MUNI FSS

JOURNAL OF PSYCHOSOCIAL RESEARCH ON CYBERSPACE
CYBERPSYCHOLOGY

Paupini, C., Kost, D., & Gjøsæter, T. (2026). Balancing the scales of privacy: Perceptions of privacy issues and digital risk among domestic Internet of Things users. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 20*(4), Article 6. https://doi.org/10.5817/CP2026-4-6

Balancing the Scales of Privacy: Perceptions of Privacy Issues and Digital Risk Among Domestic Internet of Things Users

Cristina Paupini [1], *Dominique Kost* [2], *& Terje Gjøsæter* [3]

[1] Department of Computer Science, Oslo Metropolitan University, Oslo, Norway
[2] Department of Leadership and Organizational Behaviour, Norwegian Business School (BI), Oslo, Norway
[3] Department of Information Systems (IS), University of Agder, Agder, Norway

Abstract

While the proliferation of smart home technologies and the domestic Internet of Things (IoT) bring opportunities for a high level of control over household appliances and entertainment systems, it also presents challenges, not least in terms of privacy. In this study, we explore domestic IoT users' perceptions of privacy issues and digital risk through in-depth semistructured interviews and digital home visits with 12 adults in 10 households in Norway. Based on the results of this study, we present a framework for an updated understanding of current privacy protection behaviors and decision-making from the perspective of domestic IoT users. Our "Scales of Privacy" model provides a holistic view of the process underlying the privacy calculus framework, incorporating both perceived risks and perceived benefits of data disclosure and including neutralizing factors, such as privacy cynicism and "nothing to hide" arguments. The results show a variety of perceived sources of risk, including national entities, technology companies, hackers, and partners/family. However, we highlight a discrepancy between the understanding of risk and perceived risk of our informants, on the one hand, and their actual behavior, on the other. We examine users' stated reasons for utilizing an IoT-connected technology despite the risk, identifying five underlying motivations. Two were intrinsically related to the frictionless user experience provided by the devices (i.e., convenience and ease of use), whereas the remaining three (i.e., inevitability, unimpeachability and indiscernibility) revealed attitudes toward privacy protection partially influenced by a sense of being overwhelmed by the friction-filled experience of setting boundaries around personal data in the current digital environment.

Keywords: Internet of Things; privacy; illusion of understanding; risk perception; privacy cynicism

Editorial Record

First submission received:
April 24, 2025

Revisions received:
January 15, 2026
May 17, 2026

Accepted for publication:
May 30, 2026

Editor in charge:
Lenka Dedkova

Introduction

With the COVID-19 pandemic, the adoption of smart home technologies has accelerated significantly, and the most recent projections estimate that the total number of domestic Internet of Things (IoT) devices adopted by 2030 will be close to 39 billion globally (Sinha, 2025). This surge can be attributed to a heightened demand for comfort and efficiency in various aspects of consumers' lives based on the ability of the IoT to create a network of devices that share information with the purpose of increasing the level of automation for users (Hassija et al.,

2019). In a smart home setup, IoT-connected devices, such as thermostats, lighting systems, security cameras, door locks, and appliances, can be conveniently monitored, controlled, and managed remotely through a central hub or smartphone app. For example, homeowners now have the ability to monitor and adjust the temperature, lighting, door access, and security cameras of their homes from anywhere via an internet connection (Korneeva et al., 2021).

Recent literature reviews emphasize that domestic IoT ecosystems create persistent privacy and security challenges because the devices used in such systems continuously collect, transmit, and sometimes share sensitive household data across interconnected platforms and with third parties. These risks are amplified by weak default configurations, uneven update practices, and fragmented security standards across consumer IoT markets (Kumar, 2025; Magara & Zhou, 2024b). Despite these concerns, IoT adoption continues to increase, even though many users remain only partially aware of the privacy risks involved (Al Muhander et al., 2025; Nemmaoui et al., 2023). This tension is commonly discussed in terms of the privacy paradox and the privacy calculus model. However, these frameworks offer limited insight into how users evaluate risks under conditions of opacity and may overestimate user understanding of privacy-related information. To investigate this subject, we adopt a qualitative approach that examines how users make sense of privacy risks to justify the continued use of the domestic IoT. In doing so, we develop a conceptualization of privacy-related decision-making that goes beyond a simple risk–benefit trade-off. Specifically, we show that users' evaluations are shaped not only by perceived benefits but also by justificatory arguments that downplay privacy concerns and by users' overestimation of their own understanding of privacy risks. By identifying these mechanisms, this study provides new insight into how privacy-related decisions are made under conditions of uncertainty and information opacity.

Background

In the following section, we explore different aspects of risk and risk perception as well as different approaches to privacy protection as a background for the study.

The Issues With the Domestic Internet of Things and Privacy Protection

Privacy and security are generally recognized as two critical areas of risk in regard to accessing and using technology (Al-Suhimat et al., 2024; Fei et al., 2023; Magara & Zhou, 2024a), and this is especially relevant for domestic IoT technologies, as such technologies access, manage and record sensitive data about users. As domestic IoT technologies become increasingly pervasive, the number of unintended data breach reports has been rising rapidly (Ferrara & Spoto, 2018; Kumar, 2025). Despite the growth in IoT adoption, the security of IoT-linked devices has not kept pace (Buntak et al., 2021; Shakya et al., 2025), and many such devices, especially home-based ones, have deficient security systems and upgrade opportunities (Magara & Zhou, 2024b; Xi & Ling, 2016). According to Angrishi, part of the reason for such a lack of focus on security features in IoT devices is the way domestic technology is perceived compared to what it actually is: a smart refrigerator, for example, tends to be considered an upgraded regular refrigerator, even though it would be more accurate to consider it a computer that keeps things cold (Angrishi, 2017). The difference, in this case, is in the perceived security and privacy risk that is associated with a refrigerator vs. a computer, and the consequence of it is that the design of IoT devices often does not include security measures at all (Angrishi, 2017).

An even more salient element of risk in regard to domestic IoT technologies has been identified in the users' approach to privacy protection. Research indicates that nearly half of users are unaware of the privacy risks associated with IoT devices (Al Muhander et al., 2025; Internet Society, & Consumers International, 2019), and a survey by Deloitte (2016) revealed that 91% of people agree with the terms and conditions of using such devices without reading them, a rate that increases to 97% among people aged 18–34 years (Deloitte, 2016). Furthermore, most of the tools designed to protect users' privacy and personal data on IoT devices are not accessible for people with disabilities, older people and other groups of socially disadvantaged individuals (Saka & Das, 2025). As a consequence, such users are frequently forced to rely on the help of family members or others who have technical skills (Fuglerud, 2011).

Privacy Risk Perception

Privacy risks in domestic IoT devices are not only a topic of academic debate but also a concern for end users. While targeted advertising may seem benign, the harvesting of location data can reveal highly sensitive behavioral patterns, such as which health clinics or pharmacies you visit. This information has been sold, for example, to political operatives, who use it to influence messaging (Tau, 2023). Moreover, many IoT vendors share household data with unnamed contractors and third-party service providers, creating opaque data flows that increase the chance of leaks or misuse (Zuboff, 2019). Finally, always-on devices, such as smart speakers and cameras, can transmit live audio and video directly back to corporate entities (Lutz & Newlands, 2021). Both Amazon Alexa and Ring have been criticized for allowing employees and external partners to review private recordings—sometimes of minors—to train machine-learning algorithms (Jillson, 2023).

These examples demonstrate 'contextual transgressions', which violate the reasonable expectation of privacy given the context, for instance, when information shared in one context (e.g., social interaction or domestic life) is repurposed in another (e.g., advertising, surveillance, or profiling) (Nissenbaum, 2004). According to Nissenbaum, privacy expectations are grounded in socially learned norms governing appropriate information flows in specific contexts (Nissenbaum, 2004). The expectation of privacy tends to be greater in the context of one's private home than it is on public transportation, for example. However, the aggressive digitalization of the domestic environment and of most other aspects of social life has rendered the boundaries between different contexts more opaque and collapsible, facilitating increasing violation of users' privacy (Nissenbaum, 2011).

The collapse of contextual boundaries intensifies users' vulnerability and increases users' privacy risk. In this paper, we define perceived privacy risk as the perceived threat that arises from an increased level of information that technology gathers about its users (Collier, 1995; McLean & Osei-Frimpong, 2019). Past research has identified perceived risk as an important factor determining both the usage and adoption of IoT devices (Lau et al., 2018; McLean & Osei-Frimpong, 2019). In a qualitative study, Lau et al. (2018) reported that individuals who were highly concerned with privacy refrained from adopting IoT devices regardless of their age (Lau et al., 2018). Similarly, previous research has found no statistically significant differences between young adults and older people in terms of privacy concerns and the level of literacy on the subject of privacy (Hoofnagle et al., 2010; Kezer et al., 2016). Conversely, McLean and Osei-Frimpong (2019) reported that perceived privacy risks reduce users' usage of IoT devices (McLean & Osei-Frimpong, 2019). This definition, however, implies that IoT users only perceive one source of privacy risk, namely, the collection of personal data, and that users are aware of the privacy risks stemming from collecting personal data. Perceived privacy risk is more nuanced; users perceive risks from different sources (Lutz & Newlands, 2021; Raynes-Goldie, 2010).

One can distinguish between vertical risks (i.e., risks stemming from the organization providing the IoT device, third-party contractors and app developers, and governments) and horizontal risks (i.e., perceived privacy risks stemming from strangers and household members) (Lutz & Newlands, 2021). This distinction is important because IoT users do not appear to treat privacy risk as a single, uniform category. Rather, they assign different levels of concern to different sources of risk, suggesting that their evaluations are based on subjective perceptions rather than on a clear assessment of the probability of actual harm. For example, Lutz and Newlands (2021) reported that participants were particularly concerned about privacy risks stemming from institutions, especially third-party developers (Lutz & Newlands, 2021).

This uneven weighing of risk sources suggests that users may not fully understand the objective likelihood of different privacy threats. In turn, this limited ability to assess the probability of actual harm may help explain why users accept certain risks and continue to use their IoT devices (Lau et al., 2018). Although studies have demonstrated that risk perception may lower the adoption and usage of IoT devices (Lau et al., 2018; McLean & Osei-Frimpong, 2019), other research suggests that users continue using IoT devices despite perceiving privacy risks (Hoffmann et al., 2016). This phenomenon is also referred to as the privacy paradox: users indicate being concerned about their privacy but are nevertheless willing to share private information online (John, 2015; Norberg et al., 2007) and despite having the intention to protect their privacy.

Findings on the privacy paradox are mixed. Studies on online privacy concerns and the disclosure of personal information have found only limited evidence for its existence (Dienlin et al., 2023), while a recent meta-analysis suggested that the relationship between privacy concerns and privacy-protection behavior depends strongly on how these variables are operationalized and on participants' age (Masur, 2023). In the IoT context, however, the paradox may take a distinct form because IoT-linked devices often depend on highly personalized services. To

benefit fully from such devices, users are frequently required to share personal and sometimes sensitive information, such as health data or voice recordings, despite privacy concerns. Accordingly, IoT scholars have described this dynamic as a personalization–privacy paradox (Lee, 2021). Research in fact shows that users are often willing to personalize IoT devices by sharing personal information even when they express privacy concerns (D. Kim et al., 2019; Lee, 2021).

The privacy literature describes two theoretical foundations that may explain the paradox: users perceiving risks and these perceptions lowering adoption; at the same time, research also demonstrates the continued use of IoT devices despite the perceived risks: i.e., 1) the privacy calculus (Princi & Krämer, 2019) and 2) privacy cynicism (Hoffmann et al., 2016, 2024).

In the following section, we first discuss the privacy calculus framework in the domestic IoT context and the mechanisms underlying this 'cost-outcome' analysis. Second, we discuss the outcomes that IoT users may perceive, including perceived benefits and justifications, such as privacy cynicism.

The Privacy Calculus Model and the Overestimation of Knowledge

The origins of privacy calculus can be traced to Laufer and Wolfe (1977), who developed a theory about calculus of behavior, arguing that individuals perform a cost-benefit analysis concerning disclosure of personal data or, alternatively, a risk-benefit analysis concerning potential misuse of the data, thereby treating their personal information as an economic commodity to be traded (Laufer & Wolfe, 1977). Culnan and Armstrong (1999) applied privacy calculus to model the willingness to disclose personal information during the purchase of products and services, depending on the individual's assessment whether the information would be handled fairly and without negative consequences (Culnan & Armstrong, 1999). Dinev and Hart (2006) further developed an extended privacy calculus model for e-commerce transactions (Dinev & Hart, 2006). Furthermore, D. Kim et al. (2019) applied the privacy calculus idea to IoT services and reported that the willingness to trade personal information for the ability to personalize services is not significantly affected by perceived risk, with the exception of the health care IoT, in which case individuals are generally unwilling to share personal information because of high perceived risk (Kim et al., 2019). Although McLean and Osei-Frimpong (2019) reported that perceived risk decreases the effect of utilitarian and social benefits on IoT usage, the relationship between benefits and usage remains significant. Similarly, previous research has indicated that the greater the perceived benefit of sharing personal information is, i.e., improved personalized services and functionality of the IoT device, the more willing users are to share personal information despite perceived risks (D. Kim et al., 2019).

Prior research has expanded the privacy calculus concept by adding antecedents that shape disclosure decisions (Chen, 2018; Cloarec et al., 2024; Dinev & Hart, 2006; Kehr et al., 2015; Schomakers et al., 2022). One stream of the research integrates trust (e.g., trust beliefs, internet trust) and positive disposition toward the medium (e.g., personal internet interest, happiness with the internet) as factors that can attenuate perceived risks and are associated with greater willingness to disclose (Cloarec et al., 2024; Dinev & Hart, 2006). A second stream separates situational (e.g., information sensitivity, affect) from dispositional influences (e.g., institutional trust), showing that situational cues ultimately steer disclosure even when dispositions set initial intentions (Kehr et al., 2015; Schomakers et al., 2022).

A third line of this research focuses on privacy self-efficacy as an antecedent that shapes both protective actions and sharing (Chen, 2018). Although certain prior models account for affect and mood as bias-inducing factors (Kehr et al., 2015; Schomakers et al., 2022), they still assume that users can rationally evaluate privacy policies. This assumption is problematic in opaque IoT settings and overlooks a key bias: misattributing external information (e.g., policies, search results) to one's own knowledge.

Criticism of the Privacy Calculus Model

The privacy calculus model has, however, more recently been reexamined and critiqued; for example, Fernandes and Pereira (2021) argued that although customers in fact perform a trade-off between perceived benefits and privacy loss, this trade-off is based on an irrational process (Fernandes & Pereira, 2021). Critics of the privacy calculus approach argue that a true trade-off or cost–benefit analysis is impossible since users cannot obtain and hold all of the information and knowledge necessary to make an informed decision (Kokolakis, 2017). For example, Lau et al. (2018) conducted a qualitative study comparing the perceived privacy risks of IoT users and nonusers in which both groups demonstrated a lack of understanding concerning the capabilities of large tech companies to collect and store substantial amounts of private data and to use personal data for targeted ads (Lau et al., 2018).

Privacy decisions are based on a lack of or incomplete understanding of actual privacy risks (Masur, 2020). This finding suggests that IoT users overestimate their knowledge and understanding of privacy. De Ridder argued that people inflate their knowledge and understanding because they do not distinguish between knowledge that is in their head and knowledge that one has access to in one's environment (de Ridder, 2024). For example, IoT users may overestimate their knowledge of privacy risks because they have seen or even scrolled through the terms and conditions when accepting them and know that the privacy terms and conditions are available online. In a series of experiments, participants were asked to answer questions in different knowledge domains; one group was allowed to use Google to answer the questions, while the other group was not. Fisher et al. (2015) reported that people overestimated the amount and quality of knowledge they possessed after being able to consult Google. Participants also overestimated their knowledge in domains that were unrelated to the initial questions (Fisher et al., 2015). Researchers have additionally argued that people regard information that is available on the internet as an extension of their own memory (Fisher et al., 2015; Ward, 2013). Scholars have also reported that this view extends to understanding algorithms; merely having access to explanations on how algorithms function fosters the impression that one understands how an algorithm operates (Ostinelli et al., 2024).

We argue that the same claim holds when users briefly scan or accept IoT terms and conditions. Because application installation forces users to scroll through—and tacitly accept—privacy terms, users misattribute this external information to their own knowledge and thus feel able to identify a variety of risk sources even when they lack the requisite technical fluency (Lutz & Newlands, 2021). This illusion of understanding explains the *perceived risk* in our Scales of Privacy model. Prior research conceptualizes the outcome side of the privacy calculus largely in terms of perceived benefits—for example, convenience, automation, and cost savings (D. Kim et al., 2019; Princi & Krämer, 2020). In this paper, we incorporate neutralizers, privacy cynicism and justifications, such as the "nothing to hide" argument, which actively counterbalance risks as part of the privacy calculus.

Neutralizing Forces: Nothing to Hide and Privacy Cynicism as Equalizers in the Privacy Calculus

Nothing to Hide

In addition to the benefits outlined in the privacy calculus model (Fox, 2020; Princi & Krämer, 2019, 2020), domestic IoT users often use other justifications, such as "nothing to hide" arguments for continued use despite risks. The "nothing to hide" argument implies that as long as one engages in socially acceptable and lawful behavior, one can accept a lack of privacy and even surveillance (Solove, 2007; Stuart & Levine, 2017). In the past, this argument has, for example, been used to justify the acceptance of government surveillance (Solove, 2007). In a study on teenagers in Canada, researchers reported that the "nothing to hide" attitude enables the individual to dismiss privacy as relevant altogether since if one's behavior does not deviate from the norm, privacy is irrelevant (Adorjan & Ricciardelli, 2019). Therefore, the "nothing to hide" argument goes beyond "privacy as forsaken" or privacy cynicism, since privacy is not only futile but irrelevant. The same study also implied that the "nothing to hide" argument was used as a means to shift the responsibility of protecting privacy to the individual user instead of holding the tech companies accountable for better data protection (Adorjan & Ricciardelli, 2019). Furthermore, research has indicated that when confronted with privacy infringement, social media users minimize potential harm by arguing that they have nothing to hide (Marwick & Hargittai, 2019).

In the domestic IoT context, users agree to surveillance since voice-activated devices must be constantly switched on to function properly. Implied in the "nothing to hide" argument is that one can accept potential privacy risks since they are not harmful to the potential user as long as the user does not engage in illegal or unacceptable behavior. Stuart and Levine (2017) reasoned that the "nothing to hide" argument is a false trade-off since it disguises the potentially harmful consequences of privacy infringement (Stuart & Levine, 2017). The argument can therefore be viewed as neutralizing the perceived risk factors in a cost-outcome analysis, i.e., a privacy calculus.

Privacy Cynicism

Hoffmann et al. (2016) describe privacy cynicism as an increasingly prevalent attitude among internet users who are overwhelmed by privacy risks (Hoffmann et al., 2016). This attitude is characterized by apathy, resignation and mistrust toward the handling of personal data by online services and can lead to the perception of privacy protective behavior being futile. Cynicism serves as a coping strategy that enables those who are overwhelmed by privacy risks to overcome their cognitive dissonance and continue to use the online services they find attractive. This can explain the discrepancy between users' understanding of privacy risks and their behavior, i.e., the privacy paradox discussed above (John, 2015; Norberg et al., 2007).

Hoffmann et al. (2024) further reported that privacy cynicism is driven by structural constraints that contribute to restricting user agency. These structural constraints include interpersonal, cultural, technological, economic and political constraints, and these constraints affect different social groups unequally. Intersecting constraints compound and may impact an individual's sense of agency and privacy in unpredictable ways. The effects of social categories, such as gender, race, class, age, religion, disability, politics, or education, intersect and can trigger complex effects that are not obvious from the social categories in isolation; this intersectional perspective (Crenshaw, 1989) helps shed light on such issues. Furthermore, the lack of agency is felt particularly strongly by individuals belonging to multiple intersecting vulnerable groups, which may in turn lead to increased susceptibility to constraints, creating a vicious circle (Hoffmann et al., 2024).

Current Study

In response to the limitations of the research, this study seeks to develop a richer conceptualization of privacy-related decision-making in the context of the domestic IoT. Prior approaches, particularly the privacy calculus model, conceptualize users as weighing perceived risks against benefits (Dinev & Hart, 2006; Hargittai & Marwick, 2016) but assume that users are sufficiently informed to evaluate such trade-offs—an assumption that is problematic in contexts characterized by information opacity (Hoffmann et al., 2016). Moreover, research on privacy cynicism suggests that users may rely on justificatory narratives that downplay or normalize privacy risks (McLean & Osei-Frimpong, 2019).

Taken together, these perspectives indicate that privacy-related decision-making may reflect a more subjective and context-dependent process than existing models suggest. In particular, users may not only weigh perceived benefits against risks but also rely on justificatory responses and overestimate their own understanding of privacy-related information (de Ridder, 2024). To explore these dynamics, we adopt a qualitative approach that examines how users make sense of privacy risks and continued IoT use in everyday contexts. On the basis of this analysis, we develop a conceptual model that captures the mechanisms underlying this evaluation process, which is presented in the Discussion section as an interpretation of the findings.

Research Question and Approach

This study aims to explore the issues we have raised by examining the following research question:

What conceptualization of the privacy calculus can accurately describe privacy risk perception and continued use of the domestic IoT?

We aim to contribute to the privacy literature by investigating the mechanisms that underlie users' cost–benefit trade-offs in the IoT context. Prior research has demonstrated that IoT users engage in a privacy calculus, although they lack full awareness of the true cost and risks of sharing data (Hoffmann et al., 2016); however, it remains unclear which factors users include in their cost–benefit analysis. Therefore, our proposed model distinguishes between neutralizers, benefits, and cognitive mechanisms to demonstrate why users feel capable of an objective cost–outcome assessment—and why that perceived objectivity can be flawed.

Methods

Research Design

This research aims to explore the relationships that IoT users have with their domestic IoT devices, focusing on the perception of privacy and privacy-related risk in the context of a smart household and the routines established around such devices. For the purpose of this study, a smart household is defined as a household containing at least one smart speaker, such as Google Home or Alexa, or three different domestic IoT devices, such as smart light bulbs, smart heaters, and smart vacuum cleaners (Paupini, Teigen, & Habib, 2022). This definition was also the main criterion for the recruitment of participants, together with fluency in conversational English.

The sample consisted of thirteen participants from ten different households, several of whom were couples living together but who were interviewed separately. As shown in Table 1 below, the participants were aged 24 to 81 years, included eight men and five women and were interviewed twice for approximately 1 hour each time. The

interviews were conducted between May and October 2020, mostly via digital platforms, such as Zoom and Skype, because of the COVID-19 restrictions in place at that time.

Table 1. *Summary of the Participants in the Study: Age, Household Composition and IoT Devices.*

Pseudonym	Age	Household composition	Smart home devices
Anders	42	Son (11) and son (8)	Google Nest Hub, two Google Minis, Google Home, vacuum cleaner, TV, six light bulbs (some IKEA Trådfri and some Magic), heating
Bjørnar	35	Wife (34) and daughter (3)	Robot lawn mower, Z-wave moisture measure, Philips Hue lights system (40-50 units), Tesla with app control, Wi-Fi-connected bathroom weight, electric kick bike with app, energy measurement with app, Yale Doorman door lock, Google Nest surveillance camera, Google Home Hub smart speaker, Google Mini speaker, Bluetooth cooking thermometer, weather station, Wi-Fi "anova sous vide circulator", heat pump with app, 3 Google Chromecasts
Cecilie	31	Husband (Daniel, 30) and son (5 months)	Four Google Minis (but only uses two of them), Sonos One and Sonos Beam, Philips Hue lightning strips, nine Philips Hue light bulbs, three TP link plugs, one Nanoleaf lightning panel, one Arlo baby call, one Google Nest
Daniel	30	Wife (Cecilie, 31) and son (5 months)	Four Google Minis (but only use two of them), Sonos One and Sonos Beam, Philips Hue lightning strips, nine Philips Hue light bulbs, three TP link plugs, one Nanoleaf lightning panel, one Arlo baby call, one Google Nest
Erik	24	Wife (Frida, 24)	IKEA Trådfri light bulbs, ZigBee, ConBee2, Xiaomi sensors, Xiaomi light bulbs, (run through Home Assistant software on Raspberry Pi), ZigBee buttons, Google Home Hubs, Chromecast audio
Frida	24	Husband (Erik, 24)	IKEA Trådfri light bulbs, ZigBee, ConBee2, Xiaomi sensors, Xiaomi light bulbs, (run through Home Assistant software on Raspberry Pi), ZigBee buttons, Google Home hubs, Chromecast audio
Gabriella	27	Lives alone, part-time with dog	One Google Home, smart light bulbs, Mills heaters
Harold	74	Lives alone	One Amazon Alexa, two Google Homes, one Roomba vacuum
Ivar	81	Wife (82)	Google Home, Amazon Alexa, Roomba vacuum
Kristin	70	Lives alone	Google Nest Mini
Line	33	Husband (Martin, 34), daughter (6), and son (10 months)	IKEA Trådfri light bulbs, motion sensors, Apple TV, three Sonos speakers, motion sensor, baby call (not connected to Wi-Fi, but it can be)
Martin	34	Wife (Line, 33), daughter (6), and son (10 months).	IKEA Trådfri light bulbs, motion sensors, Apple TV, three Sonos speakers, motion sensor, baby call (not connected to Wi-Fi, but it can be)

The research design entailed two digital house visits and included several qualitative research methods. Two semistructured interviews were performed for each participant, focusing mostly on the interviewees' approach to privacy protection and the choices that guided the adoption of their IoT devices as well as the routines that stemmed from it. The questions in the interviews were aimed at understanding the participants' conceptions of privacy and privacy risk and their approach to privacy protection through recollections of their use of domestic IoT devices. Examples of questions include "How do you feel about IoT devices?", "What are some key considerations you have when buying/choosing new technologies?", "What kinds of data do you think are collected through your devices?", and "What do you think happens to these data? What are they used for?" Second, a walk-along home tour, inspired by Pink et al. (2017) and Coughlan et al. (2013), was performed, in which the research participants showed the researchers through their digital tools, such as tablets or smartphones, where their technological devices were placed in their homes (Coughlan et al., 2013; Pink et al., 2017). This method enabled the researchers to observe the participants' interactions with their environment and infrastructure and their household atmosphere. During the house visits, the participants were also encouraged to re-enact their experiences with their devices and asked to draw a floorplan of their houses, on which they indicated and discussed the placement of their IoT devices.

At the end of the second visit, the informants were assigned a 'homework' assignment to be completed over the next few weeks and consisting mainly of recording themselves, or just their hands, using one of their IoT devices. These recordings were useful for understanding the spaces these devices occupied in the dynamics of the households and, although the recordings were not used for the ultimate purpose of this study, they have been included in additional publications by the same research group.

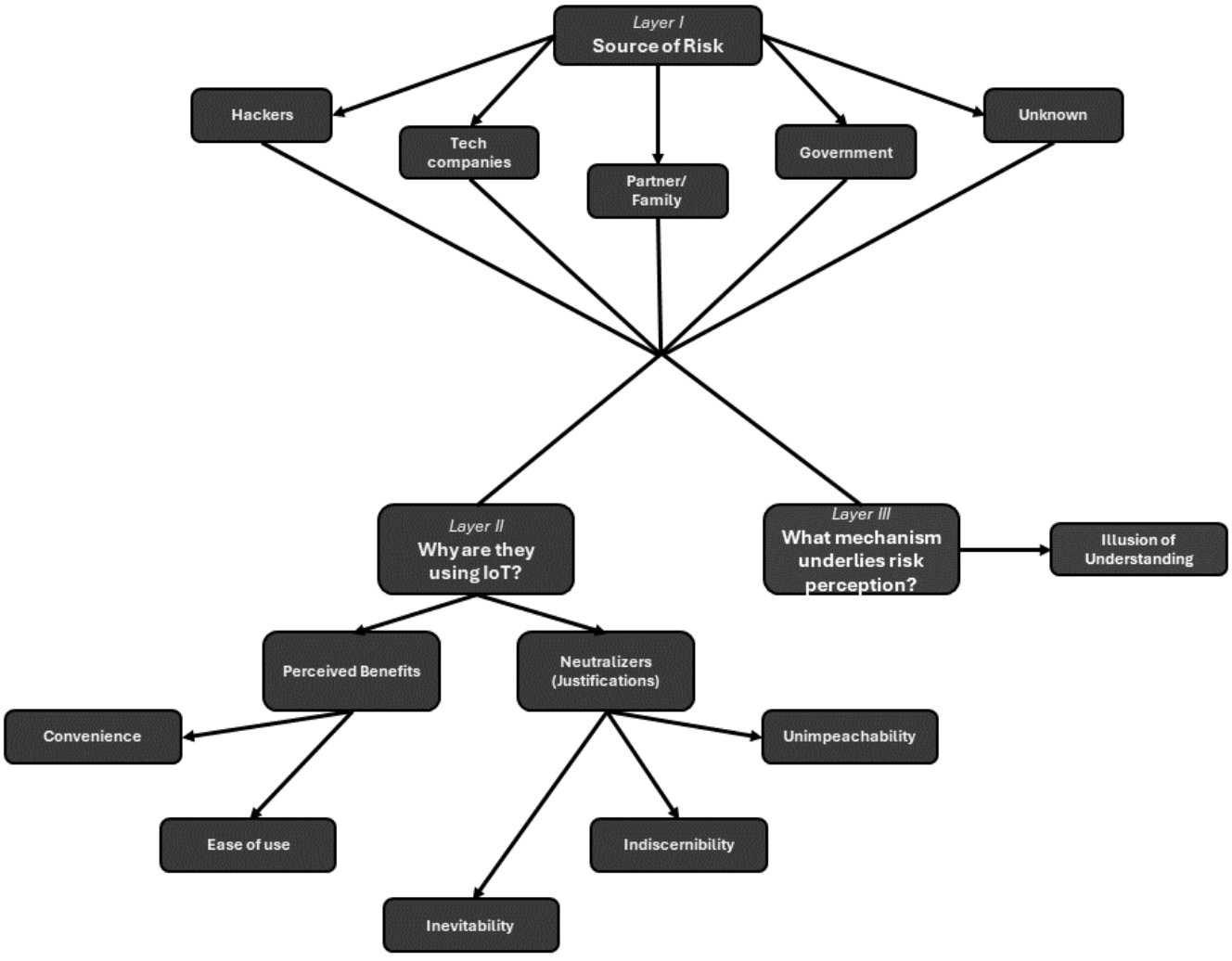
Ethical Considerations

The research project is compliant with the General Data Protection Regulation (GDPR) of the European Union and was approved by the Norwegian National Committee for Ethical Research (SIKT) in all its versions. Additional consent from SIKT was requested and provided when, owing to the COVID-19 pandemic, the methodologies and fieldwork structure had to be redesigned. In accordance with the regulations, all the data collected during the research were treated with confidentiality, and the participants were informed in advance about all aspects of their participation in the study, including the ways in which their data would be treated and for how long. Informed consent was obtained for every phase of the research, and the participants were all anonymized via pseudonyms.

Data Analysis: Inductive Approach

To analyze the collected data, an inductive approach was adopted (Chandra & Shang , 2019; Thomas, 2006) and the transcripts were read several times to distinguish themes and categorize them by grouping quotations with similar topics and meanings. This methodology was applied throughout the process of analysis, allowing the codes to emerge from the text of the transcribed interviews. Once the broad categories were identified, text fragments were organized thematically, and the transcripts were read "horizontally" (Marshall, 1999) while focusing on the broad category of "privacy". Although the coding process was performed primarily by a single researcher, the results were debated and confirmed during multiple rounds of discussion with all the authors of the paper and the subsequent stages of analysis were conducted by at least two authors at the same time. From this point forward, the analysis followed three steps (i.e., analytical layers), during which the data were approached from different perspectives (Figure 1).

Figure 1. *Representation of Findings Within the Process of Analysis.*



As themes started emerging, the codes were organized around what the informants identified as potential sources of risk to their privacy. The identification of five "sources of risk" constitutes the first analytical layer. The next step involved repeating the process while considering the horizontal transcript through the lens of "why" the informants continued using their IoT devices despite perceived risks. This stage initially generated themes related to positive outcomes of use, but it also generated themes that did not reflect benefits as such; rather, the latter themes captured justifications that downplayed or counterbalanced privacy concerns (Layer II). Within Layer II, all of these themes later crystallized into two analytically distinct categories: perceived benefits (e.g., convenience, ease of use) and neutralizers (e.g., inevitability, indiscernibility, unimpeachability). The newly identified themes were discussed and organized, and questions concerning users' perceptions of privacy risk and risk sources emerged, motivating a third round of analysis. This round highlighted a reoccurring metacognitive bias: the tendency among the participants to overestimate their understanding of privacy-related information, which we interpreted as the illusion of understanding (Layer III). The relationships among the three analytical layers were discussed extensively among the authors. Through this iterative process, we developed the conceptual distinctions that later informed the Scales of Privacy model presented in the Discussion section. Importantly, this model was not specified prior to the analysis but emerged through the interpretation of how participants described privacy risks, continued use, and their own understanding of privacy in the domestic IoT context.

Findings

The findings are presented in an order that reflects the analytical structure that emerged through the interpretation of the data. We begin with the illusion of understanding, which we conceptualized as a metacognitive bias, because participants' tendency to overestimate their own knowledge shaped how they perceived and assessed privacy risks. We then turn to the participants' accounts of privacy risk sources and to their explanations of why they continued using IoT devices despite those risks. Within these accounts of continued use, we distinguish between perceived benefits, i.e., positive outcomes associated with domestic IoT use, and neutralizers, i.e., justificatory arguments that downplay or counterbalance privacy concerns. Together, these themes form the empirical basis for the conceptual model developed in the Discussion section. The quotations included in the text have not been altered except for minimal corrections of punctuation or mistakes that do not modify the meaning or intention behind the statements. Pseudonyms were used to protect the identity of the study participants.

Risk Perception Mechanisms: The Illusion of Understanding

Our informants were asked about their privacy settings and the privacy agreements for their IoT devices. Except for a small number of individuals, the participants admitted to not having read the agreements while continuing throughout the interviews to reflect on what type of data were being collected by the devices and how the data were being used. It was therefore possible for the researchers to infer the presence of illusion of understanding mechanisms underlying the participants' decision-making process in most cases. Nonetheless, several informants were descriptive enough in their process to provide detailed examples in the course of their interviews.

Anders, one of the first users interviewed, expressed how, although he did not read through the terms and conditions of his Google Home device, he believed that his data were not being stored and, in any case, were deleted after being used to improve the services. It is interesting to note how he explains that he formulated this conviction by reading other users' experiences online, but toward the end of the quotation, he states that he chooses to believe Google on "that", even though, not having read the terms, he does not truly know what Google is doing:

> "I cannot say I have read through all the terms and agreements but through all the reviews and the research I did online based on other users, eh..., Google is usings- eh using some recording data to improve their detection, ehm, but other than that, they are not storing anything or they're deleting it afterwards, so I choose to believe Google on that and believe that is correct."

A slightly different example is provided by Daniel, a young father with a newborn in the house. Daniel was very honest in explaining how, even though he does not know what setting the privacy level on his IoT devices entails, there is "nothing going on":

> "Oh I don't know (little laughter), I don't know (how the privacy setting of the home devices are). [...] I think that nothing is going on here. It is nothing interesting; we are not talking about anything, anything they would be interested in. I wouldn't think they would listen at all, because we are not saying anything they would like to hear more about."

On the other hand, Harold has much trust in the tech company he chose and bases his understanding of how his data are treated largely on the public statements the company has made over the years:

> "From what I can understand, Apple doesn't gather data. Apple sells devices; they want me to, and they, and what they have done is they build an ecosystem that locks you into Apple pretty much, and they are quite happy with that, you know. So what they want me to do is to buy another iPhone. And I, Apple has been consistent in what they say, in particular, in particular with, with opening pass codes, given access to pin codes, there is a consistent mantra when I read Apple's statements, when I follow some of the stuff that they have been talked about, they are not in the business of data gathering."

Finally, Erik expresses how, even though he has not read through the privacy agreements for his Google Hub, he is sure that these agreements provide information about how the data the device collects will be used with respect to targeted advertisement. Clearly, he is not wrong, but what is relevant here to our concept of the illusion of understanding is his conviction of *knowing* what is in the agreements without actually having read them, an assumption he makes mostly because he knows the information is available somewhere: "I haven't actually read through all the privacy things that you agreed on when you set them up; I'm sure it says something about that (how the data shared is used for targeted advertisement)."

The preceding statements exemplify the illusion of understanding: the participants affirm having knowledge about the terms and conditions without actually having read them.

Perceived Risks

The first layer of analysis of our raw data facilitated the identification of five categories that represent sources of privacy risk according to our informants. These categories essentially define who or what the participants thought could access (unauthorized) and/or abuse the information collected by the IoT devices in their homes. The five sources of risk identified are as follows:

1. Hackers or malignant entities
2. Tech companies
3. Partner, family, or relatives
4. Government or national institutions
5. Unknown

Hackers or Malignant Entities

The most commonly mentioned source of risk by the participants in the study was hackers or some kind of malignant individual, often from a foreign country. The precise forms the description of this risk source assumed varied, but a concern regarding this type of risk was expressed by almost all the informants.

For example, hacking was one of the first considerations Erik made when deciding whether to buy a smart device for his home system:

> "Eh, usually two things I ask myself. The first one is, is this prone to hacking? Can someone sit and hack my server, my Raspberry Pi, or even sit outside and connect to my wireless system? And- and the other thing is that what's- what is- what exposure am I putting on myself? Is this- is it just information about when I turn on, off the lights? Or is it like something controllable? For example, imagine if someone hacked Tesla and they locked the car from outside and you couldn't get in, right?"

In his evaluation, privacy and security are overlapping terms. He questions the level of exposure a device would bring to his home in terms of "what would a hacker be able to do with such information?" The need for privacy protection is expressed, but without reference to the data market or targeted advertising:

> "Yeah. For example, if I- I think I said that last time as well, but I don't have smart locks, so I can't lock my door from outside or inside or unlock it, and that is because when I ask myself those questions, eh..., the- and I got to the second one and asked myself what exposure am I putting on myself, well, the exposure then would be that if somebody were to hack my system or- of some sort, either via internet or sitting outside and connecting to my wireless network, they would actually be able to get into my home. If I weren't at home, they can steal basically everything I own, but- and also if I am at home and sleeping, for example, who knows what they are able to do, right? [Small laugh] So the- those are the two things I usually ask myself during- regarding privacy."

Cecilie makes slightly different considerations while discussing her father's habits when interacting with his smart speaker. In her view, owing to her father's profession, the information he provides is worth protecting from malignant entities:

> "I think for my parents, they also have Google Home, and when my father has home office... they had to turn off their Google speaker because, because of meetings that he, my father is having with his work, and that is, that's more something I understand, because that's information that shouldn't fall into the hands of Russians."

Finally, Anders considers the possibility of lone individuals, not necessarily professional hackers, accessing his data:

> "I'm not confident that it couldn't be.... used in a wrong way. I'm not absolutely certain about it. Because even though there's frameworks in place, both in Europe, Norway and the U.S., there's always that single person that could kind of use information, can get access to information and not adhere to the framework anyway. So, I'm kind of trusting the... not only the framework and the companies, but you're also trusting single employers, employees, and single persons, or who gets access to the information. So, you can't be completely certain; you can't."

In Anders's perspective, it is possible to identify a combination of trust and helplessness in his approach to privacy: he has to trust the individuals handling his personal information in addition to the tech companies that collect it because he sees no alternative solution.

Tech Companies

The second source of risk identified by the participants in the study was the companies that produced and commercialized the devices they were using and, therefore, collected and stored the data.

In the following interview extract, Erik describes how, having taken precautions regarding the way his data are stored, he feels more comfortable that companies have reduced access to his data, even though he realizes that Google, for example, still has access to his data through his Google Home app on his phone:

> "Using Home Assistant, everything is stored locally, here and there's nothing stored in a cloud in the United States where it suddenly pops up on Facebook or something. Eh...eh, and... yeah, basically that. And I- and we also think that...because everything is stored locally on my Raspberry Pi at home and not in the cloud, I am more comfortable with the- with, like, exploring in the system more and adding more devices and everything. Because I know that IKEA or Google or, wait, Google can see it through Google Home but- yeah. Facebook, for example, cannot see what I'm doing."

Frida is Erik's wife and, by her own admission, knows nothing about how the technology functions and usually trusts her husband to take the lead on such matters. When asked about her feelings toward the devices in her house, she expresses clear unease about how the smart speaker "uses" the data it collects:

> "I'm more worried about, like, Google. I don't like the concept with it because sometimes when you are just, like, in a conversation, you don't use Google, you sit in the couch, and you talk about something, then maybe later, I on my phone, and the same thing that we just talked about is coming up on this phone. That freaks me out. And I have not, like, accepted any cookies or

> anything at a website. But the Google, like, catches up on the stuff we're talking about. So, I think that's kind of really intimidating. Yeah. I don't like it."

During the course of the interview, Frida spontaneously elaborated her position and started to consider how different her viewpoint is from her husband's:

> "It's kind of freaky, how it works, I think. Yeah. So, I think maybe my husband is, maybe, a little bit too relaxed about it. I don't know. I think I'm maybe more skeptical. Yeah, I don't know. Yeah. He's, like, "Oh, it's safe, lalala, I have it under control". But if... you never know."

Harold, in contrast, lives alone and does not have to discuss with others his decisions regarding the IoT devices that he introduces in the house. He reflects on the times his smart speaker self-activates by mistake: "I don't like the fact that Google Assistant occasionally wakes up when I haven't asked, I haven't said, Hey, Google. So, Google is listening."

He also expresses a clear preference in terms of tech companies and how he perceives that his data are managed by them:

> "The thing that I like about Apple is that Apple doesn't give stuff away. Apple is not in the business of selling information, but Google is. This is one of the things, one of the main reasons why I will not use a Samsung or an Android-based telephone. The only Google devices where I sort of begrudgingly given away stuff, is through the, the, through my mesh, my mesh points. But they are, they are passive, but I have noticed that Google collects a lot of information about my internet traffic. And I go through my Google privacy pages on my account. I keep, I have got a Google email account, just particularly that reason."

Although Harold expresses a strong preference for Apple's policy on data sharing with third parties, he does not seem to be particularly concerned about the company's internal use of the collected data.

Partner, Family, or Relatives

Certain informants expressed discomfort at the idea of other members of the household accessing data from their smart home devices.

Anders, for example, decided not to include his two sons in the system because he did not trust them with respect to the use they could make of the data: "They could, but they don't have access to the Google Assistant system. I could include them but haven't done it. Fear of- fear of misuse."

On the other hand, Cecilie is primarily irritated by how the smart speaker keeps confusing her voice with her husband's and therefore includes her search history in his. She recognized that, although she personally does not mind him having access to this history, it could be a problem:

> "When I ask something, it is, it comes up in some sort of search history on his phone; because it is his voice things, the Google thinks I am him, sometimes. Because, yeah, issue with my voice. When I search for something, maybe what can babies of 5 months eat, he will see that on his phone. Even when he is at work. So, it does, I don't mind, but, but it is annoying, but, yeah."

Finally, Erik states the reason why he has not purchased a security camera for his apartment, which he shares with his wife, identifying their right to privacy from each other:

> "I wouldn't like my wife being able to keep an eye on me when I'm home alone and vice versa (laughs). I don't think she will be comfortable with knowing that I was able to go on my phone and look up a video feed of her sitting on the couch looking at a movie or something."

In general, most of our informants recognized the importance of maintaining a certain level of privacy when considering their inner circle but rarely extended the same concern to tech companies or the government.

Government or National Institutions

In regard to national institutions, Norwegian citizens tend to be more trusting than other European citizens (Berg et al., 2005; Paupini, Van der Zeeuw, & Teigen, 2022; Sivesind et al., 2013); therefore, the government was not often mentioned as a source of privacy risk by our informants. When they discussed the possibility of national

authorities overseeing massive quantities of personal data, most of them did so using foreign countries as examples, implicitly or explicitly excluding the possibility of such behavior occurring in Norway.

According to Harold, who was a 74-year-old retired veterinarian, certain levels of profiling are acceptable, and access to such data by national entities is necessary to maintain security. Although he feels confidence in the balance that Norwegian institutions have struck between privacy protection and privacy surveillance, he considers different realities:

> "I am quite happy to, to have quite intrusive official intrusion into my privacy in order to protect me from hackers, from phishing, and I think that it is, I am willing to accept a fairly high degree of state, state-managed, democratically state-managed privacy surveillance. If it is going to make my life safer and the life of my grandchildren safer. But in order to do this, I have to accept the fact that certain things have to be tracked. And I am, at least in the European situation, in a Nordic, Norwegian, Nordic situation; I am quite happy. It is, it is a lot worse in other countries. If you have been to the United Kingdom, there are, there are video cameras everywhere. Absolutely everywhere. There is number plate tracking everywhere. And they have also, what they call active video cameras with loudspeakers, so the police are watching everything that you do. So, they can say to you, hey, you with the red jersey over there, stop kicking that guy, because they can see you. We don't have that yet in Norway; I hope we don't get there. But at least at the level of data access, the ability just to find out where we are, what we are doing on a certain level of, of privacy surveillance; for the meantime, I think Norway has got a very good balance between what is, what is regulated, what is not allowed, but what is potentially allowed or should be necessary. And I find that okay. I don't like it, but that is just the way the world is."

Bjørnar, 35, on the other hand, is primarily confident regarding the lack of interest that national entities have in his private life:

> "Like, potentially, you could, someone could surveil you through your phone at all times. And I mean it has been proven that countries like America, they have been actually doing that all over the world, illegally surveilling private persons, even Americans in America have been surveilled by the government, through their own phones. And they have the ability to do that with, supposedly they are not doing it now, but I do not really trust, I don't trust that governments, which really have the power to do stuff like that. I don't trust them; they are not doing it. But, like, I don't see the value for any government to be checking into me."

Moreover, he does not seem to consider that the Norwegian government or other Norwegian national entities have "the power" to effectively surveil their citizens: "No, I mean the interesting for, like anyone with the actual power to and ability to, to get in through phones and, like, like it has been proven in America, the government there has actually done those things."

His position accords with the results of other studies that highlight how Norwegians tend to have a more trusting approach toward national institutions (Berg et al., 2005; Paupini, Van der Zeeuw, & Teigen, 2022).

Unknown

This category groups expressions of unease connected to a certain level of awareness. Several informants mentioned feeling that they should be concerned about privacy and the way their data are collected and used but were not sure what could represent a source of risk in this regard or how it might become one.

Cecilie, 31, expresses this feeling in a notably clear way, explaining how she recognizes a sort of social pressure to protect her and her family's data: "Everyone seems to think we should be concerned about something is listening to us or getting information from what we are talking about, just in our home. Yeah, I think that is it."

In addition, just a few minutes later, she remarked as follows: "It just, I don't know what they want or who they are or anything."

Daniel expresses something similar, describing how he feels he should be worried about protecting his data and personal information from an unidentified source of risk:

> "I think, ehe, it sounds unethical, and I probably should worry more about protecting myself from giving away personal information that could be used by, could fall in the hands of, well if, like foreign companies or, someone with evil intentions."

A slightly distinct perspective on this issue is provided by Ivar, 81, who agreed to be interviewed because of his interest in understanding more about the risks of domestic IoT:

> "Quite, without knowledge actually, technical knowledge about the risks actually. I just have to rely upon, rely upon what I read and what I read is not very comforting, actually. So, I am very uncertain about how, where the, what are the risks actually for, for a private household to, to give data and things like that."

He has a feeling of unease related to a certain perception of the vulnerability of his home system but is unable to point out exactly what the risk is: "Well, you don't know actually where, as I understand it, there is very open system; it is very easily overlooked by companies and hackers in general."

Nonetheless, this feeling did not prevent him from using IoT devices as part of his daily routine.

Perceived Benefits

The objective for the second layer of analysis was to understand the underlying motivations and mechanisms that compelled the participants to use their IoT devices despite the aforementioned concerns, therefore balancing the scales, so to speak, when making privacy-related decisions or tipping them in favor of continuing use. The benefits category, including reflections on direct improvements IoT devices would make to the participants' lives, consists of two sections: convenience and ease of use.

Convenience

The first motivation to use domestic IoT-linked devices that many participants noted was the simplification that such devices brought to their lives. The automation of house functions, such as turning on and off lights or setting timers, was recognized as not being vital to household operation but nonetheless was sensed to be somewhat indispensable.

This way of relating to smart devices is well expressed by Anders as he reflects on how his IoT devices do not compare in importance to a washing machine or refrigerator but are still an important aspect of his domestic life:

> "It's kind of an integral part of, of daily life really. So, it's, it's not like we can do it out there. But it smooths out some of the small, small snags in everyday life by, I don't know, it's not like it's vital as a refrigerator or, or a stove or a washing machine, which you found a need in a normal household. It's not. It's not work. It's not like if it was switched off, you wouldn't function. But it's enough to... that it's easy enough to use and gives some kind of benefits, which, which, just... and also simplifies things a bit."

A similar consideration is made by Cecilie, who recalls how such simplification was precisely the reason that compelled her and her husband to buy their first IoT devices for the home:

> "Initially the reason why we got the lights, and the control was because we didn't want to get up from the bed to turn off the lights. So sometimes we just talk about it, like, "oh it is so nice to just lay in bed and turn on the lights" and turn off the lights. Yeah, lazy, but ... I don't think it has changed anything else as far as I can come, no, I don't, I don't think so."

Bjørn, in contrast, describes how having smart speakers in their rooms changed the way his family managed communications during the night:

> "For example, if my wife is preparing our daughter for bed, she is in the bathroom on the first floor, and maybe I'm up in the kitchen; then, she will speak through the Google speaker if she needs my help or something. So we're using that sometimes. You like broadcast a message so you will just talk to the Google Home in the kitchen, and the message goes to the bathroom or other way, instead of, I mean shouting."

A logical consequence of the introduction of IoT devices in households is that after the initial period of acclimation has passed, using the devices becomes natural. Anders, again, considers how it would be outlandish for him to give up the convenience his IoT devices provide:

> "So, like, you know, now at the present I've... it's, it's all natural for me to just switch on off the lights with my voice. It would, it would be strange for me to run around the house and switch on the light switches, for example. It kind of integrates, in a way."

As these devices become increasingly integrated into a household's life, concerns about privacy decrease and become less relevant in the face of the added convenience.

Ease of Use

Another topic that was often discussed is how frictionless the system tends to be once it is set up in the house. It is not just a matter of smoothing out small, everyday tasks; it is also about how easily IoT devices can be adopted by the entire family.

Erik, in particular, mentions how important it is to him that the devices in his house function well enough together so that his wife can use them:

> "I want everything to be in one just because it's easy. Also, because my wife is not that interested in technology, so with everything being in one place makes it a lot easier for her to, eh, to use the smart system."

In contrast, Anders remarks how seamless the process to set up the devices was, with step-by-step instructions and simplifications: "You can access really everything, and it's a kind of a user-friendly format as well. You get it step by step, or it's transferred into steps which are quite easy to follow."

These characteristics answer the need for an uncomplicated home life, as expressed by Daniel: "We just want things to be seamless, easy."

IoT devices respond effectively to the need for ease and seamlessness that many users understandably express, at least in terms of setting up the devices and integrating them into the household's routines. However, this ease of use often ends up presenting a stark contrast to the complex and frustrating language that these same devices use in their privacy agreements and policies and regarding how to access the privacy settings, almost forcing users to forego taking protective measures.

Justificative Arguments

The second category identified during the second layer of analysis, which aimed at understanding the motivations behind the informants' continuous use of IoT devices regardless of their privacy concerns, includes the justificative arguments they adopted. These arguments include considerations of privacy and technology that enable the participants to overlook rational reflections on privacy protection. This category has three components: inevitability, unimpeachability and indiscernibility.

Inevitability

One feeling that many informants expressed was a certain resignation that came with considering technological progress and the invasion of privacy as already ingrained in society and practically impossible to fight and therefore not worth the bother of trying to resist.

This view is well expressed by Gabriella: "But, yeah, Google pretty much knows me better than I know myself, I guess, so it is kind of hard to change or do anything about it."

Daniel, on the other hand, considers how pervasive the information market is, making it somewhat pointless to worry about domestic IoT collection of data that are already being accessed through social media:

> "Information gets around somehow anyway, I, people are, I am on Facebook, I am on Twitter and all such of things, and, and have a Google account as most people do and, whenever I search for something my information is, this is connected to my name, and advertisements are tailored for

> me in that way. And you get these ads on Facebook as well after you just mentioned something. Information is leaking all over the place."

Adding to the point just made, Bjørn reflects on the role that cellphones play in this context, especially in comparison with smart speakers. As most people already carry a microphone at all times, it is of no use to be concerned about having an additional one (or more) in the house:

> "Most of us are walking around with a camera microphone in our telephone so we have near our body at all times, so that is more or less the same as a smart speaker in those regards. We always have some kind of microphone connected to the internet near you anyway, at all times. So, I mean it would be strange to be paranoid about the smart speaker microphone if you always have your cellphone anyway."

Interestingly, the consequence of this reasoning is never to limit the chances of unintended data sharing by reducing the number of domestic IoT devices in one's house. In contrast, it is used to justify using more such devices.

Indiscernibility

One consideration that comforted the informants when debating privacy and data usage was that their data would be anonymized. For certain of them, it was reassuring that their data would be confused with data from millions of other users, especially when it came to the possibility of a single person being able to access their information.

Erik, here, comments on how he is not concerned about the use Google makes of his data because of his understanding that the data would be stored anonymously:

> "I'm just one of maaaany, many many users and... Google, they have made a pretty clear point that they don't store data which- in the way that it can be traced back to a single user. It's, eh..., it's stored anonymously. So, I will just be one out of maybe a couple of hundred thousand, maybe a million, users using Google Home. But I'm just one of many users, and it's- and all the data is anonymous, so they couldn't trace it back to me, either way. Or so I believe."

Martin, similarly, reflects on how, although he considers hackers a threat that he actively tries to avoid, he does not have the same concerns regarding the data collection smart speakers can perform:

> "Even though I care about not getting hacked. I also, I'm not, like, that worried about, like, privacy, I guess. So, like, if, if I have, like, let's say the Amazon Alexa or something, and it's not hacked, because I wouldn't like if, like, a hacker had... could listen to everything I said. But, like, if Amazon can that's, like, the criticism, right? Amazon can listen to everything I say because by its nature it has to be on all the time, right? And listen to me because it has to be triggered by me saying 'Alexa' or whatever trigger words. But also, I'm not that worried about, like, the privacy part of it."

There is perceived safety in the anonymity offered by large numbers on both ends of this interaction: the user is "one of many", and the data are collected by a faceless entity that is singular in the home but plural in the way it functions. It is Alexa but also no one in particular.

Unimpeachability

When asked about their feelings regarding surveillance and the possibility of their data being collected or used by tech companies or national institutions, most of the participants expressed the conviction that they had nothing of interest to say that would justify such surveillance and that therefore it would be unlikely to occur.

Bjørn, for example, comments on how his family does not have secrets: "I don't think they would find it very interesting (little laughter). We don't have any secrets."

Erik does not consider himself interesting enough to justify personalized attention: "I don't think it would be of any interest attacking me personally. For some- I- I can't imagine that."

Daniel, on the other hand, mentions how there would be no point in surveilling his family since they do not normally talk about controversial topics or have conversations about revolution: "It shouldn't because I think we don't say too much radical stuff. So, I am never worried about it."

His wife, Cecilie, commented that the things she says at home would not be interesting to a third party and that she does not consider the possibility of these things being used in any way:

> "I am not afraid that anything I say at home could be used in any way because it is not interesting. And, yeah, I don't know, I haven't thought about it so much. And I don't know what things they could hear from us that would be used in any way or, yeah, I don't know."

Kristin concludes as follows: "I think I have got the privacy I need. I am not a freak; I am on the other scale of (little laughter), of that."

Discussion

This study sought to better understand why users of domestic IoT-connected devices continue to use such devices despite perceiving their privacy risks. To this end, we adopted a qualitative approach to develop a conceptualization of privacy calculus that captures how users interpret risks, justify continued use, and assess their own understanding of privacy. The study demonstrates that perceived risks in the context of domestic IoT privacy protection are often the result of illusion of understanding, with users basing their cost-outcome evaluation on inaccurate information (Hoffmann et al., 2016). This mechanism is particularly evident when the informants' loyalty to certain tech companies is considered because, in the informants' opinion, at such companies, no data harvesting is involved beyond transparent internal use. Our study shows that objective knowledge of privacy protection and data sharing is not relevant to the user's risk assessment as long as the user retains the illusion of understanding the topic at hand.

We contribute to the privacy literature by proposing a contemporary model for understanding the mechanisms underlying such privacy risk evaluation that considers the complexity of the domestic IoT environment while recognizing the role played by the illusion of understanding. Our Scales of Privacy model, therefore, demonstrates how the perceived privacy risks are weighted against the perceived benefits of adopting a domestic IoT device in the household (Figure 2). Furthermore, we identified justificative arguments, such as privacy cynicism and perceived anonymity, that neutralize the weight of perceived risk on the scales and explain the continued usage of domestic IoT devices.

Norway represents an interesting case for studies on the domestic Internet of Things because of its well-developed digital infrastructure and the wide diffusion of high digital competence and skill among its population compared with other European countries (Langseth & Haddara, 2021). In this environment, there is a generalized political drive to include digital and technological tools and solutions in addressing societal issues (Gøthesen et al., 2023), and domestic technologies and smart home applications have spread relatively quickly (Slettemeås, 2019). In a country with this degree of receptivity toward technological development, our study reveals that consumers approach the matter of privacy protection in different ways. On the one hand, potential vulnerabilities are often recognized, with a particular focus on the actors that could gain access to private information (i.e., family or partner, national institutions, tech companies, and hackers) according to a personal system of values. On the other hand, regardless of the level of concern, various mechanisms appear to prevent users from taking definite action to protect their privacy or from acting in a manner consistent with their stated beliefs. This makes the Norwegian context particularly relevant to our study, as it illustrates how recognition of privacy risks can coexist with continued device use, supporting our argument that privacy-related decision-making in domestic IoT use cannot be reduced to a straightforward cost–benefit trade-off.

The Scales of Privacy: Perceived Risk, Justifications and Perceived Benefits

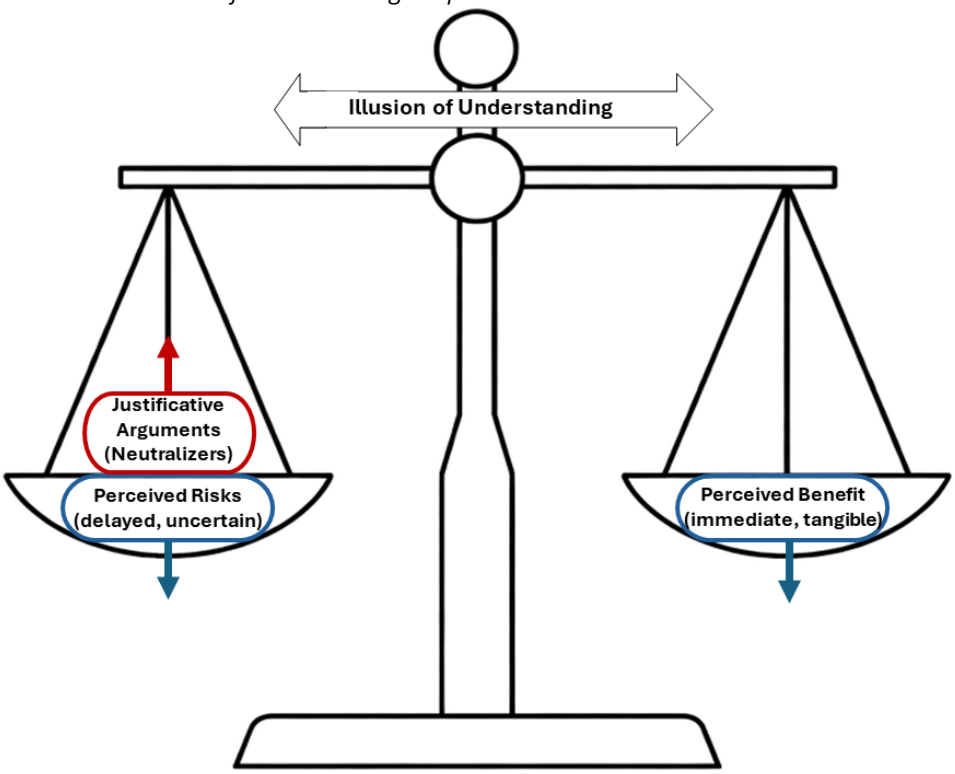
According to Laufer and Wolfe's privacy calculus concept, decisions on data disclosure are based on a type of cost–benefit/risk–benefit analysis; therefore, in certain ways, personal information can be understood as being traded as an economic commodity (Laufer & Wolfe, 1977). Although we consider the recent critiques of this model (Fernandes & Pereira, 2021; D. Kim et al., 2019; M. Kim & Choi, 2022) justified and helpful in contextualizing this concept in the current digital age, we find that an additional limitation should be highlighted. Building on D. Kim et al. (2019) research, we consider that the reasons why "the willingness to trade personal information is not meaningfully impacted by the users' perception of risk" (D. Kim et al., 2019) are a combination of the following: First, the lack of proper understanding of the consequences and risks of sharing personal data; second, the complexity of privacy agreements, which make it nearly impossible for an untrained person to fully understand

the terms of common privacy agreements. In a landscape that is designed to render a proper understanding of the "trade" effectively hopeless, performing a legitimate cost–benefit/risk–benefit analysis is impossible.

Rather than applying a fully informed cost–benefit analysis, we observe that participants engage in a subjective and biased form of privacy calculus. We conceptualize this process through the *Scales of Privacy model* (Figure 2), which consists of four analytically distinct but interrelated elements: the illusion of understanding, perceived benefits, perceived risks, and justificative arguments (i.e., neutralizers). First, our interview participants often displayed an *illusion of understanding*, that is a tendency to overestimate their knowledge of what data were collected, shared, and stored. The opacity of privacy agreements appeared to foster the impression that participants understood the implications for privacy of their use of the domestic IoT, even when that understanding was only partial.

On the basis of this perceived understanding, participants engaged in a form of privacy calculus in which the *perceived benefits* of domestic IoT use, most notably convenience, comfort, and ease of use, were weighed against what they saw as potential privacy risks (Figure 2). Moreover, this calculus was not neutral. Participants frequently emphasized that the benefits of IoT devices were immediate, tangible, and embedded in everyday life, whereas the perceived risks were typically perceived as distant, abstract, or uncertain. In this sense, the benefit was experienced in the present, while the risk remained remote.

Figure 2. *Scales of Privacy Model. Perceived Benefits Are Weighed Against Perceived Privacy Risks, Whereas Justificatory Arguments Reduce the Weight of Risks, and the Illusion of Understanding Shapes how Those Risks Are Perceived.*



In addition, our study identified a set of *justificatory arguments*, or *neutralizers*, that reduced the weight of perceived risks without constituting benefits in themselves. These neutralizers acted as counterbalances in participants' reasoning and helped explain why privacy concerns did not necessarily translate into privacy-protective behavior. One such justificatory argument, or neutralizer, was privacy cynicism (Hoffmann et al., 2016), which our interviewees expressed as resignation, mistrust, or the belief that privacy protection is ultimately futile in a world characterized by pervasive tracking, surveillance, and targeted advertising. Several participants described information sharing as an inevitable aspect of contemporary digital life and therefore not worth resisting.

A second *neutralizer* combined what we identified in the analysis as indiscernibility and unimpeachability. Here, participants downplayed privacy concerns by implying either that their data would not be particularly noticeable or valuable to others or that they themselves had done nothing that would justify concern. In the Norwegian context, such responses may also be interpreted in light of cultural norms related to *likhet* and *Janteloven*, which

emphasize social uniformity and may discourage individuals from viewing themselves as exceptional or especially exposed (Avant & Knutsen, 1993; Başak, 2021; Gullestad, 2002).

There are safety and reassurance in the sense of anonymity given by big numbers, as several participants in the study have highlighted by describing themselves as just "one of many users". However, multiple informants expressed a variation of this sense of comfort in anonymity that comes from not having anything to hide or not being interesting because they have no secrets. Notably, this argument represents an evolution of Nissenbaum's contextual integrity model (Nissenbaum, 2004, 2011), as the reasonable expectation of privacy given a certain context has gradually shifted over the years: the "nothing to hide" argument expresses the expectation of *not* having privacy in the context of a connected household, and this violation of privacy becomes acceptable because of the lack of secrets being discussed. Another evolution of this reflection comes with feeling safe in the information shared because nothing "radical" is being said. Our interviewees often expressed a sentiment similar to not seeing "the value for any government to be checking" on them. As a consequence, the perceived risks weigh less on the privacy scales because of the perceived "innocence" of the household. The dangerous implication of such considerations is that surveillance can be warranted in cases in which consumers have "secrets" or are behaving inconveniently or in which the institutions and government consider the infringement valuable for some reason. In fact, having "something to hide", whatever that may mean, or not conforming to societal norms might justify the loss of the right to privacy. The more a society encourages conformity, the more "something to hide", "something radical" and "something interesting" could end up coinciding with simply "something different", perhaps in disagreement with the status quo.

The internet has been and continues to be a central medium for activism and the expression of dissent that, following this logic, may well be considered reason enough to revoke privacy rights. Related to this issue, D'Acunto et al. (2022) investigated the influence of surveillance on individual behavior, concluding that it can exacerbate conformity with societal norms and heighten intolerance toward deviations from them (D'Acunto et al., 2022). In certain ways, it seems that the more pervasive surveillance and privacy infringement are, the more justifiable they become. Or, as our interviewee Kristin concluded, "I think I have got the privacy I need; I am not a freak."

Limitations and Suggestions for Future Research

Although our study was conducted with stringent care and provides relevant insights, some limitations can be identified. First, owing to circumstances of the fieldwork, the study was based on a relatively small group of 12 participants across 10 Norwegian households. While qualitative research does not necessarily aim for statistical generalizability, the small sample size and context-specific nature of the data limit the transferability of our findings to other populations or cultural settings. As Maxwell (2013) notes, qualitative inquiry is context-dependent and better suited to exploring processes and meanings rather than making general claims (Maxwell, 2013). Furthermore, we acknowledge the peculiarity of the Norwegian digital development context compared with that of other European countries. Future studies should consider cross-validating our Scales of Privacy model in different digital landscapes.

Second, we did not investigate differences in privacy conceptions between the person who purchased the IoT device and other household members (although in certain cases, we interviewed both individuals) as this would have transcended the scope of this article. Household members who did not initiate the purchase of IoT devices may experience increased privacy concerns since they were not part of implementing the devices and often express less confidence in their understanding of technology. Therefore, future research on this topic could include investigating the issue of consent and delegation in the smart home environment, as well as exploring how the younger members of the household, i.e., teenagers and younger, interact with such devices in regard to data sharing and privacy protection. In houses in which the roles regarding the handling of domestic IoT devices tend to be well established, with one member making the important decisions on privacy protection on behalf of the rest of the household, exploring the dynamics and understanding of this boundary could offer insightful perspectives on an issue that is all the more pressing in our time, especially by also investigating the role that gender dynamics play in this regard. Additionally, the role that IoT devices play in the daily routines of the users should be investigated, especially in relation to how such devices are used by the different members of the household. Future research on this topic could seek to shed light on the way privacy risk perception and confidence levels in the use of technology influence dynamics within the household and on the styles of IoT device management.

Finally, the illusion of understanding and its underlying mechanisms in the IoT context should be further investigated, especially considering the limited number of participants in this study. As per the nature of semi structured interviews, this theme emerged from the spontaneous contributions of the participants more than from preset questions. Future research could further investigate this theme's implications both quantitatively and qualitatively. For example, a quantitative approach could monitor access to terms and conditions when new devices are set up, providing insights into which sources of risk the participants perceive. Additionally, qualitative interviews would be relevant in assessing according to which information users construct their perceptions of risk.

Conclusions

Because of its advanced digital infrastructure and the high level of digital literacy among its population, Norway represents a remarkable case for studying the domestic Internet of Things (IoT). These factors, in addition to the country's political emphasis on using technology to address societal issues, have contributed to the rapid adoption of smart home applications among private consumers. In regard to privacy risks, our informants identified five possible risk sources, which were mostly based on personal values: government or national institutions, technological companies, hackers, and partners or family members. When the reasons why such considerations on privacy would not hinder their use of domestic IoT devices were investigated, five underlying motivations were identified, of which two were intrinsically related to the frictionless user experience provided by the devices (i.e., convenience and ease of use). The remaining three (i.e., inevitability, unimpeachability and indiscernibility) revealed attitudes toward privacy protection partially influenced by a sense of being overwhelmed given by the friction-*filled* experience of navigating setting boundaries around personal data in the current digital environment. On the basis of the results of this study, we developed a new model of the privacy calculus to represent the cost–benefit analysis underlying privacy decisions in the context of the current digital landscape. Our Scales of Privacy model provides a holistic view of the process underlying the privacy calculus, incorporating both the perceived risks and the perceived benefits of data disclosure and including neutralizing factors such as privacy cynicism and "nothing to hide" arguments that lighten the weight of the perceived risk on the scales.

Conflict of Interest

The authors have no conflicts of interest to declare.

Use of AI Services

The authors declare they have not used any AI services to generate any part of the manuscript or data.

Data Availability Statement

All the raw data from this project will be deleted at the end of the RELINK project, in June 2025.

Authors' Contribution

Cristina Paupini: conceptualization, data curation, formal analysis, investigation, methodology, project administration, validation, visualization, writing—original draft, writing—review & editing. **Dominique Kost:** conceptualization, formal analysis, methodology, supervision, validation, writing—original draft, writing—review & editing. **Terje Gjøsæter:** conceptualization, data curation, methodology, project administration, supervision, validation, writing—original draft, writing—review & editing.

Acknowledgement

This paper is based on research performed within the RELINK - Relinking the "weak link". Building resilient digital households through interdisciplinary and multilevel exploration and intervention project, funded by the Research Council of Norway, IKTPluss, grant no. 288663, and headed by Consumption Research Norway (SIFO) and Oslo Metropolitan University (OsloMet).

References

Adorjan, M., & Ricciardelli, R. (2019). A new privacy paradox? Youth agentic practices of privacy management despite "nothing to hide" online. *Canadian Review of Sociology/Revue Canadienne De Sociologie*, *56*(1), 8–29. https://doi.org/10.1111/cars.12227

Al Muhander, B., Arachchilage, N., Majib, Y., Alosaimi, M., Rana, O., & Perera, C. (2025). PrivacyCube: Data physicalization for enhancing privacy awareness in IoT. *ACM Transactions on Internet of Things*, *6*(2), 1–35. https://doi.org/10.1145/3722232

Al-Suhimat, R. I., Ibrahim, A., Maaitah, N. O., & Al-Dmour, N. A. (2024). Review of Security Challenges Encountered in Internet of Things Technology. In *2024 IEEE 2nd International Conference on Cyber Resilience (ICCR)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICCR61006.2024.10533052

Angrishi, K. (2017). *Turning Internet of Things (IoT) into internet of vulnerabilities (iov): Iot botnets.* arXiv. https://doi.org/10.48550/arXiv.1702.03681

Avant, G. R., & Knutsen, K. P. (1993). Understanding cultural differences: Janteloven and social conformity in Norway. *ETC: A review of general semantics*, *50*(4), 449–460. https://www.jstor.org/stable/42577494

Başak, R. (2021). Janteloven: Scandinavian social conformity, IKEA, minimalism, and the socialism of design. *ARTS: Artuklu Sanat ve Beşerî Bilimler Dergisi*, *6*, 159–185. https://doi.org/10.46372/arts.909874

Berg, L., Kjaernes, U., Ganskau, E., Minina, V., Voltchkova, L., Halkier, B., & Holm, L. (2005). Trust in food safety in Russia, Denmark and Norway. *European Societies*, *7*(1), 103–129. https://doi.org/10.1080/1461669042000327045

Buntak, K., Brlek, P., & Cesarec, B. (2021). The impact of the Internet of Things and artificial intelligence on the supply chain. *Business Logistics in Modern Management*, *21*, 369–383. https://ideas.repec.org/a/osi/bulimm/v21y2021p369-383.html

Chandra, Y., & Shang, L. (2019). Inductive coding. In *Qualitative research using R: A systematic approach* (pp. 91–106). Springer. https://doi.org/10.1007/978-981-13-3170-1_8

Chen, H.-T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist*, *62*(10), 1392–1412. https://doi.org/10.1177/0002764218792691

Cloarec, J., Meyer-Waarden, L., & Munzel, A. (2024). Transformative privacy calculus: Conceptualizing the personalization-privacy paradox on social media. *Psychology & Marketing*, *41*(7), 1574–1596. https://doi.org/10.1002/mar.21998

Collier, G. (1995). Information privacy. *Information Management & Computer Security*, *3*(1), 41–45. https://doi.org/10.1108/09685229510792979

Coughlan, T., Leder Mackley, K., Brown, M., Martindale, S., Schlögl, S., Mallaband, B., Arnott, J., Hoonhout, J., Szostak, D., & Brewer, R. (2013). Current issues and future directions in methods for studying technology in the home. *PsychNology Journal*, *11*(2), 159–184. https://www.psychnology.org/index_page-abstract---volume-11---caughlan.html

Crenshaw, K. (1989). Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *The University of Chicago Legal Forum*, *1989*(1), Article 8. http://chicagounbound.uchicago.edu/uclf/vol1989/iss1/8

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

D'Acunto, F., Schnorpfeil, P., & Weber, M. (2022). Big Brother watches you (even when he's dead): Surveillance and long-run conformity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4097692

de Ridder, J. (2024). Online illusions of understanding. *Social Epistemology*, *38*(6), 727–742. https://doi.org/10.1080/02691728.2022.2151331

Deloitte, U. (2016). *Global mobile consumer survey: US edition*. Deloitte US.

Dienlin, T., Masur, P. K., & Trepte, S. (2023). A longitudinal analysis of the privacy paradox. *New Media & Society*, *25*(5), 1043–1064. https://doi.org/10.1177/14614448211016316

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Fei, W., Ohno, H., & Sampalli, S. (2023). A systematic review of IoT security: Research potential, challenges, and future directions. *Association for Computing Machinery Computing Surveys*, *56*(5), Article 111. https://doi.org/10.1145/3625094

Fernandes, T., & Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? *Telematics and Informatics*, *65*, Article 101717. https://doi.org/10.1016/j.tele.2021.101717

Ferrara, P., & Spoto, F. (2018). Static analysis for GDPR compliance. In *Proceedings of the Second Italian Conference on Cyber Security (ITASEC 2018)* (Vol. 2058, Article 10). CEUR-WS. https://ceur-ws.org/Vol-2058/paper-10.pdf

Fisher, M., Goddu, M. K., & Keil, F. C. (2015). Searching for explanations: How the Internet inflates estimates of internal knowledge. *Journal of Experimental Psychology: General*, *144*(3), 674–687. https://doi.org/10.1037/xge0000070

Fox, G. (2020). "To protect my health or to protect my health privacy?" A mixed-methods investigation of the privacy paradox. *Journal of the Association for Information Science and Technology*, *71*(9), 1015–1029. https://doi.org/10.1002/asi.24369

Fuglerud, K. S. (2011). The barriers to and benefits of use of ICT for people with visual impairment. In C. Stephanidis (Ed.), *Universal Access in Human-Computer Interaction* (pp. 452–462). Springer. https://doi.org/10.1007/978-3-642-21672-5_49

Gøthesen, S., Haddara, M., & Kumar, K. N. (2023). Empowering homes with intelligence: An investigation of smart home technology adoption and usage. *Internet of Things*, *24*, Article 100944. https://doi.org/10.1016/j.iot.2023.100944

Gullestad, M. (2002). Invisible fences: Egalitarianism, nationalism and racism. *Journal of the Royal Anthropological Institute*, *8*(1), 45–63. https://doi.org/10.1111/1467-9655.00098

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757. https://ijoc.org/index.php/ijoc/article/view/4655/1738

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access*, *7*, 82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4), Article 7. https://doi.org/10.5817/CP2016-4-7

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2024). Inequalities in privacy cynicism: An intersectional analysis of agency constraints. *Big Data & Society*, *11*(1). https://doi.org/10.1177/20539517241232629

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1589864

Internet Society, & Consumers International. (2019). *The trust opportunity: Exploring consumer attitudes to the Internet of Things*. Internet Society. https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/

Jillson, E. (2023, June 13). *Hey Alexa! What are you doing with my data?* Federal Trade Commission. https://www.ftc.gov/business-guidance/blog/2023/06/hey-alexa-what-are-you-doing-my-data?

John, L. K. (2015). The consumer psychology of online privacy: Insights and opportunities from behavioral decision theory. In M. I. Norton, D. D. Rucker, & C. Lamberton (Eds.), *The Cambridge handbook of consumer psychology* (pp. 619–646). Cambridge University Press. https://doi.org/10.1017/CBO9781107706552.023

Kehr, F., Wentzel, D., Kowatsch, T., & Fleisch, E. (2015). Rethinking privacy decisions: Pre-existing attitudes, pre-existing emotional states, and a situational privacy calculus. In *ECIS 2015 Completed Research Papers* (Article 95). https://doi.org/10.18151/7217379

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(1), Article 2. https://doi.org/10.5817/CP2016-1-2

Kim, D., Park, K., Park, Y., & Ahn, J.-H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273–281. https://doi.org/10.1016/j.chb.2018.11.022

Kim, M., & Choi, B. R. (2022). The impact of privacy control on users' intention to use smart home Internet of Things (IoT) services. *Asia Marketing Journal*, *24*(1), Article 4. https://doi.org/10.53728/2765-6500.1586

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

Korneeva, E., Olinder, N., & Strielkowski, W. (2021). Consumer attitudes to the smart home technologies and the Internet of Things (IoT). *Energies*, *14*(23), Article 7913. https://www.mdpi.com/1996-1073/14/23/7913

Kumar, S. M. (2025). The Potential Consequences of a Data Breach in Big Data Systems with Compromised Cyber Security and Privacy. In *2025 IEEE 17th International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 1072–1076). IEEE. https://doi.org/10.1109/CICN67655.2025.11368157

Langseth, M., & Haddara, M. (2021). Exploring data analytics adoption in public procurement: The case of Norway. In M. Langseth & J. O. Similä (Eds.), *Å kjøpe for Norge* (pp. 223–256). Cappelen Damm Akademisk. https://doi.org/10.23865/noasp.128.ch9

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-computer Interaction*, *2*(CSCW), Article 102. https://doi.org/10.1145/3274371

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Lee, A.-R. (2021). Investigating the personalization–privacy paradox in Internet of Things (IoT) based on dual-factor theory: Moderating effects of type of IoT service and user value. *Sustainability*, *13*(19), Article 10679. https://doi.org/10.3390/su131910679

Lutz, C., & Newlands, G. (2021). Privacy and smart speakers: A multi-dimensional approach. *The Information Society*, *37*(3), 147–162. https://doi.org/10.1080/01972243.2021.1897914

Magara, T., & Zhou, Y. (2024a). Internet of Things (IoT) of smart homes: privacy and security. *Journal of Electrical and Computer Engineering*, *2024*(1), Article 7716956. https://doi.org/10.1155/2024/7716956

Magara, T., & Zhou, Y. (2024b). Security and privacy concerns in the adoption of IoT smart homes: A user-centric analysis. *American Journal of Information Science and Technology*, *8*(1), 1–14. https://doi.org/10.11648/j.ajist.20240801.11

Marshall, M. N. (1999). Improving quality in general practice: Qualitative case study of barriers faced by health authorities. *BMJ*, *319*(7203), 164–167. https://doi.org/10.1136/bmj.319.7203.164

Marwick, A., & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*, *22*(12), 1697–1713. https://doi.org/10.1080/1369118X.2018.1450432

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, *8*(2), 258–269. https://doi.org/10.17645/mac.v8i2.2855

Masur, P. K. (2023). Understanding the effects of conceptual and analytical choices on 'finding' the privacy paradox: A specification curve analysis of large-scale survey data. *Information, Communication & Society*, *26*(3), 584–602. https://doi.org/10.1080/1369118X.2021.1963460

Maxwell, J. A. (2013). *Qualitative research design: An interactive approach* (3rd ed.). SAGE Publications.

McLean, G., & Osei-Frimpong, K. (2019). Hey Alexa… examine the variables influencing the use of artificial intelligent in-home voice assistants. *Computers in Human Behavior*, *99*, 28–37. https://doi.org/10.1016/j.chb.2019.05.009

Nemmaoui, S., Baslam, M., & Bouikhalene, B. (2023). Privacy conditions changes' effects on users' choices and service providers' incomes. *International Journal of Information Management Data Insights*, *3*(1), Article 100173. https://doi.org/10.1016/j.jjimei.2023.100173

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–158. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48. https://doi.org/10.1162/DAED_a_00113

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Ostinelli, M., Bonezzi, A., & Lisjak, M. (2024). Unintended effects of algorithmic transparency: The mere prospect of an explanation can foster the illusion of understanding how an algorithm works. *Journal of Consumer Psychology, 35*(2), 203–219. https://doi.org/10.1002/jcpy.1416

Paupini, C., Teigen, H. F., & Habib, L. (2022). A change of space: Implications of digital fieldwork in connected homes during the COVID-19 pandemic. *Digital Creativity*, *33*(3), 204–218. https://doi.org/10.1080/14626268.2022.2130943

Paupini, C., Van der Zeeuw, A., & Teigen, H. F. (2022). Trust in the institution and privacy management of Internet of Things devices. A comparative case study of Dutch and Norwegian households. *Technology in Society*, *70*, Article 102026. https://doi.org/10.1016/j.techsoc.2022.102026

Pink, S., Mackley, K. L., Moroşanu, R., Mitchell, V., & Bhamra, T. (2017). *Making homes: Ethnography and design*. Routledge.

Princi, E., & Krämer, N. C. (2019). Acceptance of smart electronic monitoring at work as a result of a privacy calculus decision. *Informatics*, *6*(3), Article 40. https://doi.org/10.3390/informatics6030040

Princi, E., & Krämer, N. C. (2020). Out of control–privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices. *Frontiers in Psychology*, *11*, Article 582054. https://doi.org/10.3389/fpsyg.2020.582054

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1). https://doi.org/10.5210/fm.v15i1.2775

Saka, S., & Das, S. (2025). SoK: Reviewing two decades of security, privacy, accessibility, and usability studies on Internet of Things for older adults. In *2016 International Conference on Industrial Informatics - Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII)* (pp. 98–115). Association for Computing Machinery. https://dl.acm.org/doi/10.1145/3779208.3785270

Schomakers, E.-M., Lidynia, C., & Ziefle, M. (2022). The role of privacy in the acceptance of smart technologies: Applying the privacy calculus to technology acceptance. *International Journal of Human–Computer Interaction*, *38*(13), 1276–1289. https://doi.org/10.1080/10447318.2021.1994211

Shakya, S., Abbas, R., & Maric, S. (2025). *A novel zero-touch, zero-trust, AI/ML enablement framework for IoT network security.* arXiv. *https://doi.org/10.48550/arXiv.2502.03614*

Sinha, S. (2025, October 28). *State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally.* IoT Analytics GmbH. https://web.archive.org/web/20251029083039/https://iot-analytics.com/number-connected-iot-devices/

Sivesind, K. H., Pospíšilová, T., & Frič, P. (2013). DOES VOLUNTEERING CAUSE TRUST?: A comparison of the Czech Republic and Norway. *European Societies*, *15*(1), 106–130. https://doi.org/10.1080/14616696.2012.750732

Slettemeås, D. (2019). *Smart technologies in connected homes–A 2019 Norwegian consumer survey.* Consumption Research Norway (SIFO), Oslo Metropolitan University. https://uni.oslomet.no/relink/wp-content/uploads/sites/193/2019/06/Relink-Preliminary-Survey-Results-on-Home-IoT.pdf

Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review*, *44*(289), 745–772. https://ssrn.com/abstract=998565

Stuart, A., & Levine, M. (2017). Beyond 'nothing to hide': When identity is key to privacy threat under surveillance. *European Journal of Social Psychology*, *47*(6), 694–707. https://doi.org/10.1002/ejsp.2270

Tau, B. (2023, May 18). *Antiabortion group used cellphone data to target ads to planned parenthood visitors.* The Wall Street Journal. https://www.wsj.com/us-news/society/antiabortion-group-used-cellphone-data-to-target-ads-to-planned-parenthood-visitors-446c1212

Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation, 27*(2), 237–246. https://doi.org/10.1177/1098214005283748

Ward, A. F. (2013). Supernormal: How the Internet is changing our memories and our minds. *Psychological Inquiry*, *24*(4), 341–348. https://doi.org/10.1080/1047840X.2013.850148

Xi, W., & Ling, L. (2016). Research on IoT privacy security risks. In *2016 International Conference on Industrial Informatics-Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII)* (pp. 259–262). IEEE. https://doi.org/10.1109/ICIICII.2016.0069

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

About Authors

Dr. Cristina Paupini is a graduate from the Roma Tre University of Rome with a MA in Education and a thesis in Inclusive education. Her current research focuses on the risks related to Internet of Things in the context of the household and from a Universal Design's perspective. She is a PhD fellow at the department of Computer Science and the Oslo Metropolitan University, where she teaches ethics within the realm of technology use and design to bachelor students.

https://orcid.org/0000-0003-4139-6331

Dr. Dominique Kost is an Associate Professor at the Department of Leadership and Organizational Behaviour at the Norwegian Business School (BI) and holds a PhD in organizational psychology from BI Norwegian Business School. Dr. Kost's research has been published in top-tier academic journals such as Human Resource Management Journal, Journal of Occupational and Organizational Psychology, and Computers in Human Behavior. Her research focuses on telework and home office, relationships among employees, communication processes in virtual teams, and digital labour.

https://orcid.org/0000-0002-8084-5833

Dr. Terje Gjøsæter is an Associate Professor at the Department of Information Systems (IS) at the University of Agder and is an active member of their cross-disciplinary Centre for Integrated Emergency Management (CIEM). His current research focus is divided between Universal Design of ICT for Emergency Management and Cybersecurity. He completed his PhD at University of Agder in 2015, on design principles and usability of meta-modelling tools. His research interests include such diverse topics as universal design and accessibility, cyber-security, usable security, privacy, computer language theory and metamodeling. He has published over 50 peer-reviewed articles and conference papers across these topics.

https://orcid.org/0000-0002-1688-7377

Correspondence to
Cristina Paupini, Department of Computer Science, Oslo Metropolitan University, Pilestredet 46, 0167, Oslo, Norway, cristina.paupini@protonmail.com