark differences between technologies that we initially expected. Instead, privacy concerns followed consistent patterns, with certain factors influencing them in predictable directions. This observation aligns with findings from previous studies on privacy perceptions toward sensing technologies. Building on our findings and prior work, I developed a conceptual model of privacy concerns in intelligent environments (see Figure 4.1). The model outlines various personal, technological, and situational factors and uses color-coding to indicate their directional influence: red factors increase privacy concern as their presence or intensity rises, while green factors reduce concern. Additionally, the model includes modulating factors, which can alter the direction or strength of all other influences. Two-way arrows between factors illustrate their interdependence. For example, the perceived benefit of a system is closely tied to both the type of technology and its deployment context. In the following, I will describe the model in detail.

Personal Factors

People's beliefs and experiences impact privacy concerns. One of the most influential factors is the technology's **perceived benefit**. We found in [Core4] that as people saw more value in a technology, their acceptance increased and privacy concerns decreased. This was particularly evident in health-related scenarios, where many participants were willing to sacrifice privacy to protect themselves or close others. In contrast, willingness to engage dropped significantly when the system offered analytical insights without a clear personal benefit. This pattern aligns with prior research showing that people are generally more willing to share data for beneficial purposes like health, but resist doing so for less beneficial uses such as advertising. This holds true not only for smart home devices [95], but also for highly sensitive information, including intimate health data [60] and brain data [65]. A similar effect was found regarding **technological familiarity**: the more familiar people were with a technology, whether through ownership or usage, the less concerned they were about its privacy implications. This was evident in [Core1], where participants expressed greater concern about smart home technology than personal computing devices, despite both offering similar capabilities. Apthorpe et al. [11] report similar findings for smart devices. **Trust in the device owner** also played a key role. In [Core1, Core4], we showed that the stronger the trust relationship with the device owner, the lower the privacy concerns — a finding echoed in related work [146]. Although not a central focus in our studies, prior research consistently highlights the impact of the **acceptability of data use**, such as who has access to the data and how long it is stored, on people's privacy concerns [95, 60, 65]. Finally, **awareness** of privacy-relevant processes was another contributing factor. In [Core2], participants' concerns increased once they reflected on the scenario and became aware of how many different actors were involved, a finding also reported by Prange et al. [101].

Technology Factors

Data sensitivity emerged as a crucial factor. In [Core1], participants expressed the greatest concern about technologies like cameras and microphones, while showing little worry about less invasive sensors such as those detecting temperature or motion. Similarly, in [Core4], concerns centered on the extensive insights that could be derived from both camera and RF data. This pattern is consistently reflected in related work [95, 60], which shows that the more sensitive the data being collected, the higher the level of privacy concern. **Technological intrusiveness** also played a significant role. In [Core3], participants voiced stronger concerns with more capable domestic robots, particularly fearing that the robots might invade private spaces or access personal belongings and in [Core4], participants were especially uneasy about RF sensing's ability to penetrate most materials, including walls, making it difficult to avoid being tracked.

Scenario Factors

The **sensitivity of the location** was a key factor across our studies [Core1, Core4] and in prior research [95, 146]. The more intimate or private the setting, the greater the participants' concerns. Similarly, the **sensitivity of the activity** influenced participants' privacy concerns. In [Core4], people worried that RF sensors might detect sensitive activities, while in [Core3], they were concerned about the robot appearing unexpectedly during private moments. Prior work similarly identifies activity context as a critical factor [14]. Finally, participants in [Core4] highlighted the importance of **exposure duration**. While participants were generally unconcerned about occasionally visiting acquaintances who used tracking technology, many opposed having such devices in their own homes or those of close friends. They felt prolonged or repeated exposure increased the likelihood of revealing patterns, making it easier to interpret and potentially misuse the data.

Modulating Factors

Finally, modulating factors can influence both the strength and direction of all other privacy-related concerns. One such factor is the availability of **protective measures**, including legal regulations that limit data misuse, technical solutions like obfuscation to remove identifiable information, or physical safeguards [Core4]. Another important factor is a person's **life circumstances**, particularly whether they belong to a vulnerable group. In [Core4], for instance, one participant expressed concern that RF sensing could reveal a pregnancy they were not yet ready to disclose. Similarly, [77] demonstrated how smart technologies can be misused in abusive relationships. Lastly, a person's **culture** also plays a significant role. Prior research has consistently shown that cultural norms shape privacy expectations. For example, people in the United States are often found to be more privacy-conscious than those in India or China [137], but less so than Europeans [135].

My conceptual model shows how different personal, technological, and situational factors influence privacy concerns. I observed a striking consistency in the factors shaping privacy concerns across diverse application scenarios and data types. Regardless of whether the technology was familiar or novel, the core concerns remained stable: People are more comfortable when technology offers clear personal or societal benefits, when it is familiar, when they trust those handling the data, and when they are made aware of what is happening. They are more concerned when technologies operate in private spaces, collect sensitive data, or target vulnerable individuals. Even with disruptive, novel systems like RF sensing, the overarching patterns held. These findings raise a critical question: Have we reached a saturation point in understanding privacy concerns?

I argue that we may indeed be approaching such a saturation point. Much of the recent research reveals familiar patterns with only minor variations rather than truly new concerns. As a result, I suggest that rather than repeatedly documenting the same issues, researchers should be more selective and ensure they have a strong, evidence-based rationale before conducting new studies. In other words, we should ask: Is there a compelling reason to believe that this technology genuinely reshapes privacy perceptions in ways that prior research has not already captured? Instead of duplicating the same findings, the more pressing challenge may now be to develop, implement, and test solutions that address the already identified concerns. Of course, I do not dismiss the possibility that future technological breakthroughs could fundamentally disrupt the privacy landscape. For example, RF sensing's ability to see through walls has raised new concerns about intrusiveness [Core4]. Yet, while we should critically observe technological innovations, it seems more likely that further research will refine, rather than radically redefine, our understanding of privacy concerns.

4.2 A Privacy Research Playbook to Elicit Effective Mechanisms

In our second research question (**RQ2**), we asked: How can privacy concerns in intelligent environments be effectively mitigated? We addressed this question through seven investigations in which we developed mitigation strategies targeting the privacy concerns identified earlier. Three of these investigations focused on tangible privacy mechanisms, which we found to be particularly promising for smart home environments.

In the vision outlined at the beginning of this dissertation, we emphasized the need for human-centered mechanisms that integrate seamlessly into daily life. Our tangible smart home privacy board presented in [Core10] exemplifies this vision by making privacy management effortless. Thanks to its convenient placement and intuitive interaction, participants could easily incorporate it into their routines and one participant specifically noted how they would "quickly turn the knob" when leaving home, highlighting how they embedded privacy management into their daily behavior. Beyond these concrete prototypes, we also developed two abstract design frameworks: one for mitigating technology-facilitated privacy violations in the physical world, and one for enabling effective consent in spontaneous technology interactions. Drawing from these investigations, we propose a research playbook to elicit effective privacy-preserving mechanisms in intelligent environments (see Figure 4.2).

The Privacy Research Playbook is a practical guide to help researchers design and evaluate privacy-preserving mechanisms. It consists of four steps, each with a goal and recommended methods: (1) **Understanding the problem space:** The goal is to identify privacy-relevant situations that require mitigation mechanisms. I recommend using user-centered methods such as surveys, focus groups, and interviews to develop a scenario taxonomy. (2) **Selecting a**

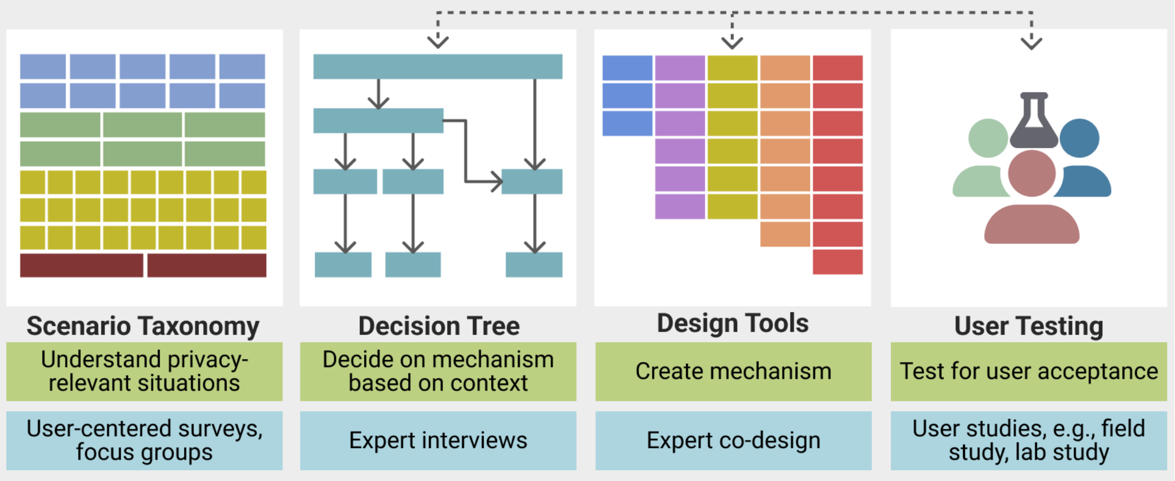
Scenario Taxonomy
Understand privacy-relevant situations
User-centered surveys, focus groups
Decision Tree
Decide on mechanism based on context
Expert interviews
Design Tools
Create mechanism
Expert co-design
User Testing
Test for user acceptance
User studies, e.g., field study, lab study

Figure 4.2: A privacy research playbook to elicit effective privacy mitigation mechanisms in intelligent environments. The playbook has four steps. Each step has a goal (top green box) and a method (bottom blue box). The arrows above the tools indicate an iterative process, indicating that researchers might revisit earlier steps based on evaluation outcomes.

strategy: Here, the aim is to choose the most suitable mitigation mechanism based on the specific context. I recommend creating a decision tree informed by expert discussions about privacy strategies. (3) **Designing the mechanism:** At this stage, the goal is to create concrete mechanisms by considering all possible design attributes through design tools. These tools can be derived by systematically analyzing expert sketches from co-design activities. (4) **Testing the mechanism:** Finally, the mechanism needs to be evaluated for user acceptance and usability through lab or field studies, depending on the prototype's maturity. If the user test reveals issues, the researcher should return to the design tools to explore different design realizations. If testing reveals fundamental problems, the researcher can return to the decision tree to select an alternative strategy. By following these steps, researchers can systematically identify privacy challenges and develop effective, user-accepted mitigation strategies. The iterative nature of the playbook ensures that design solutions remain responsive to user needs and context-specific constraints.

In practice, the process could look like the following. Imagine a researcher wants to design a privacy-preserving mechanism for an assistive domestic robot. First, they conduct surveys and focus groups with users to understand privacy-relevant situations in homes, including what types of data users are concerned about and which contextual factors shape these concerns. This results in a scenario taxonomy describing typical contexts where users want control over their privacy. Next, the researcher asks privacy experts to use the taxonomy to create privacy-relevant situations and to design concrete mechanisms while thinking aloud. Afterward, they discuss the appropriateness of the mechanisms under different circumstances. Based on these discussions, a decision tree maps contextual parameters to the different types of mechanisms, such as notice-and-choice mechanisms or privacy-by-design solutions. Next, the designs are systematically evaluated to distill the different design parameters, including, for example, the timing, modality, and content of the mechanisms. The researcher or designer can then use these tools to implement a concrete mechanism. Finally, the researcher conducts a lab study with users to evaluate the usability and acceptance of the prototype. To improve understanding, the researcher can return to the design tools if the mechanisms appear effective but need minor refinements, such as different text. However, if the prototype does not align with users' situational expectations, the researcher might return to the decision tree and select a different mechanism type. Through this process, the researcher systematically moves from understanding privacy concerns to developing and testing a theoretically grounded and user-validated solution.

4.3 Methodological Reflections on Privacy Research in HCI

Privacy concerns are inherently subjective. As a result, researchers must often rely on self-reported data collected through interviews or questionnaires. While these methods help capture users' beliefs and intentions, they may not accurately reflect actual behavior [69]. The reliance on self-reported measures becomes even more critical when studying emerging technologies such as RF sensing or advanced domestic robots. Since these technologies are not yet widely adopted, participants are typically unfamiliar with them, so researchers must thoroughly explain the technology and its implications before asking questions about it. Our studies found that supporting participant immersion through visuals and videos significantly improved engagement and response quality, especially in large-scale online surveys. Here, researchers should also be wary of potential Large Language Model (LLM) use. We found that including self-attestation statements, using character counters to detect pasted text, and disabling copy-paste functionality can help discourage the use of an LLM and foster authentic responses. However, these are ultimately short-term mitigations in what is likely to become an arms race. As LLMs become increasingly capable of mimicking human responses, HCI researchers must grapple with the risk of misuse and the temptation to replace participants altogether. While recent work has reflected on replacing human responses with LLMs [117], I argue that such approaches fall short when investigating novel or disruptive technologies. LLMs are trained on existing data and cannot substitute for authentic human perception, particularly in early-stage research, where user reactions, intuitions, and concerns often diverge from prior discourse. In the long term, we need robust frameworks to evaluate participant authenticity and critical reflection on where LLM-generated responses are appropriate and where they fundamentally fail to capture lived experience.

The second half of this dissertation focused on evaluating the effectiveness of privacy-preserving prototypes. One key challenge is that the narrative can heavily influence user perceptions. We showed in [Pub4] that simply framing a prototype as privacy-enhancing can make users feel better protected, even when the prototype lacks any real functionality. In our study, participants even reported seeing less personalized content, despite no actual visual changes. This highlights how perceived privacy can be shaped not only by a system's actual functionality, but also by the story researchers provide. Hence, accounting for potential placebo effects in privacy studies is crucial. We suggest including perception control conditions to help isolate the effects of narrative framing from genuine technical improvements. Whenever introducing a placebo condition is not feasible, we recommend acknowledging a potential placebo effect in the interpretations or accounting for the effect post-study in the statistical analysis. Finally, while we favored in-the-wild deployments over short-term lab studies throughout our investigations [Core8, Core9, Core10, Pub3], I recognize that even two-week deployments might be too short to cause actual behavior change. Haliburton et al. [52] found in their study in the context of smartphone overuse interventions that the biggest magnitude of behavior change occurs in the first three weeks, and we found in [Pub3] through a mid-study questionnaire that the initial excitement about the tool wore off after five days and participants started to use it differently. Hence, I call for even more extended deployments to measure the actual impact of privacy-preserving tools over time. Yet, I also acknowledge that such long-term deployments might be challenging due to the typical short duration of PhD projects, participant fluctuation, and technological challenges, as the prototypes need to function reliably over extended periods.

4.4 Reflections on the Future of Privacy in Intelligent Environments

Most of the concrete prototypes we developed in this thesis are “on-top solutions,” i.e., interventions built onto existing products to mitigate privacy symptoms rather than address the root causes. Such solutions would be unnecessary if the underlying technologies were inherently privacy-preserving or embedded in regulatory environments that proactively prevented privacy violations. The European Union has attempted to create such an environment through the GDPR, which mandates principles like data minimization, privacy by design, and non-discrimination. However, the GDPR’s effectiveness is limited. Companies continue exploiting loopholes due to narrow interpretations of the law, weak enforcement mechanisms, or penalties too minor to serve as real deterrents. This makes a strong case for continued research into “on-top” privacy solutions that offer individuals greater control. Yet, individual control as a privacy strategy has also experienced criticism. For example, Kröger et al. [71] argue that individual control is a myth as it fails to account for broader societal consequences and reinforces a model where privacy becomes a personal burden rather than a collective right. Hartzog [54] goes further, claiming that privacy control is not only ineffective but harmful and illusory, as the available controls are typically constrained and preselected by data collectors. Further, in the context of cookie banners, companies often employ deceptive patterns [98] to nudge users toward consenting to the most intrusive options. Still, I argue that privacy controls can empower users. But only when supported by robust legal and regulatory frameworks that ensure meaningful choices and accountability.

Interestingly, the GDPR clearly requires that users provide informed consent for data collection, emphasizing principles such as easy accessibility and plain language. Moreover, the

GDPR mandates that data subjects must know who is collecting their data and for what purposes [109]. However, in practice, this requirement is often interpreted narrowly: providers are expected only to present the information without ensuring that users truly comprehend it. This raises a critical question: how can we be sure that users actually understand what they are consenting to? One way to address this is to shift the burden of proof to providers, requiring them to demonstrate that users understand their data practices before consent is considered valid. For example, one might envision mechanisms like a brief quiz that users must complete before proceeding to a website or service. Critics may argue that this is impractical, as even simple cookie banners are perceived as time-consuming and burdensome. However, such measures could fundamentally reshape the consent landscape. Under the right regulatory framework, where non-compliance is met with significant fines and misconduct is actively pursued, providers might limit data collection to what is strictly necessary and present information in genuinely accessible ways. This would ensure that consent is not just a legal formality but a meaningful safeguard of users' rights. Ultimately, achieving this requires not just technical solutions but also robust legislation and enforcement to hold providers accountable.

This need for strong regulatory frameworks becomes even more urgent with the rise of technologies like AI and RF sensing, which often operate invisibly or require large amounts of data. Some even warn that privacy may soon become a relic of the past. Prior research suggest that many individuals are willing to trade privacy for convenience and functionality, which might be interpreted as consent [1]. But this view risks oversimplification. Privacy is not merely a matter of individual preference. Even if some are willing to give it up, the consequences, such as surveillance and dissemination of false information [75], can affect others who did not make that choice. This is precisely where regulatory interventions are crucial. Much like public health laws restrict harmful substances regardless of individual consent, privacy laws should protect citizens from systemic risks they cannot meaningfully opt out of. This would also relieve individuals from the constant burden of making complex privacy decisions and, instead, ensure baseline protections for all.

4.5 Conclusion

This dissertation aims to understand and mitigate privacy concerns in intelligent environments. Motivated by the growing capabilities of emerging technologies and the increasing adoption of sensor-rich devices, we first explored people's mental models and privacy concerns in future intelligent environments. Through four investigations, we moved from investigating current technologies to more advanced and autonomous systems. In the second half of the dissertation, we focused on addressing these concerns through seven projects. We developed conceptual frameworks and concrete prototypes emphasizing tangible privacy control and awareness for smart homes. Our findings show that privacy concerns are shaped by users' understanding of the technology, as well as by personal, technological, and situational factors. I condensed these insights into a conceptual model of privacy concerns in intelligent environments in the discussion. Here, I also reflect on whether research on privacy concerns may be approaching saturation, making truly novel contributions increasingly rare. The studies in the second half of the dissertation suggest that tangible privacy mechanisms offer a promising path toward usable and seamlessly integrated privacy management. Building on two conceptual frameworks, I derived a research playbook for eliciting privacy-preserving mechanisms in intelligent environments. I conclude the discussion by reflecting on methodological challenges in usable privacy research, particularly the limitations of relying on subjective measures and the potential for placebo effects to skew study results. I contribute toward a privacy-preserving future in intelligent environments by contributing a model of privacy concerns and a framework for designing effective countermeasures.

4.6 Final Remarks

The boundary between technology and everyday life continues to blur as intelligent environments become pervasive. Instead of requiring explicit commands, devices can now sense, interpret, and act — often invisibly and continuously. This challenges the feasibility of traditional, consent-based privacy approaches such as notices or user-managed settings. This dissertation contributes to a deeper understanding of privacy concerns in such environments and offers concrete strategies to address them. We focused on translating concerns into human-centered mechanisms, e.g., through tangible interfaces, contextual communication strategies, and conceptual frameworks. With that, our work demonstrates that privacy management can be embedded into daily routines and made more intuitive without undermining the functionality of intelligent systems. Yet, the next wave of privacy research must tackle challenges beyond individual control. Privacy is not merely a personal concern but is shared and negotiated across social contexts such as households and workplaces. At the same time, new privacy issues arise as AI agents become more autonomous and can make decisions and act on users' behalf. These include misaligned delegation (i.e., a system acts in a way that misaligns with the users' expectations or values), unintended inference (i.e., a system draws conclusions from sensor data or behavior without users' awareness), and opaque action (e.g., a system does something without the users' knowledge). Tackling these challenges calls for a new research agenda focused on (1) transparency mechanisms to clearly communicate what autonomous agents do and why; (2) override systems that let users predefine boundaries, intervene in real-time, or undo agent actions; and (3) accountability interfaces that allow users to retrace what data was shared, when, and with whom, which enables them to meaningfully adjust system behavior to their needs. Ultimately, the goal is not just to minimize harm but to envision a future where privacy is sustained by default and socially negotiated, technologically embedded, and systemically enforced.

Clarification of Contributions

Table 4.1 gives an overview of the contributions of all collaborators on the core publications included in this thesis.

Table 4.1: Clarification of contributions for all core publications.

	Begin of Table
	Contributions
[Core1]	I was the first author and led this project. The concept was developed collaboratively through weekly meetings with **Sven Mayer**. I took the lead in conducting the study, analyzing the data, and writing the paper. Throughout the process, Sven Mayer provided valuable feedback, contributed to refining the studies, helped analyze the data, helped film the videos for the study, and assisted in revising the paper draft.
[Core2]	This work builds on **Magdalena Schlegel's** master thesis, which I co-supervised with **Sven Mayer**. Magdalena Schlegel conducted the studies, and we collaboratively analyzed the data. I took the lead in the final data analysis and the paper writing process. Sven Mayer provided support throughout all stages, including conceptualization, data analysis, and paper writing.
[Core3]	I was the first author and led this project. The work was developed collaboratively through weekly meetings with **Jan Leusmann** and **Sven Mayer**. I conducted studies 1 and 3, while I conducted study 2 together with Jan Leusmann. Throughout, I received valuable feedback and engaged in discussions with both Jan Leusmann and Sven Mayer. I also took the lead on data analysis and paper writing, with support from Jan Leusmann and Sven Mayer. **Sebastian S. Feger** and **Albrecht Schmidt** contributed to the conceptualization and high-level vision of this work.
[Core4]	This work was conducted during my research visit at Carnegie Mellon University in Pittsburgh. I was the first author and led the project. The concept and studies were collaboratively developed through weekly meetings with **Lorrie Cranor**, **Omer Akgul**, and **Nathan Malkin**. I took the lead in conducting the studies, analyzing the data, and writing the paper. All authors provided valuable feedback throughout the process, contributed to refining the studies, and assisted in revising the paper draft.

Continuation of Table 4.1

	Contributions
[Core5]	This work builds on **Verena Winterhalter's** master thesis, which I co-supervised with **Sven Mayer**. Verena Winterhalter conducted the studies, and we collaboratively analyzed the qualitative data. I led the final data analysis and the paper writing process. **Albrecht Schmidt** contributed to shaping the concept and providing the high-level vision for this work.
[Core6]	This work builds on **Petra Laboda's** master thesis, which I co-supervised with **Sven Mayer**. Petra Laboda conducted the studies, and we collaboratively analyzed the qualitative data. I led the final data analysis and the paper writing process.
[Core7]	I was the first author and led this project. The concept was developed collaboratively through weekly meetings with **Sebastian S. Feger**. I took the lead in conducting the studies, analyzing the data, and writing the paper. Throughout the process, Sebastian S. Feger provided valuable feedback, contributed to refining the studies, and assisted in revising the paper draft.
[Core8]	I was the first author and led this project. The concept was developed collaboratively through weekly meetings with **Sebastian S. Feger**. I led the execution of the studies, data analysis, and paper writing. Sebastian S. Feger contributed by creating study artifacts, including 3D printing and constructing the wooden dashboard, and provided support in data analysis and paper writing. **Albrecht Schmidt** guided the overall vision of the paper and contributed to writing the discussion.
[Core9]	This work builds on **Alexander Hiesinger's** master thesis, which I co-supervised with **Robin Welsch** and **Sebastian S. Feger**. Alexander Hiesinger developed the prototype, conducted the studies, and performed the initial data analysis. I led the final data analysis and the paper writing process. Robin Welsch contributed to data analysis, conceptualization, and paper writing. Sebastian S. Feger provided support in conceptualization, prototype development, and paper writing. **Albrecht Schmidt** shaped the overarching concept and high-level vision of the paper.

Continuation of Table 4.1	
	Contributions
[Core10]	This work builds on **Philipp Thalhammer's** and **David Müller's** master theses, which I co-supervised with **Sebastian S. Feger**. The students developed the prototype, conducted the studies, and carried out the initial data analysis. I led the final data analysis and the paper writing process. Sebastian S. Feger contributed to the conceptualization, prototype development, and paper writing. **Albrecht Schmidt** shaped the overarching concept and provided the high-level vision for the paper.
End of Table	

List of Figures

List of Tables

Glossary

AR Augmented Reality

ATI Affinity for Technology Interaction

CCPA California Consumer Privacy Act

FIPs Fair Information Practice Principles

GDPR General Data Protection Regulation

HIPAA Health Insurance Portability and Accountability Act

IUIPC Internet Users’ Information Privacy Concerns

LLM Large Language Model

OSF Open Science Framework

PETs Privacy-Enhancing Technologies

RF Radio Frequency

TaPSI Tangible Privacy and Security Interfaces

VAS Visual Analog Scale

References

[1] Acquisti, A. and Grossklags, J. 'Privacy and rationality in individual decision making.' In: *IEEE Security & Privacy* 3.1 (2005), pp. 26–33. DOI: 10.1109/MSP.2005.22.

[2] Adib, Fadel, Kabelac, Zach, Katabi, Dina, and Miller, Robert C. '3D Tracking via Body Radio Reflections.' In: *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*. Seattle, WA: USENIX Association, 2014, pp. 317–329.

[3] Adib, Fadel and Katabi, Dina. 'See through walls with WiFi!' In: *SIGCOMM Comput. Commun. Rev.* 43.4 (2013), pp. 75–86. DOI: 10.1145/2534169.2486039.

[4] Adib, Fadel, Mao, Hongzi, Kabelac, Zachary, Katabi, Dina, and Miller, Robert C. 'Smart Homes that Monitor Breathing and Heart Rate.' In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. CHI '15. Seoul, Republic of Korea: Association for Computing Machinery, 2015, pp. 837–846. DOI: 10.1145/2702123.2702200.

[5] Ahmad, Imtiaz, Farzan, Rosta, Kapadia, Apu, and Lee, Adam J. 'Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy.' In: *Proc. ACM Hum.-Comput. Interact.* 4.CSCW2 (2020). DOI: 10.1145/3415187.

[6] Ahmed, Tousif, Kapadia, Apu, Potluri, Venkatesh, and Swaminathan, Manohar. 'Up to a Limit? Privacy Concerns of Bystanders and Their Willingness to Share Additional Information with Visually Impaired Users of Assistive Technologies.' In: *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2.3 (2018). DOI: 10.1145/3264899.

[7] Ali, Kamran, Liu, Alex X., Wang, Wei, and Shahzad, Muhammad. 'Keystroke Recognition Using WiFi Signals.' In: *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. MobiCom '15. Paris, France: Association for Computing Machinery, 2015, pp. 90–102. DOI: 10.1145/2789168.2790109.

[8] Allen, Anita. Unpopular privacy: What must we hide? Oxford University Press, 2011.

[9] Apthorpe, Noah, Reisman, Dillon, and Feamster, Nick. 'A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic.' In: *Workshop on Data and Algorithmic Transparency* (2016).

[10] Apthorpe, Noah, Reisman, Dillon, Sundaresan, Srikanth, Narayanan, Arvind, and Feamster, Nick. 'Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic.' In: *arXiv preprint arXiv:1708.05044* (2017). DOI: 10.48550/arXiv.1708.05044.

[11] Apthorpe, Noah, Shvartzshnaider, Yan, Mathur, Arunesh, Reisman, Dillon, and Feamster, Nick. 'Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity.' In: *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2.2 (2018). DOI: 10.1145/3214262.

[12] Arabo, Abdullahi, Brown, Ian, and El-Moussa, Fadi. 'Privacy in the Age of Mobility and Smart Devices in Smart Homes.' In: *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*. 2012, pp. 819–826. DOI: 10.1109/SocialCom-PASSAT.2012.108.

[13] Banerjee, Arijit, Maas, Dustin, Bocca, Maurizio, Patwari, Neal, and Kasera, Sneha. 'Violating privacy through walls by passive monitoring of radio windows.' In: *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks*. WiSec '14. Oxford, United Kingdom: Association for Computing Machinery, 2014, pp. 69–80. DOI: 10.1145/2627393.2627418.

[14] Barbosa, Natã M, Park, Joon S, Yao, Yaxing, and Wang, Yang. '"What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes.' In: *Proceedings on Privacy Enhancing Technologies* 2019.4 (2019), pp. 211–231. DOI: 10.2478/popets-2019-0066.

[15] Bertarini, Marica. Smart glasses: Interaction, privacy and social implications. Student Report. Zurich, Switzerland: ETH Zurich, Department of Computer Science, 2014.

[16] Blandford, Ann, Furniss, Dominic, and Makri, Stephann. Qualitative HCI Research: Going Behind the Scenes. Synthesis Lectures on Human-Centered Informatics. Cham, Switzerland: Springer Cham, 2016, pp. 51–60. DOI: 10.2200/S00706ED1V01Y201602HCI034.

[17] Bocca, Maurizio, Kaltiokallio, Ossi, Patwari, Neal, and Venkatasubramanian, Suresh. 'Multiple Target Tracking with RF Sensor Networks.' In: *IEEE Transactions on Mobile Computing* 13.8 (2014), pp. 1787–1800. DOI: 10.1109/TMC.2013.92.

[18] California Consumer Privacy Act of 2018. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. California Civil Code Title 1.81.5, Sections 1798.100–1798.199. 2018.

[19] Calo, M. Ryan. 'Peeping Hals.' In: *Artificial Intelligence* 175.5 (2011). DOI: 10.1016/j.artint.2010.11.025.

[20] Calo, Ryan. 'Robotics and the Lessons of Cyberlaw.' In: *California Law Review* 103.3 (2015).

[21] Carnegie Mellon University. The Personalized Privacy Assistant Project. https://privacyassistant.org/. Last accessed: April 9, 2025. 2019.

[22] Cavoukian, Ann. 'Privacy by Design: The 7 Foundational Principles.' In: *Information and Privacy Commissioner of Ontario, Canada* 5 (2009), p. 12.

[23] Chalhoub, George, Kraemer, Martin J, Nthala, Norbert, and Flechais, Ivan. '"It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products.' In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI '21. Yokohama, Japan: Association for Computing Machinery, 2021. DOI: 10.1145/3411764.3445691.

[24] Changede, Shrenik and Dhekne, Ashutosh. 'IntruSense: an enhanced physical security system using UWB.' In: *Proceedings of the 23rd Annual International Workshop on Mobile Computing Systems and Applications*. HotMobile '22. Tempe, Arizona: Association for Computing Machinery, 2022, pp. 41–47. DOI: 10.1145/3508396.3512884.

[25] Chen, Andrew Tzer-Yeu, Biglari-Abhari, Morteza, and Wang, Kevin I-Kai. 'Context is King: Privacy Perceptions of Camera-based Surveillance.' In: *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*. New York, NY, USA: IEEE, 2018, pp. 1–6. DOI: 10.1109/AVSS.2018.8639448.

[26] Chen, Yuxin, Li, Huiying, Teng, Shan-Yuan, Nagels, Steven, Li, Zhijing, Lopes, Pedro, Zhao, Ben Y., and Zheng, Haitao. 'Wearable Microphone Jamming.' In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI '20. Honolulu, HI, USA: Association for Computing Machinery, 2020, pp. 1–12. DOI: 10.1145/3313831.3376304.

[27] Chetty, Kevin, Smith, Graeme E., and Woodbridge, Karl. 'Through-the-Wall Sensing of Personnel Using Passive Bistatic WiFi Radar at Standoff Distances.' In: *IEEE Transactions on Geoscience and Remote Sensing* 50.4 (2012), pp. 1218–1226. DOI: 10.1109/TGRS.2011.2164411.

[28] Chung, Ji Won, Fu, Xiyu Jenny, Deocadiz-Smith, Zachary, Jung, Malte F, and Huang, Jeff. 'Negotiating Dyadic Interactions through the Lens of Augmented Reality Glasses.' In: *Proceedings of the 2023 ACM Designing Interactive Systems Conference*. DIS '23. Pittsburgh, PA, USA: Association for Computing Machinery, 2023, pp. 493–508. DOI: 10.1145/3563657.3595967.

[29] Corbett, Matthew, David-John, Brendan, Shang, Jiacheng, Hu, Y. Charlie, and Ji, Bo. 'BystandAR: Protecting Bystander Visual Data in Augmented Reality Systems.' In: *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*. MobiSys '23. Helsinki, Finland: Association for Computing Machinery, 2023, pp. 370–382. DOI: 10.1145/3581791.3596830.

[30] Corbett, Matthew, David-John, Brendan, Shang, Jiacheng, Hu, Y. Charlie, and Ji, Bo. 'Securing Bystander Privacy in Mixed Reality While Protecting the User Experience.' In: *IEEE Security & Privacy* 22.1 (2024), pp. 33–42. DOI: 10.1109/MSEC.2023.3331649.

[31] Cranor, Lorrie Faith. 'Internet privacy.' In: *Commun. ACM* 42.2 (1999), pp. 28–38. DOI: 10.1145/293411.293440.

[32] Culnan, Mary J and Bies, Robert J. 'Consumer privacy: Balancing economic and justice considerations.' In: *Journal of social issues* 59.2 (2003), pp. 323–342. DOI: 10.1111/1540-4560.00067.

[33] Cyber Security Agency of Singapore. Cybersecurity Certification for Organisations. https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-certification-for-organisations. Accessed: 2025-05-06. 2025.

[34] Denning, Tamara, Dehlawi, Zakariya, and Kohno, Tadayoshi. 'In situ with bystanders of augmented reality glasses: perspectives on recording and privacy-mediating technologies.' In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '14. Toronto, Ontario, Canada: Association for Computing Machinery, 2014, pp. 2377–2386. DOI: 10.1145/2556288.2557352.

[35] Denning, Tamara, Matuszek, Cynthia, Koscher, Karl, Smith, Joshua R., and Kohno, Tadayoshi. 'A spotlight on security and privacy risks with future household robots: attacks and lessons.' In: *Proc. of the 11th International Conference on Ubiquitous Computing*. UbiComp '09. Orlando, Florida, USA: ACM, 2009. DOI: 10.1145/1620545.1620564.

[36] Diederichs, Kailtyn, Qiu, Amy, and Shaker, George. 'Wireless Biometric Individual Identification Utilizing Millimeter Waves.' In: *IEEE Sensors Letters* 1.1 (2017), pp. 1–4. DOI: 10.1109/LSENS.2017.2673551.

[37] Do, Youngwook, Park, Jung Wook, Wu, Yuxi, Basu, Avinandan, Zhang, Dingtian, Abowd, Gregory D., and Das, Sauvik. 'Smart Webcam Cover: Exploring the Design of an Intelligent Webcam Cover to Improve Usability and Trust.' In: *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5.4 (2022). DOI: 10.1145/3494983.

[38] Emami-Naeini, Pardis, Agarwal, Yuvraj, Cranor, Lorrie Faith, and Hibshi, Hanan. 'Ask the experts: What should be on an IoT privacy and security label?' In: *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2020, pp. 447–464. DOI: 10.1109/SP40000.2020.00043.

[39] Emami-Naeini, Pardis, Dheenadhayalan, Janarth, Agarwal, Yuvraj, and Cranor, Lorrie Faith. 'An Informative Security and Privacy "Nutrition" Label for Internet of Things Devices.' In: *IEEE Security & Privacy* 20.2 (2022), pp. 31–39. DOI: 10.1109/MSEC.2021.3132398.

[40] Emami-Naeini, Pardis, Dixon, Henry, Agarwal, Yuvraj, and Cranor, Lorrie Faith. 'Exploring How Privacy and Security Factor into IoT Device Purchase Behavior.' In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI '19. Glasgow, Scotland Uk: Association for Computing Machinery, 2019, pp. 1–12. DOI: 10.1145/3290605.3300764.

[41] Fan, Lijie, Li, Tianhong, Fang, Rongyao, Hristov, Rumen, Yuan, Yuan, and Katabi, Dina. 'Learning Longterm Representations for Person Re-Identification Using Radio Signals.' In: *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. New York, NY, USA: IEEE, 2020, pp. 10696–10706. DOI: 10.1109/CVPR42600.2020.01071.

[42] Federal Communications Commission. U.S. Cyber Trust Mark. https://www.fcc.gov/CyberTrustMark. Accessed: 2025-05-06. 2025.

[43] Federal Trade Commission. Fair Information Practice Principles. https://www.ftc.gov/tips-advice/business-center/guidance/privacy-online-fair-information-practices. Accessed: April 3, 2025. 2012.

[44] Franke, Thomas, Attig, Christiane, and Wessel, Daniel. 'A personal resource for technology interaction: development and validation of the affinity for technology

interaction (ATI) scale.' In: *International Journal of Human–Computer Interaction* 35.6 (2019), pp. 456–467. DOI: 10.1080/10447318.2018.1456150.

[45] Funke, Frederik and Reips, Ulf-Dietrich. 'Why Semantic Differentials in Web-Based Research Should Be Made from Visual Analogue Scales and Not from 5-Point Scales.' In: *Field Methods* 24.3 (2012). DOI: 10.1177/1525822X12444061.

[46] Gallardo, Andrea, Choy, Chris, Juneja, Jaideep, Bozkir, Efe, Cobb, Camille, Bauer, Lujo, and Cranor, Lorrie. 'Speculative Privacy Concerns about AR Glasses Data Collection.' In: *Proceedings on Privacy Enhancing Technologies* 2023.4 (2023), pp. 416–435. DOI: 10.56553/popets-2023-0117.

[47] Geeng, Christine and Roesner, Franziska. 'Who's In Control? Interactions In Multi-User Smart Homes.' In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, 2019, pp. 1–13.

[48] Geneiatakis, Dimitris, Kounelis, Ioannis, Neisse, Ricardo, Nai-Fovino, Igor, Steri, Gary, and Baldini, Gianmarco. 'Security and privacy issues for an IoT based smart home.' In: *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. 2017, pp. 1292–1297. DOI: 10.23919/MIPRO.2017.7973622.

[49] Gerber, Nina, Reinheimer, Benjamin, and Volkamer, Melanie. 'Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats.' In: *Proceedings of An Interactive Workshop on the Human aspects of Smarthome Security and Privacy (WSSP)*. Baltimore, MD, USA: USENIX, 2018.

[50] Gerber, Nina, Reinheimer, Benjamin, and Volkamer, Melanie. 'Investigating people's privacy risk perception.' In: *Proceedings on Privacy Enhancing Technologies* (2019). DOI: 10.2478/popets-2019-0047.

[51] Gross, Ralph and Acquisti, Alessandro. 'Information revelation and privacy in online social networks.' In: *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. WPES '05. Alexandria, VA, USA: Association for Computing Machinery, 2005, pp. 71–80. DOI: 10.1145/1102199.1102214.

[52] Haliburton, Luke, Grüning, David Joachim, Riedel, Frederik, Schmidt, Albrecht, and Terzimehić, Nađa. 'A Longitudinal In-the-Wild Investigation of Design Frictions to Prevent Smartphone Overuse.' In: *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. CHI '24. Honolulu, HI, USA: Association for Computing Machinery, 2024. DOI: 10.1145/3613904.3642370.

[53] Harboe, Gunnar and Huang, Elaine M. 'Real-World Affinity Diagramming Practices: Bridging the Paper-Digital Gap.' In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. CHI '15. Seoul, Republic of Korea: Association for Computing Machinery, 2015, pp. 95–104. DOI: 10.1145/2702123.2702561.

[54] Hartzog, Woodrow. 'The case against idealising control.' In: *Eur. Data Prot. L. Rev.* 4 (2018), p. 423.

[55] Hartzog, Woodrow. 'What is privacy? That's the wrong question.' In: *U. Chi. L. Rev.* 88 (2021), p. 1677.

[56] Health Insurance Portability and Accountability Act of 1996 (HIPAA). https://www.hhs.gov/hipaa/for-professionals/privacy/index.html. Public Law 104-191. 1996.

[57] Hsu, Chen-Yu, Ahuja, Aayush, Yue, Shichao, Hristov, Rumen, Kabelac, Zachary, and Katabi, Dina. 'Zero-Effort In-Home Sleep and Insomnia Monitoring using Radio Signals.' In: *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1.3 (2017). DOI: 10.1145/3130924.

[58] Hu, Jinhan, Iosifescu, Andrei, and LiKamWa, Robert. 'LensCap: split-process framework for fine-grained visual privacy control for augmented reality apps.' In: *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*. MobiSys '21. Virtual Event, Wisconsin: Association for Computing Machinery, 2021, pp. 14–27. DOI: 10.1145/3458864.3467676.

[59] Hu, Yuming, Zhu, Mingyu, Jin, Qiao, Qian, Feng, and Li, Bin. 'MagicCloth: Protect User Privacy in AR Streaming.' In: *Proceedings of the 1st ACM Workshop on Mobile Immersive Computing, Networking, and Systems*. ImmerCom '23. Madrid, Spain: Association for Computing Machinery, 2023, pp. 222–228. DOI: 10.1145/3615452.3617936.

[60] Hudig, Anna Ida and Singh, Jatinder. 'Intimate Data Sharing: Enhancing Transparency and Control in Fertility Tracking.' In: *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. CHI '25. Association for Computing Machinery, 2025. DOI: 10.1145/3706598.3714089.

[61] Jana, Suman, Narayanan, Arvind, and Shmatikov, Vitaly. 'A Scanner Darkly: Protecting User Privacy from Perceptual Applications.' In: *2013 IEEE Symposium on Security and Privacy*. New York, NY, USA: IEEE, 2013, pp. 349–363. DOI: 10.1109/SP.2013.31.

[62] Jensen, Jk, Hu, Jinhan, Rahmati, Amir, and LiKamWa, Robert. 'Protecting Visual Information in Augmented Reality from Malicious Application Developers.' In: *The 5th ACM Workshop on Wearable Systems and Applications*. WearSys '19. Seoul, Republic of Korea: Association for Computing Machinery, 2019, pp. 23–28. DOI: 10.1145/3325424.3329659.

[63] Jia, Yunhan Jack, Chen, Qi Alfred, Wang, Shiqi, Rahmati, Amir, Fernandes, Earlence, Mao, Zhuoqing Morley, Prakash, Atul, and Unviersity, SJ. 'ContexloT: Towards providing contextual integrity to appified IoT platforms.' In: *NDSS*. Vol. 2. 2. San Diego. 2017, pp. 2–2.

[64] Jin, Haojian, Guo, Boyuan, Roychoudhury, Rituparna, Yao, Yaxing, Kumar, Swarun, Agarwal, Yuvraj, and Hong, Jason I. 'Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes.' In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. CHI '22. New Orleans, LA, USA: Association for Computing Machinery, 2022. DOI: 10.1145/3491102.3517602.

[65] Kablo, Emiram and Arias-Cabarcos, Patricia. 'Privacy in the Age of Neurotechnology: Investigating Public Attitudes towards Brain Data Collection and Use.' In: *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. CCS '23. Copenhagen, Denmark: Association for Computing Machinery, 2023, pp. 225–238. DOI: 10.1145/3576915.3623164.

[66] Kaminski, Margot E, Rueben, Matthew, Smart, William D, and Grimm, Cindy M. 'Averting robot eyes.' In: *Md. L. Rev.* 76 (2016).

[67] Kjeldskov, Jesper and Skov, Mikael B. 'Was it worth the hassle? ten years of mobile HCI research discussions on lab and field evaluations.' In: *Proceedings of the 16th International Conference on Human-Computer Interaction with Mobile Devices & Services*. MobileHCI '14. Toronto, ON, Canada: Association for Computing Machinery, 2014, pp. 43–52. DOI: 10.1145/2628363.2628398.

[68] Koelle, Marion, Ananthanarayan, Swamy, Czupalla, Simon, Heuten, Wilko, and Boll, Susanne. 'Your smart glasses' camera bothers me! exploring opt-in and opt-out gestures for privacy mediation.' In: *Proceedings of the 10th Nordic Conference on Human-Computer Interaction*. NordiCHI '18. Oslo, Norway: Association for Computing Machinery, 2018, pp. 473–481. DOI: 10.1145/3240167.3240174.

[69] Kokolakis, Spyros. 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon.' In: *Computers & Security* 64 (2017), pp. 122–134. DOI: https://doi.org/10.1016/j.cose.2015.07.002.

[70] Kotsios, Andreas. 'Privacy in an augmented reality.' In: *International Journal of Law and Information Technology* 23.2 (2015), pp. 157–185. DOI: 10.1093/ijlit/eav003.

[71] Kröger, Jacob Leon, Lutz, Otto Hans-Martin, and Ullrich, Stefan. 'The Myth of Individual Control: Mapping the Limitations of Privacy Self-management.' In: *SSRN Electronic Journal* (2021). SSRN Scholarly Paper No. 3881776. DOI: 10.2139/ssrn.3881776.

[72] Kwon, Hyosun, Fischer, Joel E., Flintham, Martin, and Colley, James. 'The Connected Shower: Studying Intimate Data in Everyday Life.' In: *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2.4 (2018). DOI: 10.1145/3287054.

[73] Lafontaine, Evan, Sabir, Aafaq, and Das, Anupam. 'Understanding People's Attitude and Concerns towards Adopting IoT Devices.' In: *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI'21. New York, NY, USA: Association for Computing Machinery, 2021. DOI: 10.1145/3411763.3451633.

[74] Lau, Josephine, Zimmerman, Benjamin, and Schaub, Florian. 'Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers.' In: *Proc. ACM Hum.-Comput. Interact.* 2.CSCW (2018). DOI: 10.1145/3274371.

[75] Lee, Hao-Ping (Hank), Yang, Yu-Ju, Von Davier, Thomas Serban, Forlizzi, Jodi, and Das, Sauvik. 'Deepfakes, Phrenology, Surveillance, and More! A Taxonomy of AI Privacy Risks.' In: *Proceedings of the 2024 CHI Conference on Human Factors*

in Computing Systems. CHI '24. Honolulu, HI, USA: Association for Computing Machinery, 2024. DOI: 10.1145/3613904.3642116.

[76] Lee, Min Kyung, Tang, Karen P., Forlizzi, Jodi, and Kiesler, Sara. 'Understanding Users' Perception of Privacy in Human-Robot Interaction.' In: *Proc. of the 6th International Conference on Human-Robot Interaction*. HRI '11. Lausanne, Switzerland: ACM, 2011. DOI: 10.1145/1957656.1957721.

[77] Leitão, Roxanne. '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, CA, USA: Association for Computing Machinery, 2019, pp. 527–539. DOI: 10.1145/3322276.3322366.

[78] Lin, Huichen and Bergmann, Neil W. 'IoT Privacy and Security Challenges for Smart Home Environments.' In: *Information* 7.3 (2016). DOI: 10.3390/info7030044.

[79] Liu, Hankai, Liu, Xiulong, Xie, Xin, Tong, Xinyu, Shi, Tuo, and Li, Keqiu. 'Application-Oriented Privacy Filter for mmWave Radar.' In: *IEEE Communications Magazine* 61.12 (2023), pp. 168–174. DOI: 10.1109/MCOM.011.2200580.

[80] Liu, Jianwei, Xiao, Chaowei, Cui, Kaiyan, Han, Jinsong, Xu, Xian, Ren, Kui, and Mao, Xufei. 'A Behavior Privacy Preserving Method towards RF Sensing.' In: *2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS)*. New York, NY, USA: IEEE, 2021, pp. 1–10. DOI: 10.1109/IWQOS52092.2021.9521278.

[81] Luo, Jun, Cao, Hangcheng, Jiang, Hongbo, Yang, Yanbing, and Chen, Zhe. 'MIMOCrypt: Multi-User Privacy-Preserving Wi-Fi Sensing via MIMO Encryption.' In: *arXiv preprint arXiv:2309.00250* (2023).

[82] Luria, Michal, Hoffman, Guy, and Zuckerman, Oren. 'Comparing Social Robot, Screen and Voice Interfaces for Smart-Home Control.' In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. CHI '17. Denver, Colorado, USA: Association for Computing Machinery, 2017, pp. 580–628. DOI: 10.1145/3025453.3025786.

[83] Lutz, Christoph, Schöttler, Maren, and Hoffmann, Christian Pieter. 'The privacy implications of social robots: Scoping review and expert interviews.' In: *Mobile Media & Communication* 7.3 (2019). DOI: 10.1177/2050157919843961.

[84] Lutz, Christoph and Tamó-Larrieux, Aurelia. 'The robot privacy paradox: Understanding how privacy concerns shape intentions to use social robots.' In: *Human-Machine Communication* 1 (2020). DOI: 10.30658/hmc.1.6.

[85] Malhotra, Naresh K, Kim, Sung S, and Agarwal, James. 'Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model.' In: *Information systems research* 15.4 (2004), pp. 336–355. DOI: 10.1287/isre.1040.0032.

[86] Malkin, Nathan, Bernd, Julia, Johnson, Maritza, and Egelman, Serge. '"What Can't Data Be Used For?" Privacy Expectations about Smart TVs in the US.' In: *Proceedings of the 3rd European Workshop on Usable Security (EuroUSEC), London, UK*. 2018. DOI: 10.14722/eurousec.2018.23016.

[87] Mare, Shrirang, Roesner, Franziska, and Kohno, Tadayoshi. 'Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts.' In: *Proceedings on Privacy Enhancing Technologies* 2020.2 (2020), pp. 436–458. DOI: 10.2478/popets-2020-0035.

[88] Marky, Karola, Prange, Sarah, Krell, Florian, Mühlhäuser, Max, and Alt, Florian. '"You just can't know about everything": Privacy Perceptions of Smart Home Visitors.' In: *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia*. MUM '20. Essen, Germany: Association for Computing Machinery, 2020, pp. 83–95. DOI: 10.1145/3428361.3428464.

[89] Marky, Karola, Voit, Alexandra, Stöver, Alina, Kunze, Kai, Schröder, Svenja, and Mühlhäuser, Max. '"I Don't Know How to Protect Myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments.' In: *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. NordiCHI '20. Tallinn, Estonia: Association for Computing Machinery, 2020. DOI: 10.1145/3419249.3420164.

[90] Matejka, Justin, Glueck, Michael, Grossman, Tovi, and Fitzmaurice, George. 'The Effect of Visual Appearance on the Performance of Continuous Sliders and Visual Analogue Scales.' In: *Proc. of the 2016 CHI Conference on Human Factors in Computing Systems*. CHI '16. San Jose, California, USA: ACM, 2016. DOI: 10.1145/2858036.2858063.

[91] McDonald, Aleecia M and Cranor, Lorrie Faith. 'The Cost of Reading Privacy Policies.' In: *Isjlp* 4 (2008), p. 543.

[92] McReynolds, Emily, Hubbard, Sarah, Lau, Timothy, Saraf, Aditya, Cakmak, Maya, and Roesner, Franziska. 'Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys.' In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. CHI '17. Denver, Colorado, USA: Association for Computing Machinery, 2017, pp. 5197–5207. DOI: 10.1145/3025453.3025735.

[93] Molina-Markham, Andrés, Shenoy, Prashant, Fu, Kevin, Cecchet, Emmanuel, and Irwin, David. 'Private Memoirs of a Smart Meter.' In: *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*. BuildSys '10. Zurich, Switzerland: Association for Computing Machinery, 2010, pp. 61–66. DOI: 10.1145/1878431.1878446.

[94] Moncrieff, Simon, Venkatesh, Svetha, and West, Geoff. 'Dynamic Privacy in a Smart House Environment.' In: *2007 IEEE International Conference on Multimedia and Expo*. 2007, pp. 2034–2037. DOI: 10.1109/ICME.2007.4285080.

[95] Naeini, Pardis Emami, Bhagavatula, Sruti, Habib, Hana, Degeling, Martin, Bauer, Lujo, Cranor, Lorrie Faith, and Sadeh, Norman. 'Privacy Expectations and Preferences in an IoT World.' In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, 2017, pp. 399–412.

[96] Nissenbaum, Helen. 'Privacy as Contextual Integrity.' In: *Washington Law Review* 79.1 (2004), pp. 119–159.

[97] Nissenbaum, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Redwood City: Stanford University Press, 2009. DOI: doi:10.1515/9780804772891.

[98] Nouwens, Midas, Liccardi, Ilaria, Veale, Michael, Karger, David, and Kagal, Lalana. 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence.' In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI '20. Honolulu, HI, USA: Association for Computing Machinery, 2020, pp. 1–13. DOI: 10.1145/3313831.3376321.

[99] Obermaier, Johannes and Hutle, Martin. 'Analyzing the Security and Privacy of Cloud-Based Video Surveillance Systems.' In: *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*. IoTPTS '16. Xi'an, China: Association for Computing Machinery, 2016, pp. 22–28. DOI: 10.1145/2899007.2899008.

[100] Ozturk, Muhammed Zahid, Wu, Chenshu, Wang, Beibei, and Liu, K. J. Ray. 'RadioMic: Sound Sensing via Radio Signals.' In: *IEEE Internet of Things Journal* 10.5 (2023), pp. 4431–4448. DOI: 10.1109/JIOT.2022.3217968.

[101] Prange, Sarah, Mayer, Sven, Bittl, Maria-Lena, Hassib, Mariam, and Alt, Florian. 'Investigating User Perceptions Towards Wearable Mobile Electromyography.' In: *Human-Computer Interaction – INTERACT 2021: 18th IFIP TC 13 International Conference, Bari, Italy, August 30 – September 3, 2021, Proceedings, Part IV*. Bari, Italy: Springer-Verlag, 2021, pp. 339–360. DOI: 10.1007/978-3-030-85610-6_20.

[102] Prange, Sarah, Rodriguez, Sarah Delgado, Mecke, Lukas, and Alt, Florian. '"I saw your partner naked": Exploring Privacy Challenges During Video-based Online Meetings.' In: *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia*. MUM '22. Lisbon, Portugal: Association for Computing Machinery, 2022, pp. 71–82. DOI: 10.1145/3568444.3568468.

[103] Profita, Halley, Albaghli, Reem, Findlater, Leah, Jaeger, Paul, and Kane, Shaun K. 'The AT Effect: How Disability Affects the Perceived Social Acceptability of Head-Mounted Display Use.' In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. CHI '16. San Jose, California, USA: Association for Computing Machinery, 2016, pp. 4884–4895. DOI: 10.1145/2858036.2858130.

[104] Pu, Qifan, Gupta, Sidhant, Gollakota, Shyamnath, and Patel, Shwetak. 'Whole-home gesture recognition using wireless signals.' In: *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*. MobiCom '13. Miami, Florida, USA: Association for Computing Machinery, 2013, pp. 27–38. DOI: 10.1145/2500423.2500436.

[105] Qiao, Yue, Zhang, Ouyang, Zhou, Wenjie, Srinivasan, Kannan, and Arora, Anish. 'PhyCloak: Obfuscating Sensing from Communication Signals.' In: *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. Santa Clara, CA: USENIX Association, 2016, pp. 685–699.

[106] Raja, Muneeba and Sigg, Stephan. 'Applicability of RF-based methods for emotion recognition: A survey.' In: *2016 IEEE International Conference on Pervasive Computing*

and Communication Workshops (PerCom Workshops). New York, NY, USA: IEEE, 2016, pp. 1–6. DOI: 10.1109/PERCOMW.2016.7457119.

[107] Raval, Nisarg, Srivastava, Animesh, Lebeck, Kiron, Cox, Landon, and Machanavajjhala, Ashwin. 'MarkIt: privacy markers for protecting visual secrets.' In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*. UbiComp '14 Adjunct. Seattle, Washington: Association for Computing Machinery, 2014, pp. 1289–1295. DOI: 10.1145/2638728.2641707.

[108] Reagle, Joseph and Cranor, Lorrie Faith. 'The platform for privacy preferences.' In: *Commun. ACM* 42.2 (1999), pp. 48–55. DOI: 10.1145/293411.293455.

[109] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj. Official Journal of the European Union, L 119, 4 May 2016, pp. 1–88. 2016.

[110] Reidenberg, Joel R, Breaux, Travis, Cranor, Lorrie Faith, French, Brian, Grannis, Amanda, Graves, James T, Liu, Fei, McDonald, Aleecia, Norton, Thomas B, Ramanath, Rohan, et al. 'Disagreeable privacy policies: Mismatches between meaning and users' understanding.' In: *Berkeley Tech. LJ* 30 (2015), p. 39. DOI: 10.2139/SSRN.2418297.

[111] Reips, Ulf-Dietrich and Funke, Frederik. 'Interval-level measurement with visual analogue scales in Internet-based research: VAS Generator.' In: *Behavior Research Methods* 40.3 (2008). DOI: 10.3758/BRM.40.3.699.

[112] Resuli, Nuerzati, Skubic, Marjorie, and Kovaleski, Scott. 'Learning Room Structure and Activity Patterns Using RF Sensing for In-Home Monitoring of Older Adults.' In: *2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*. New York, NY, USA: IEEE, 2020, pp. 2054–2061. DOI: 10.1109/BIBM49941.2020.9313335.

[113] Rodriguez, Sarah Delgado, Prange, Sarah, Ossenberg, Christina Vergara, Henkel, Markus, Alt, Florian, and Marky, Karola. 'PriKey – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors.' In: *Proceedings of the 12th Nordic Conference on Human-Computer Interaction:* NordiCHI '22. delgado2022nordichi. Denmark: Association for Computing Machinery, 2022.

[114] Roesner, Franziska, Denning, Tamara, Newell, Bryce Clayton, Kohno, Tadayoshi, and Calo, Ryan. 'Augmented reality: hard problems of law and policy.' In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*. UbiComp '14 Adjunct. Seattle, Washington: Association for Computing Machinery, 2014, pp. 1283–1288. DOI: 10.1145/2638728.2641709.

[115] Roesner, Franziska, Kohno, Tadayoshi, and Molnar, David. 'Security and privacy for augmented reality systems.' In: *Commun. ACM* 57.4 (2014), pp. 88–96. DOI: 10.1145/2580723.2580730.

[116] Roesner, Franziska, Molnar, David, Moshchuk, Alexander, Kohno, Tadayoshi, and Wang, Helen J. 'World-Driven Access Control for Continuous Sensing.' In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. CCS '14. Scottsdale, Arizona, USA: Association for Computing Machinery, 2014, pp. 1169–1181. DOI: `10.1145/2660267.2660319`.

[117] Schmidt, Albrecht, Elagroudy, Passant, Draxler, Fiona, Kreuter, Frauke, and Welsch, Robin. 'Simulating the Human in HCD with ChatGPT: Redesigning Interaction Design with AI.' In: *Interactions* 31.1 (2024), pp. 24–31. DOI: `10.1145/3637436`.

[118] Shah, Syed Aziz and Fioranelli, Francesco. 'RF Sensing Technologies for Assisted Daily Living in Healthcare: A Comprehensive Review.' In: *IEEE Aerospace and Electronic Systems Magazine* 34.11 (2019), pp. 26–44. DOI: `10.1109/MAES.2019.2933971`.

[119] Sharkey, Noel and Sharkey, Amanda. 'The eldercare factory.' In: *Gerontology* 58.3 (2012). DOI: `10.1159/000329483`.

[120] Sheehan, Kim Bartel and Hoy, Mariea Grubbs. 'Dimensions of Privacy Concern among Online Consumers.' In: *Journal of Public Policy & Marketing* 19.1 (2000), pp. 62–73. DOI: `10.1509/jppm.19.1.62.16949`. eprint: `https://doi.org/10.1509/jppm.19.1.62.16949`.

[121] Shenoy, Jayanth, Liu, Zikun, Tao, Bill, Kabelac, Zachary, and Vasisht, Deepak. 'RF-protect: privacy against device-free human tracking.' In: *Proceedings of the ACM SIGCOMM 2022 Conference*. SIGCOMM '22. Amsterdam, Netherlands: Association for Computing Machinery, 2022, pp. 588–600. DOI: `10.1145/3544216.3544256`.

[122] Shu, Jiayu, Zheng, Rui, and Hui, Pan. 'Cardea: Context-aware visual privacy protection from pervasive cameras.' In: *arXiv preprint arXiv:1610.00889* (2016). DOI: `10.48550/arXiv.1610.00889`.

[123] Shu, Jiayu, Zheng, Rui, and Hui, Pan. 'Your Privacy Is in Your Hand: Interactive Visual Privacy Control with Tags and Gestures.' In: *Communication Systems and Networks*. Cham: Springer International Publishing, 2017, pp. 24–43. DOI: `10.1007/978-3-319-67235-9_3`.

[124] Sigg, Stephan, Scholz, Markus, Shi, Shuyu, Ji, Yusheng, and Beigl, Michael. 'RF-Sensing of Activities from Non-Cooperative Subjects in Device-Free Recognition Systems Using Ambient and Local Signals.' In: *IEEE Transactions on Mobile Computing* 13.4 (2014), pp. 907–920. DOI: `10.1109/TMC.2013.28`.

[125] Singh, Akash Deep, Wang, Brian, Garcia, Luis, Chen, Xiang, and Srivastava, Mani. 'Understanding factors behind IoT privacy–A user's perspective on RF sensors.' In: *arXiv preprint arXiv:2401.08037* (2024).

[126] Solove, Daniel J. '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy.' In: *San Diego Law Review* 44 (2007), pp. 745–772.

[127] Solove, Daniel J. Understanding Privacy. Harvard University Press, 2008.

[128] Spiekermann, Sarah and Cranor, Lorrie Faith. 'Engineering privacy.' In: *IEEE Transactions on software engineering* 35.1 (2008), pp. 67–82. DOI: 10.1109/TSE.2008.88.

[129] Tan, Sheng and Yang, Jie. 'WiFinger: leveraging commodity WiFi for fine-grained finger gesture recognition.' In: *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. MobiHoc '16. Paderborn, Germany: Association for Computing Machinery, 2016, pp. 201–210. DOI: 10.1145/2942358.2942393.

[130] Templeman, Robert, Korayem, Mohammed, Crandall, David, and Kapadia, Apu. 'PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces.' In: *NDSS '14: Proceedings of the 2014 Network and Distributed System Security Symposium*. ISBN 1-891562-35-5. San Diego, CA, USA: Internet Society, 2014.

[131] Thakkar, Parth Kirankumar, He, Shijing, Xu, Shiyu, Huang, Danny Yuxing, and Yao, Yaxing. '"It Would Probably Turn into a Social Faux-Pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes.' In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. CHI '22. New Orleans, LA, USA: Association for Computing Machinery, 2022. DOI: 10.1145/3491102.3502137.

[132] Tiefenau, Christian, Häring, Maximilian, Gerlitz, Eva, and Zezschwitz, Emanuel von. Making Privacy Graspable: Can we Nudge Users to use Privacy Enhancing Techniques? 2019. DOI: 10.48550/ARXIV.1911.07701.

[133] Tonkin, Meg, Vitale, Jonathan, Ojha, Suman, Clark, Jesse, Pfeiffer, Sammy, Judge, William, Wang, Xun, and Williams, Mary-Anne. 'Embodiment, Privacy and Social Robots: May I Remember You?' In: *Social Robotics: 9th International Conference*. ICSR 2017. Springer. 2017. DOI: 10.1007/978-3-319-70022-9_50.

[134] Townsend, Daphne, Knoefel, Frank, and Goubran, Rafik. 'Privacy versus autonomy: A tradeoff model for smart home monitoring technologies.' In: *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. New York, NY, USA: IEEE, 2011, pp. 4749–4752. DOI: 10.1109/IEMBS.2011.6091176.

[135] Trepte, Sabine and Masur, Philipp K. 'Cultural differences in social media use, privacy, and self-disclosure: Research report on a multicultural study.' In: (2016).

[136] United Nations. Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights. Accessed: 2025-03-27. 1948.

[137] Wang, Yang, Norice, Gregory, and Cranor, Lorrie Faith. 'Who Is Concerned about What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites.' In: *Trust and Trustworthy Computing*. Ed. by Jonathan M. McCune, Boris Balacheff, Adrian Perrig, Ahmad-Reza Sadeghi, Angela Sasse, and Yolanta Beres. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 146–153.

[138] Wang, Yuxi, Wu, Kaishun, and Ni, Lionel M. 'WiFall: Device-Free Fall Detection by Wireless Networks.' In: *IEEE Transactions on Mobile Computing* 16.2 (2017), pp. 581–594. DOI: 10.1109/TMC.2016.2557792.

[139] Warren, S. D. and Brandeis, L. D. 'The Right to Privacy.' In: *Harvard Law Review* 4.5 (1890), pp. 193–220. DOI: 10.2307/1321160.

[140] Westin, Alan F. 'Privacy and freedom.' In: *Washington and Lee Law Review* 25.1 (1968), p. 166.

[141] Wobbrock, Jacob O. and Kientz, Julie A. 'Research Contributions in Human-Computer Interaction.' In: *Interactions* 23.3 (2016), pp. 38–44. DOI: 10.1145/2907069.

[142] Worthy, Peter, Matthews, Ben, and Viller, Stephen. 'Trust Me: Doubts and Concerns Living with the Internet of Things.' In: *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. DIS '16. Brisbane, QLD, Australia: Association for Computing Machinery, 2016, pp. 427–434. DOI: 10.1145/2901790.2901890.

[143] Yang, Yuzhe, Yuan, Yuan, Zhang, Guo, Wang, Hao, Chen, Ying-Cong, Liu, Yingcheng, Tarolli, Christopher G., Crepeau, Daniel, Bukartyk, Jan, Junna, Mithri R., Videnovic, Aleksandar, Ellis, Terry D., Lipford, Melissa C., Dorsey, Ray, and Katabi, Dina. 'Artificial intelligence-enabled detection and assessment of Parkinson's disease using nocturnal breathing signals.' In: *Nature Medicine* 28.10 (2022), pp. 2207–2215. DOI: 10.1038/s41591-022-01932-x.

[144] Yao, Yao, Li, Yan, Liu, Xin, Chi, Zicheng, Wang, Wei, Xie, Tiantian, and Zhu, Ting. 'Aegis: An Interference-Negligible RF Sensing Shield.' In: *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. New York, NY, USA: IEEE, 2018, pp. 1718–1726. DOI: 10.1109/INFOCOM.2018.8485883.

[145] Yao, Yaxing, Basdeo, Justin Reed, Kaushik, Smirity, and Wang, Yang. 'Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes.' In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI '19. Glasgow, Scotland Uk: Association for Computing Machinery, 2019, pp. 1–12. DOI: 10.1145/3290605.3300428.

[146] Yao, Yaxing, Basdeo, Justin Reed, Mcdonough, Oriana Rosata, and Wang, Yang. 'Privacy Perceptions and Designs of Bystanders in Smart Homes.' In: *Proc. ACM Hum.-Comput. Interact.* 3.CSCW (2019). DOI: 10.1145/3359161.

[147] Ye, Tengqi, Moynagh, Brian, Albatal, Rami, and Gurrin, Cathal. 'Negative FaceBlurring: A Privacy-by-Design Approach to Visual Lifelogging with Google Glass.' In: *Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management*. CIKM '14. Shanghai, China: Association for Computing Machinery, 2014, pp. 2036–2038. DOI: 10.1145/2661829.2661841.

[148] Yue, Shichao, He, Hao, Wang, Hao, Rahul, Hariharan, and Katabi, Dina. 'Extracting Multi-Person Respiration from Entangled RF Signals.' In: *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2.2 (2018). DOI: 10.1145/3214289.

[149] Zeng, Youwei, Wu, Dan, Xiong, Jie, Yi, Enze, Gao, Ruiyang, and Zhang, Daqing. 'FarSense: Pushing the Range Limit of WiFi-based Respiration Sensing with CSI Ratio of Two Antennas.' In: *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 3.3 (2019). DOI: 10.1145/3351279.

[150] Zhang, Jie, Tang, Zhanyong, Li, Meng, Fang, Dingyi, Nurmi, Petteri, and Wang, Zheng. 'CrossSense: Towards Cross-Site and Large-Scale WiFi Sensing.' In: *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. MobiCom '18. New Delhi, India: Association for Computing Machinery, 2018, pp. 305–320. DOI: 10.1145/3241539.3241570.

[151] Zhao, Mingmin, Adib, Fadel, and Katabi, Dina. 'Emotion recognition using wireless signals.' In: *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*. MobiCom '16. New York City, New York: Association for Computing Machinery, 2016, pp. 95–108. DOI: 10.1145/2973750.2973762.

[152] Zheng, Serena, Apthorpe, Noah, Chetty, Marshini, and Feamster, Nick. 'User Perceptions of Smart Home IoT Privacy.' In: *Proc. ACM Hum.-Comput. Interact.* 2.CSCW (2018). DOI: 10.1145/3274469.

[153] Zhu, Yanzi, Xiao, Zhujun, Chen, Yuxin, Li, Zhijing, Liu, Max, Zhao, Ben Y, and Zheng, Haitao. 'Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors.' In: *Network and Distributed Systems Security (NDSS) Symposium 2020*. 2020.

A APPENDIX

A.1 Declaration on Writing Aids

This thesis is composed of my and my co-authors' original thoughts and comments. I used Grammarly[1] for grammar and typo corrections and ChatGPT[2] for ideation and proofreading.

[1] https://grammarly.com/

[2] https://chatgpt.com/

A 2

Eidesstattliche Versicherung

(Siehe Promotionsordnung vom 12.07.11, § 8, Abs. 2 Pkt. 5)

Hiermit versichere ich an Eides statt, dass ich die vorliegende Dissertation selbständig und nur mit den angegebenen Hilfsmitteln verfasst habe. Alle Passagen, die ich aus der Literatur oder aus anderen Quellen übernommen habe, habe ich deutlich als Zitat mit Angabe der Quelle kenntlich gemacht.

München, den 1. Juli 2025

Maximiliane Windl