Dr. Convenience Love or: How I Learned to Stop Worrying and Love my Voice Assistant*

Sujay Shalawadi
sujaybs@cs.aau.dk
Aalborg University
Aalborg, Denmark

Florian Echtler
floech@cs.aau.dk
Aalborg University
Aalborg, Denmark

Dimitrios Raptis
raptis@cs.aau.dk
Aalborg University
Aalborg, Denmark

ABSTRACT

This paper explores the relationship between privacy concerns from voice assistant (VA) users and their persistent dependence on these devices for convenience. To gain a deeper understanding, we investigated using two studies. In the first study, we conducted semi-structured interviews with 13 participants, applying the lens of system justification theory. This approach enabled us to discover the cognitive and psychological mechanisms that people use when rationalizing and justifying their privacy versus convenience trade-off when using a VA. In the second study, we deployed VoxMox, a provotype, in three households. Our objective was to prompt participants to reflect more deeply on their privacy rationalizations and justifications, potentially motivating them to take action. Overall, our findings from both studies revealed several instances of apathetic attitudes toward privacy. We discuss privacy apathy in relation to the existing literature and offer research and design implications for breaking these attitudes in future studies.

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in HCI**.

KEYWORDS

voice assistants, privacy, apathy, provotype, self-cringe, system justification theory

ACM Reference Format:
Sujay Shalawadi, Florian Echtler, and Dimitrios Raptis. 2024. Dr. Convenience Love or: How I Learned to Stop Worrying and Love my Voice Assistant. In *Nordic Conference on Human-Computer Interaction (NordiCHI 2024), October 13–16, 2024, Uppsala, Sweden.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3679318.3685364

1 INTRODUCTION

Voice assistants (VAs) such as Amazon Alexa, Google Home, and Apple Siri, have been integrated into millions of homes, transforming the way people perform everyday tasks. They offer convenience by enabling users to easily control devices, access information, and perform tasks using voice commands. However, incorporating VAs into everyday life also raises privacy concerns, as they need to constantly monitor the home environment to operate properly. This presents householders with the challenge of how to effectively manage their privacy.

People often complain about the data practices of VAs, yet they do not necessarily refrain from using such devices [59, 60]. This discrepancy between attitude and actual behavior complicates research- and design-based attempts to help people manage privacy of contemporary technology. This attitude-behavior discrepancy is also central to the well-known phenomenon of the *privacy paradox*. The privacy paradox is often referred to as a phenomenon in which people say they value privacy, but act in contradictory ways. As the privacy paradox appeared in several privacy studies, some have even argued that the observed discrepancy may not be paradoxical at all [59, 60, 69].

Some researchers explain the privacy paradox through a commodity-based perspective, where users engage in a *privacy calculus*, weighing benefits against risks [29]. Other possible explanations include contextual inconsistency [53], ambiguity and lack of control [64] and therefore it has remained a fundamental concept in privacy research for decades. Common approaches, such as privacy calculus, rely on people's rational assessments of benefits and trade-offs when disclosing private information. These approaches attribute the privacy paradox to rational risk assessment in privacy-related behavior. However, a recent review highlights that the paradox arises from extrapolating findings across specific situations and general attitudes [69].

Given the extensive use of the privacy paradox as an analytical lens in studying privacy in various contemporary technology contexts, we aim to explore whether the paradox extends beyond rational trade-offs between convenience and privacy within smart home settings. We contend that strict adherence to rationality in analyzing the paradox within the context of VAs may be limiting, overlooking nuanced influences and broader social dynamics. By considering both rationalizations and deeper justifications, we seek a more comprehensive understanding of the privacy paradox between users and VAs that are deeply integrated into their daily lives due to the variety of essential conveniences they tend to offer in exchange for personal data. Furthermore, we believe that examining the paradox beyond scenarios focused solely on the willingness of users to disclose information, and exploring householders' perspectives after prolonged use of VAs can help to better understand it [41].

Our approach to unpacking the privacy paradox involves two studies. We first conducted semi-structured interviews with 13 VA owners, using system justification theory (SJT) [33, 42, 78] as an analytical lens. This study explored the psychological and social

*Paper title is clearly inspired by Stanley Kubrick's movie "Dr. Strangelove": https://www.imdb.com/title/tt0057012/

NordiCHI 2024, October 13–16, 2024, Uppsala, Sweden

ACM ISBN 979-8-4007-0966-1/24/10
https://doi.org/10.1145/3679318.3685364

mechanisms that influence people's privacy decisions. The findings of this study revealed instances of rationalization and justification of the privacy paradox discourse that were intertwined with emotional responses. We then applied these findings in the second study, where we developed VoxMox, a physical provotype (*provo*cative proto*type*) [11] that targets rationalized and justified discourses to further provoke reflections upon the privacy paradox. The results of the field study and interviews with three households using VoxMox indicate apathetic behavior toward privacy decisions and similar usage patterns to their own VAs.

Our study contributes to the privacy paradox discourse in two significant ways. Firstly, we utilize system justification theory [33] to uncover the psychological mechanisms behind individuals' rationalization of privacy versus convenience trade-offs. Additionally, we introduce VoxMox, a technology probe aimed at prompting deeper reflections on privacy and convenience considerations. Secondly, by synthesizing findings from both studies, we explore the prevalent attitude of apathy towards privacy actions, situating it within existing literature. Lastly, we provide implications for future studies aimed at addressing and mitigating privacy apathy. In the subsequent sections, we outline related work, detail the procedures of the two studies, present their respective findings, and conclude by discussing privacy apathy among VA users, linking various instances of apathetic behavior to our study findings.

2 RELATED WORK

VAs like Amazon Echo (Alexa), Google Home, or Apple's Siri present a trade-off between convenience and privacy. While these assistants offer easy voice-activated controls for home devices and services, they function by continuously monitoring audio data for efficient response. This data collection by third-party tech companies raises concerns about misuse and unauthorized access [90]. Despite concerns, users often use these assistants for their perceived benefits. This study builds on previous research on user experience, privacy self-management, and privacy control mechanisms to examine user dynamics with VAs, particularly with regard to audio data management.

2.1 User experiences with Voice Assistants

Several studies [28, 39, 46, 86, 88] have investigated smart homes, interviewing household members to determine directions for future research on smart home privacy. Broadly speaking, these investigations reveal that smart homes, like traditional homes, accommodate a wide range of primary and secondary users. These users have varying expectations about the conveniences offered by smart home devices [2, 36, 39], different skill levels in using these devices [28, 39], and different privacy expectations [76]. Studies have identified privacy concerns in the context of VAs that extend beyond just primary users, the individuals directly interacting with the technology. They also encompass secondary users, individuals who may be inadvertently affected by the primary user's interactions with the device. Baumer more generally refers to this category as usees, "individuals who neither are clearly users of a system nor are clearly non-users" [8]. As VAs have become integrated into our daily lives, the potential sharing of personal information, unintentional activation, and the exposure of sensitive data to unintentional listeners raise complex privacy considerations [21, 25].

Chalhoub et al. [14] through their longitudinal analysis found that VA users often repurpose their devices from planned use, resulting primarily in loss of control and eventual frustrations. Lau et al. [40], found that users who installed smart speakers in their homes were often more aware of privacy settings than other members of the household. Ur et al. [76], found differences in privacy expectations between adolescents and their parents [87], and Mare et al. [44, 45] found a similar misalignment between AirBnb hosts and their guests. Some studies investigated multi-user smart home scenarios identifying a frequent presence of a lead user or a 'driver' in smart households [28, 39]. These drivers acted as a sort of system administrator for their home, taking more responsibility for the acquisition, installation, and control of devices at home. Geeng et al. [28] also identified in their longitudinal analysis that these drivers were primarily men who frequently had female partners as secondary users. Beyond identifying different types of smart home users, several studies have simultaneously identified privacy violations experienced by both types of users. Primary users wrestle with the trade-off between convenience and potential privacy risks due to continuous data monitoring [34, 70]. Secondary users, often unaware of device activities, face privacy concerns when exposed to VAs in shared spaces, requiring solutions that allow them to manage these devices effectively and respect their privacy [1, 72, 73].

2.2 Privacy and Convenience Rationalizations in Smart Homes

Privacy encompasses a range of dimensions, from data control to power dynamics and the appropriateness of data use [4, 49, 54, 66–69, 82]. However, there is a paradox in which convenience often takes precedence over stated privacy concerns [29]. This paradox persists even when users are aware of the privacy risks associated with smart devices [1, 72]. Rooted in Westin's notion of privacy as an individual's right to control data sharing [82], this perspective calls for self-management. However, companies that offer conveniences to end users assume a uniform ability of users to perform effective privacy actions [47, 55]. The dominant data collection approach of companies relies on notice and consent, but users rarely read privacy policies that are the typical means of asking users to consent to tracking their data, often due to convoluted language [51]. Privacy notices, including informing the status of the device through software solutions (e.g., whether a device is listening or watching using LEDs), often prove ineffective due to complexity, limited choices, user fatigue, or device disconnection, particularly evident with smart home sensors [38]. This issue also extends to secondary users of the devices, who are often considered more vulnerable due to their limited grasp of technology and the corresponding privacy implications [47, 55]. To counteract passive notice and consent models that rely on purely language-based privacy notices, visceral notice was suggested as an improvement to experience privacy warnings, such as cellphones that use shutter noises when taking photos despite not having a physical shutter [13]. Geeng et al. [27] extend the concept of visceral notice to a new VA persona to make notice of data capture, storage, access, and use extremely

visceral with the hope of evoking strong emotional reactions in users. Similarly, Seymour et al. [62] used fictional and speculative approaches to decontextualize familiar and imagine alternatives for reflecting on technology that has become part of everyday rituals and routines.

The concept of self-management of privacy has been extensively examined in the context of Web privacy, with the aim of empowering users to have control over their personal data collection [26, 76, 89]. Various innovative approaches have been explored, including visualizing privacy policies in ways similar to nutrition labels [35] and introducing contextual permission systems for IoT environments [61], all with the goal of improving the ability of users to manage their data access. However, focusing solely on individual control might overlook the broader societal implications [59]. As discussions continue, emerging frameworks such as personalized privacy assistants and government regulations seek to strike a balance between individual control and societal concerns. In the context of smart homes, where data collection is highly intimate, robust control mechanisms are essential to meet both legal requirements and societal expectations while also mitigating privacy risks. Users often rationalize privacy risks and justify their choices for convenience, leading to cognitive dissonance between their concerns and their usage patterns. Differentiating between rationalization and justification for both primary and secondary users is essential to understand how these cognitive processes influence decision making and design effective solutions that meet both privacy and convenience needs.

2.3 Privacy Awareness Mechanisms

VAs seamlessly blend into daily routines, offering unmatched convenience through voice-controlled functions and personalized services; concurrently, their "TARDIS" effect renders several dimensions of their capabilities and operations invisible to end users. Wallace et al. [81] describe the Internet of Things (IoT) as having technological capacity on the inside that far exceeds our perceptions of the object from the outside. They call this the TARDIS effect, a name taken from the British Sci-Fi series Doctor Who, in which the hero travels through space and time in a telephone box that is far bigger on the inside than the outside. Shorter et al. [65] implicate two important design aspects for privacy, control, and transparency: how to make users aware of what is happening when the user interacts with these invisible systems and how do users know what to interact with in the first place. Rogers et al. [57] explored the advocacy for the voice-enabled Internet through a series of physical props. Chatting et al. [15] extended physical props with metaphors and design patterns to make invisible computations appear again for users to improve their privacy and security of smart devices. Wallace et al. [81] argue that making complex data physically visible can make it more personal and meaningful for users to take privacy actions. This concept echoes the influence of physical proximity on perceptions of ownership, as closer physical connection often intensifies the sense of ownership. Taylor et al. [74] demonstrated an increased user engagement with dynamic physical data representations, which are considered more compelling, legible, and viewable compared to static on-screen charts. They also agree with Wallace et al. [81] in asserting that physical data representations establish meaningful connections in the real world, allowing onlookers to understand and relate to the data more effectively.

In the context of VAs, researchers have delved into minimalist prototypes that offer users means to monitor VA status and assert control, exemplified by Project Alias [37], which ensures that the assistant is paralyzed and unable to listen by simply attaching a physical clip to a default VA [17]. Chen et al. [16] introduce wearable jammers to improve the transparency of constant control on listening devices. Tiefenau et al. [75] introduce a privacy hat that makes privacy actions graspable through tangible interactions to further enhance the effect. Windl et al. [83] explored privacy mechanisms within the concept of "tangible privacy" by Ahmad et al. [2] that caters to inclusive privacy, benefiting less tech-savvy users such as children and older adults. Desjardins et al. [22] designed the Inner Ear in response and in contrast to a growing collection of 'always on and recording' smart home devices. In their work, they use data physicalizations to increase awareness and stimulate reflection among users. Do et al. [23] recently introduced perceptible assurance of privacy with smart speakers. In their system, the microphone can only be powered by harvesting energy from intentional user interactions. Additionally, users have the ability to visually inspect the connection status between the energy harvesting module and the microphone, enhancing their confidence in their perceptions of privacy. In summary, transparency, proactive awareness, and tangible privacy mechanisms have been shown to be vital to improving VA privacy and user understanding, helping to balance the benefits of convenience with privacy concerns. In our study, we take similar strides from the above-mentioned work in designing a provocation in the second part of our study.

3 STUDY A: UNDERSTANDING THE PRIVACY PARADOX

The purpose of this study was to explore the psychological and cognitive processes used by people in the rationale between the benefits of convenience and the privacy concerns of VAs.

3.1 Demographics and Procedure

We used opportunity sampling to find VA users primarily through online social networks. All participants volunteered to participate in the study and had no previous relationship with any of the authors. Our inclusion criteria were that participants must own and have used a VA for more than 3 months.

The median age of the participants was 35 years, ranging from 22 to 45 years. All participants interviewed claimed to be the primary users of their VAs. Five participants identified themselves as women, while eight participants identified themselves as men. Eight participants came from Denmark, while five participants came from Japan (see Table 1). Our inclusion of Japanese participants was motivated because they typically own VAs that have different characteristics from typical devices such as the ones from Google or Amazon. For example, most of our Japanese participants owned Clova (see Figure 1), a VA developed by LINE [19]. Clova is different from typical VA because it is anthropomorphic and "*themed after the popular LINE characters Brown and Sally*" [18] to make its users "*feel as they are talking to the character*" [18].

We ensured that our study adhered to the ethical guidelines established by our Institutional Review Board. Subsequently, we conducted the study by first clearly explaining the intention of the study to all our participants, and only after they gave their consent did we proceed with the following steps. We emphasized that participation in the study was voluntary and that participants had the right to withdraw at any time without consequences. To protect the confidentiality of our participants, we removed personally identifiable information from the interview transcripts. In this first study, we conducted semi-structured interviews with the 13 participants to better understand the privacy paradox of VAs. The interviews lasted between 28 and 60 minutes. The interview questions revolved around a general understanding of VA and privacy concerns, explanations of beliefs or assumptions the participants had about the way their data were used, and discussions of how they trade off privacy and convenience. In what follows, we explain the role of system justification theory in study A.

3.2 Data Analysis: System Justification Theory

System Justification Theory (SJT) is a theory that explains how people tend to defend and rationalize existing social, economic, and political systems, even when these systems may be unfair or lead to inequalities [33, 42, 52, 78]. SJT can offer reasons why users justify their underlying motivations, norms, and psychological processes. SJT includes the following mechanisms (no particular order):

(1) **Stereotyping**. Stereotypes can shape people's understanding of the privacy risks of voice assistants [33]. For example, people may stereotype a specific tech company as always putting profits first or believe that people who are concerned for their privacy are of a certain type, leading them to underestimate potential privacy risks.
(2) **Rationalization of Status Quo**. Rationalization involves justifying the current state of affairs, even if it disadvantages certain groups or individuals [33]. In the context of VAs, people may rationalize the privacy paradox by focusing only on the benefits while downplaying privacy concerns.
(3) **Internalization of Structural Inequalities**. People may internalize the idea that power imbalances and data collection practices are inherent in the 'system'. Thus, they may accept data collection as a norm, making them less likely to question or resist [33].

Although SJT is typically utilized for studying systems, our decision to employ it in exploring the perceptions of VA users was informed by previous research [1, 72]. These studies revealed that users often perceive VAs as autonomous devices, overlooking the underlying complexities that define them as systems, such as cloud-based processing, Internet dependence, and integration with third-party services. We also anticipated that SJT mechanisms could help address the tension between privacy protection aspirations and practical challenges posed by existing systems/structures [59, 60].

We applied a deductive thematic analysis [9] using SJT as a framework to examine our interview transcripts. Two authors went through all interview transcripts and identified several codes that were most informative. Subsequently, with the participation of all authors, we iteratively progressed from open coding to thematic coding, collaboratively using the three SJT mechanisms to categorize codes extracted from the interview transcripts. In the following, we present these categorized codes in line with the three SJT mechanisms.

4 FINDINGS FROM STUDY A: HOW AND WHY THE PRIVACY PARADOX IS JUSTIFIED

Our findings show that the primary reason for our participants to use VAs was *convenience*. In short, all participants praised the VAs for automating routine tasks, effectively saving valuable time. Participants seamlessly integrated VAs into their daily routines, relying on them for various tasks such as setting timers and playing music. They even found educational value in VAs, using them to get answers to questions and improve language skills. One participant highlighted this by saying, "*So, every morning I don't have to check my smartphone for schedule or weather*" (Participant K). This convenience, closely related to hands-free interaction, also influenced participants' choices regarding the placement of VAs (see Table 1). Obviously, such finding is also reported by other VA studies [5, 14, 28]. Convenience was also the main driving force behind learning how to interact with a new device, such as a VA. Managing the mental load associated with remembering various voice commands often posed a challenge that most householders were willing to overcome. One of our participants reached their limits: "*I forgot the [Amazon] Echo device skill name. What skill I enabled and what skill [...] I don't remember every skill name, so I stopped using additional skills*" (Participant M).

4.1 Stereotyping

We identified two instances of *stereotyping* which are elaborated next.

VAs as human servants. A notable observation was how the participants humanized their VA, mainly using feminine pronouns and attributing human-like personalities to them. This stereotyping component led most participants to perceive their VAs as more than machines, and more likely as servants, as also described by Strengers et al. [71]. For example, one participant referred to Alexa's ability to remember important items, highlighting how the VA was at their service: "*She [Alexa] can remember where you put your important stuff like a passport or something*" (Participant C). Some moved a step further assigning to their 'servant' a unique and even somewhat sassy personality: "*Alexa does tend to [...] a bit more of a fun personality. And I think Amazon has a little more leeway when it comes to giving Alexa more of an actual personality with a bit of an attitude*" (Participant D). In addition, participants personalized their VAs' wake words, treating them as integral parts of their households that are always ready to serve: "*I think it is ridiculous that you wake it by the company name. Personalizing it in one way or another would be fun. Also, because it's kind of Study of the family in the way we use it. It's kind of a pet you can just call*" (Participant M).

Perceived cuteness was also the reason that participants often ignored their VA (servants') mistakes. This was more evident for the Clova VA. For example, one participant appreciated Clova's attempts to understand words and its endearing responses: "*When Clova tries to understand words but mishears and responds with 'what*

Table 1: Demographics of the participants in Study A.

#	Gender	Age	Location	Occupants	VA Models	Placement
A	Female	32	Denmark	2	Amazon Echo	Living room, Kitchen
B	Male	24	Denmark	1	Google Home Mini	Living room
C	Male	23	Denmark	2	Google Home, Google Home Mini	Kitchen, Living room
D	Male	36	Denmark	3	2 Google Assistants	Office room, Kitchen
E	Male	29	Denmark	3	Amazon Echo Dot	Living room, Bedroom, Bathroom
F	Male	45	Denmark	4	Google Home Mini	Bathroom, Living room, Office room
G	Male	40	Denmark	4	Google Home, 2 Google Home Mini	Bathroom, Living room
H	Female	30	Denmark	3	Google Home, Google Home Mini	Bedroom
I	Female	32	Japan	2	Echo Play, Clova, Echo Spot, 2 Google Home Mini	Living room, Kitchen
J	Female	35	Japan	1	Google Home Mini, 2 Amazon EchoDot	Kitchen
K	Male	36	Japan	3	Amazon Echo, Clova, Google Home Mini, Amazon Echo Dot	Living room, Office room
L	Female	38	Japan	1	Google Home, Clova	Living room
M	Male	38	Japan	8	2 Amazon Echo, Clova, Google Home	Living room, Kitchen

can I help you with?'—even though it's not the best functionality, I kind of appreciate it because it reflects her personality, and I find it endearing" (Participant M). In addition, the physical appearance of Clova (see Figure 1) played the main role in being perceived as a cute servant, showing that participants associated its design with personality traits: "*Amazon Echo and Assistant blend well with my home decor, but Clova is a bit too cute for my taste. However, my daughter loves its design*" (Participant L).

I enjoy that we are all similar. The ability to dress up Clova was very important for some participants, who assumed that all Clova users behave similarly to them. As exemplified by one participant: And I actually, I've been to community events, where they like, create an outfit for Clova and like [...] so, some like, some girls, we get together in a weekend and we create an outfit, for like a few hours and then we put it on Clova and it, you know, it's on our own Clova. And like 'See my Clova is the cutest' and things like that" (Participant I).

4.2 Rationalization of Status Quo

In our analysis, we have identified three instances of *rationalization of status quo.*

To trust or not to trust? Although all participants really valued their convenience. Most did not care about their privacy being violated: "*everyone is monitored by their phones or computers anyhow*" (H, female). However, some had limits on which tasks VAs were allowed to perform and on what kind of data they could access. For example, by being skeptical about the absence of a visual interface and by not having the possibility to clearly see a price participant J reported "*I can't see how you can trust it enough to buy things*" (Participant J). Furthermore, some did not want to provide their VAs with full access to their personal data, despite the fact that these devices where placed inside their homes: "*The devices [Alexa and Google Assistant] we have at home right now, they do not have access to any of my personal data. So, we're not doing any interaction with calendars or email or anything like that with those at the moment*" (Participant D).

Where should you live? Most of the participants did not care much about where their VAs were located, in relation to possible privacy violations (see Table 1 for details). Very few reflected on what kind of data these devices could collect depending on the room in which they were placed. As exemplified by one participant: "*In the living room we can talk about anything [...] It is not good to have a smart speaker in the bedroom*" (Participant K). What most participants (especially the Danish ones) were interested in was how the design of a VA would fit the style of the room it was placed in: "*So, of course, I think a bit about it, but I also wanted it to be a bit neutral to our already existing house*" (Participant C), reflecting a rationalization of maintaining the status quo.

I am ordinary. The primary reason, however, to justify the fact that data collection and privacy violations are part of the system was

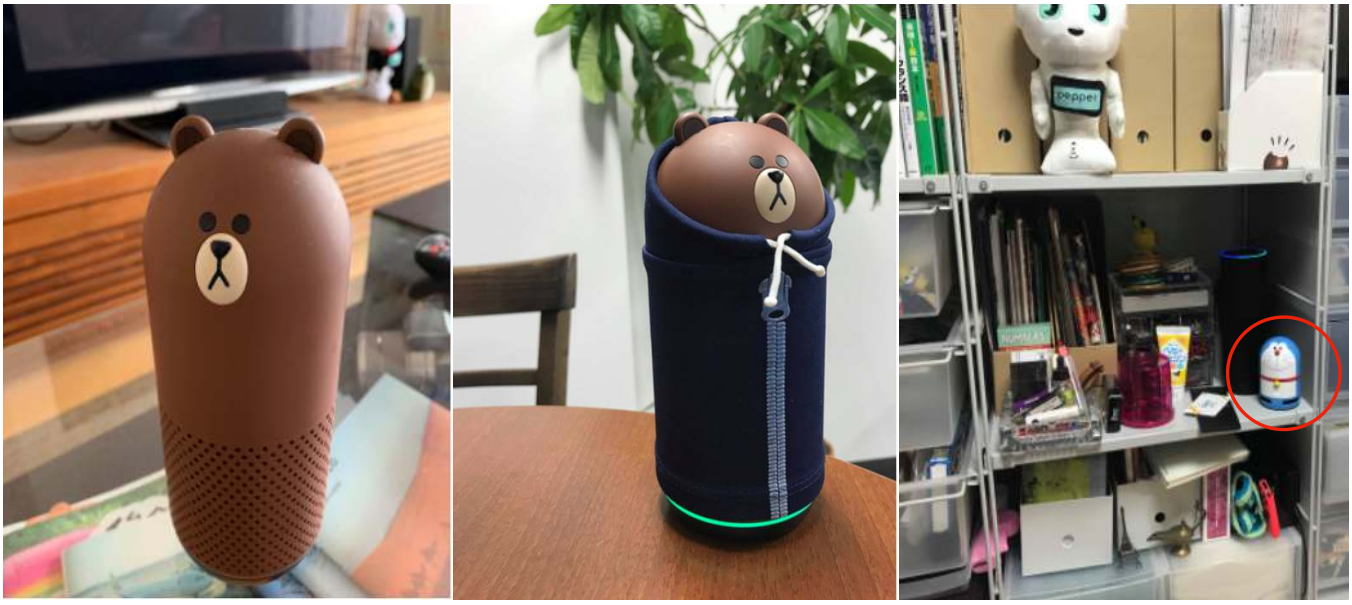

Figure 1: Anthropomorphic Voice Assistant Clova. Householders can also dress their device (middle image, participant J). Clova placed in the living room of participants: I and M (first and second image).

how *ordinary* householders were. As expressed by one participant: "*There are a billion people in the world, so if they want to listen to me, go ahead [...] I think I am boring. I don't think I'm such a special person that they want to*" (Participant F).

4.3 Internalization of Structural Inequalities

Finally, we identified two instances in which our participants *internalized structural inequalities.*

Don't remind me! Although most VAs provide notifications about updates to privacy policies and data handling from third-party skills, many participants consciously chose to remain oblivious. Although the importance of these updates was recognized, participants found it easy to overlook information on such matters, utilizing a "looking away" approach from the situation. One participant asked for easier ways of being informed about this: "*It would be kind of cool to have the device itself somehow indicate if it has learned new skills, or you could ask it, for instance, being able to ask: What did you learn today, Alexa*" (Participant G).

My home, my rules? Many participants acknowledged that their VAs could violate the privacy of secondary users (other members of their household and/or guests). As described by one participant: "*There are two types of people. There are people like my friends who have ten assistants in their home, and they all know how to talk with them. But there are others who believe that assistants are sneaking [in] our home. For them, maybe it's kind of scary*" (Participant L). Even in those cases, though, none of our participants reported acting to protect the privacy of secondary users, by, for example, shutting down a VA or stop using it for a while.

5 STUDY B: DESIGNING AGAINST THE PRIVACY PARADOX

Inspired by our findings in Study A that include indifference to the physical location of the VA, self-perception as ordinary individuals, lack of empathy for household members, and a tendency to overlook policy updates regarding data handling with third parties. Our aim in Study B was to design to make people reflect deeper on their justifications. The approach was to produce a *provotype* [32, 48], and use it as a probe in real world settings to facilitate in challenging the identified justifications. Our hope was that through provotyping we would be able to help our participants identify the problem (and not so much a solution), provoke reactions, stimulate discussions, and help them reflect upon their assumptions [11]. Provotypes have been successfully implemented with similar objectives in multiple settings, such as challenging energy consumption practices [56], inequalities in pay [3], worship services [84], or participatory innovation [10].

5.1 VoxMox, a provocative Voice Assistant

Our provotype is called VoxMox (see Figure 2). Its name combines the words 'vox' (Latin for "voice") and 'mox' (derived from the English word "moxie", meaning force of character, determination, or nerve). As we have already observed several instances in study A findings that participants justify their lack of concern to privacy for the sake of VA conveniences. Our aim with VoxMox was to understand how provocation is experienced in the real world (provocation in use [10]), and how it can challenge existing practices. In line with this aim, we developed VoxMox by heavily relying on Bardzell et al's. [7] framework of *aesthetic*, *functional*, and *conceptual* provocation. This approach was aimed at making users more aware of and reflect on their privacy decisions and the compromises they make for convenience. By stimulating strong reactions, we hoped to encourage a deeper understanding and discussion of privacy issues related to smart home devices.

Aesthetic provocation refers to how far away from the norm are the aesthetics of a design [7]. Instead of opting for the sleek

Figure 2: VoxMox placed next to a sleek Google Assistant.

and minimalistic design that most VAs have (e.g. see Figure 2) or a more anthropomorphic one like Clova (e.g. see Figure 1), VoxMox encompasses a bulky design that clearly signifies the recording capabilities of VAs. In the context of study A findings, participants attributed human characteristics, such as cuteness, to VAs based on their physical appearance. Simultaneously, discernible power dynamics emerged, where users perceived their VAs as subservient entities, dutifully executing mundane tasks without exhibiting any form of resistance or rebellion. To make users reflect on such stereotypical instances, we modified the housing of a real-world cassette player/recorder (Blaupunkt Bari CR 7652). Furthermore, to further highlight the recording capabilities of the device, the red recording button was always pressed (Figure 3A) and every time the device was activated, a red light was turning on (Figure 3B) and the cassette pins (Figure 3C) would start spinning producing a humming sound.

Functional provocation refers to how far away from the norm a design functions [7]. In addition to the clear aesthetic link between VoxMox and a recording device, VoxMox goes beyond typical VA functionality. VoxMox extends the hand-free interaction of VAs with an 16x2-character LCD screen (Figure 3D). In Study A, we observed that participants were cognizant of but did not contemplate the data tracked or the frequency of their interactions with their VAs. We attribute this lack of reflection to the inherent opacity of internal functionalities, such as listening and recording, which lack explicit feedback mechanisms. This opacity resembles the phenomenon known as the "TARDIS" effect, as discussed in our related work [65, 81]. To encourage users to reflect on their usage frequency, we implemented a solution: the upper line of the LCD screen now displays the total duration the device has been actively listening in the household (referred to as "Total Listening Time" - see Figure 4), while the bottom line shows the timestamp of the last interaction recorded by the device (referred to as "Last Recording Time" - see Figure 4).

Conceptual provocation refers to the idea/belief/concept that someone wants to provoke through a design [7]. The prevalent idea that privacy is the sole responsibility of an individual instead of the tech manufacturers (e.g. system) underpins the design of default privacy settings and policy solutions to be less in favor of the users [59]. Moreover, the advertisements from manufacturers introduce VAs as convenient devices that immediately provide users with seamless control of their home environment which can overshadow the potential privacy breaches from the back-end complexities (e.g., sharing data with third parties) [1, 50, 65, 72]. We expect that by visually rendering the data flows of VAs more vividly through VoxMox, we can provoke a conceptual shift. This shift may challenge ingrained behaviors observed in Study A, such as ignoring privacy policy updates and displaying a lack of empathy towards secondary users.

In order to build VoxMox, we utilized a Raspberry Pi 3 Model B to host a Google Assistant (Figure 5E), a speaker (Figure 5D) and a USB microphone (Figure 5A), a servo motor to control the cassette pins (Figure 5C) and the LCD screen (Figure 5B). The implementation utilized the Google Assistant Library (GAL) in Python, and Python was also used for controlling all hardware components. Finally, Python scripts were also used to log users' interactions with the device.

5.2 Procedure, Participants and Analysis

VoxMox was implemented as a technology probe study [31] aligning with the aim of understanding how provocation is experienced in the real world and challenging existing practices in three households (different from Study A). All households were recruited through social media and used the provotype for one week each. Similar to study A, participants in this study had no previous relationship with any of the authors. A common inclusion criterion for all households was that they owned and used a Google Assistant for at least three months. Similarly to Study A, we ensured that our study adhered to the ethical guidelines established by our Institutional Review Board. Subsequently, through a consent form, all households agreed to a) log into their own Google Assistant through VoxMox, and b) to provide us with their usage data before and after VoxMox deployment. This is the reason, for example, that in Figure 4 the 'Total listening time' is in days, since this household owned a Google Assistant for 91 days, 11 hours and 27 minutes. After the initial setup, each household placed VoxMox in their home, and was instructed that they could move it, turn it OFF and end the study at any moment without any consequences. All households placed VoxMox in their living room (Figure 6 and Figure 7).

We made sure to clearly explain the intention of the study to all our participants, and only after they gave their consent did we proceed with the following steps. We informed our participants that VoxMox was offering the same functionality as their own VAs, with the addition of them being informed about the hidden listening/recording functionalities. We also emphasized that participation in the study was voluntary and that participants had the right to freely withdraw at any time. To protect the confidentiality of our participants, we took measures to remove personally identifiable information from the collected data, and the log data were only used anonymously for statistical purposes. Similarly to Study A, all participants volunteered to participate in the study.

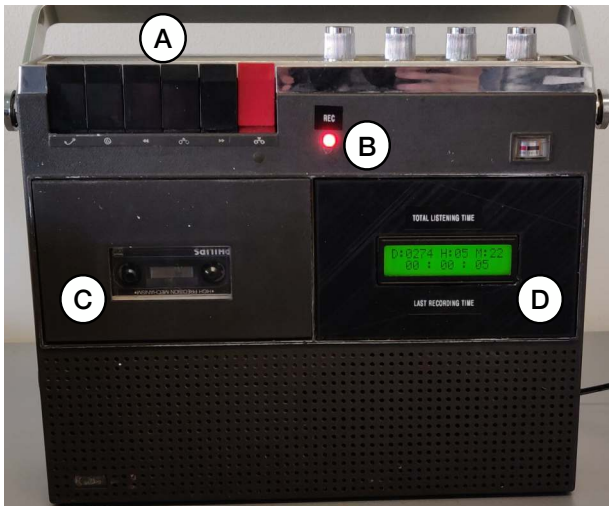

Figure 3: VoxMox: A) Red recording button - always pressed, B) Red light indicating a recording, C) Cassette pins spinning upon activation, D) LCD screen displaying times.

Figure 4: Closeup of VoxMox's LCD screen. The upper row displays time since activation and bottom row the duration of last interaction.

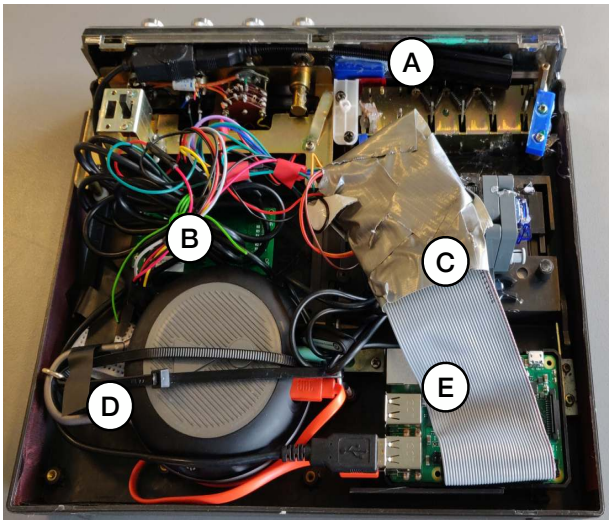

Figure 5: VoxMox hardware components: (A) USB-microphone, (B) LCD screen, (C) servo motor, (D) speaker, and (E) Raspberry Pi.

Household 1 (participants N and O) consisted of a man and a woman aged 31 and 29 years, respectively. Their household also included two children (two and four years old). Both adults had full-time jobs, the man working as a marketing assistant and the woman as a carpenter. Household 2 (participants P and Q) consisted of two male roommates, both 22 years old, who lived in a relatively small apartment. One of the participants had a job in IT-support and the other was on a break from university. Household 3 (participant R) consisted of a 25-year-old male computer science student who had no relation to the project team. We interviewed both occupants

Figure 6: Household 1. VoxMox (right) replacing a Google Home Mini (left) below the TV in their living room.

Figure 7: Household 3. VoxMox (right) replacing a Google Home Mini (left) below the TV in their living room.

from household 1, both occupants from household 2 and the single occupant from household 3 after they had used VoxMox for a week. All the interviewed participants considered themselves the primary user of their VAs. The interview transcripts followed the same two-step procedure as described in Study A for anonymization. The transcripts underwent thematic analysis [12] by the same two authors from Study A. With the input of all authors, we iteratively progressed from open to thematic coding, identifying instances of privacy violations being observed, acknowledged, reflected upon, or rationalized. These findings are presented in the following section.

6 FINDINGS FROM STUDY B: WHAT HAPPENS WHEN YOU PROVOKE THE STATUS QUO?

Similar to Study A and also other studies with VAs [5, 14, 28], the main reason for having a VA was convenience. For example, participant R informed us that they use a VA because sometimes they like "*being lazy, when I use it as a remote*" (Household 3, participant R).

Things became more visible. The design differences between our provotype and a typical VA were immediately observed by our participants. For some, the physical design was perceived as ugly: "*I'm not fond of the design. I think it stands out too much and is too old school for me*" (Household 3, participant R). Furthermore, the LCD screen with its reported times (Figure 4) was characterized as *spooky*, the recording sounds as *creepy*, and the thing as a whole as *old school* and *intimidating*: "*It was intimidating because it shows how much data you feed the VA with*" (Household 2, participant P). Despite the uncomfortableness though, VoxMox was successful in making the privacy challenges visible for all participants and urged them to reflect on their practices: "*My first thought when acquiring the Mini was excitement, but also frightening. The element of having an active microphone in your home, which you do not really know when listens*" (Household 2, participant Q).

These reflections urged one of our participants to discuss in detail the need for more regulatory control: "*I would prefer that there were some kind of control, for instance, at the government level, to control it, so that there were other instances overlooking them rather than having free play. It would definitely be nice if there were some kind of control regulations that looked at the data [the VA is collecting]. It is unrealistic, but it would be the most ideal for all the data they [organizations] gather to be screened before the organization gets the data*" (Household 1, participant O).

But maybe you exaggerate a bit? Even though VoxMox was essentially households' own Google Assistant with some additions, many participants believed that we were exaggerating on the level of surveillance we presented to them though the provotype. For example, participant O from Household 1, felt surprised when they realized that their own device was recording, as they believed that VoxMox recording time "*[...] that was probably one giant lie*". Additionally, when reflecting on the VoxMox's recording sounds, all participants believed that we were surveying them more than a typical VA: "*The way it works. It keeps recording. Something Happens.*" (Household 2, participant P).

Justification and Apathy. All participant encompassed the privacy paradox and started justifying the fact they have been listened to by their VAs. Some, mentioned that they *trusted* the companies that produced their VAs: "*It is showing trust in having an active Google Assistant at home because there is a chance that it will listen all the time. Also when you have not talked to it. If there is no baseline of trust to the product or Google, or who ever has these [VAs], Amazon, or Apple. If you do not trust it, it would be absurd to acquire one of these devices*" (Household 3, participant R). Furthermore, VoxMox was also trusted from one of our participants as it essentially was their own VA in disguise: "*I realized that Google Assistant has been listening to us for quite some time, and VoxMox is just a temporary addition for the study. So, it didn't bother me much after that realization.*" (Household 2, participant Q).

But even though some fears were expressed "*I fear that the data they give to the VA can be used against them if they are leaked. The thought of having an assistant, 'a helper', that you are afraid to be turned against you is wrong*" - (Household 2, participant Q), all participants showed apathy [80] in prioritizing their privacy over their comfort. This was observed in two ways. Some of the participants reasoned that the situation could have been worse and that the companies were the best they could have encountered under the circumstances: "*Who else would it be? It [data] should not be in the hands of anyone, preferably*" (Household 2, participant Q), and "*They are known to spy on people and their whereabouts using their services. I don't mind much, because they will listen anyway if we talk about privacy. There is a chance that they will get data elsewhere anyhow. If you have any piece of technology, if it is a PC, a smart speaker, maybe even a refrigerator. There is always something under the ropes that listens. It is directly or, as is called, indirectly*" (Household 3, participant R). Second, thinking of companies as not desirable but partially acceptable, culminates in participants characterizing themselves as *normal* and *not unique*, and accepted being apathetic in the fact that their personal data could/should be divulged to these companies.

Finally, as one of our participants stated only if facing extreme situations people would be interested is changing their practices: "*It would need some kind of scandal so that we would all wake up and take more responsibility*" (Household 1, participant N). Apathy was also observed while examining the log data we collected for the three households. All households interacted more than normal with VoxMox the first day of deployment possibly due to it being something new and exciting. But, then despite feeling provoked and challenged by VoxMox, all households returned to their normal apathetic practices. Although the quantification of apathetic behavior may not be immediately evident in Figure 8 as it is in our interview findings, the categories with the highest usage, such as controlling services, controlling other devices, and jokes, exhibit similar patterns between Google VAs and VoxMox across the three households.

7 DISCUSSION

In this paper, we explore the cognitive and psychological mechanisms underlying individuals' rationales for balancing the conveniences of VAs with potential privacy risks. Initially, we used system justification theory [33] as a framework to guide thematic analysis of interviews with 13 participants from Denmark and Japan. Subsequently, using the insights from Study A, we developed a provotype named VoxMox, following the provocation framework outlined by

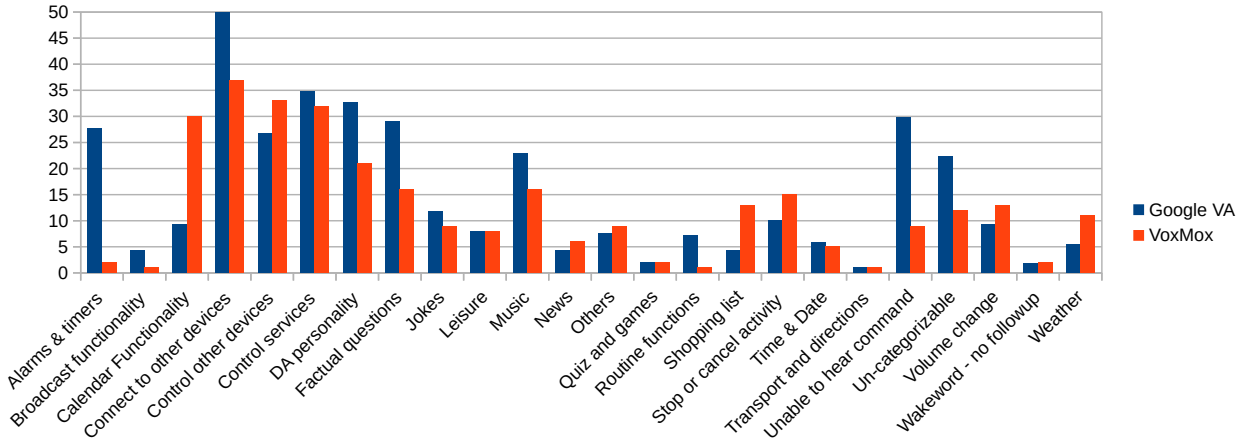

Figure 8: Combined average usage patterns of typical VA tasks of all three households using VoxMox (red) and their own VA (blue) for the duration of a week. Task categorizations emerged from [58].

Bardzell et al. [7]. VoxMox served as a technology probe to foster deeper reflections on instances where convenience is prioritized over privacy concerns. Central to the findings of both studies is the pervasive attitude of apathy toward privacy actions, a focus we elaborate on in this section.

7.1 Privacy Apathy through Insights from VA users

Our participants voiced concerns about potential privacy violations arising from their frequent use of VAs in daily life, yet they did not take proactive measures to address these concerns. This apathetic stance suggests that the privacy paradox persists in the context of VA usage. However, delving deeper, several nuances shed light on the interplay between privacy concerns and attitudes towards privacy actions.

Apathetic attitudes towards privacy have been extensively discussed in the context of online privacy, particularly in social networking sites, where individuals express resignation about privacy violations and perceive an inability to change the situation. This resignation can sometimes transform into cynicism, where individuals believe they have no privacy control when using social networking sites [43]. In such scenarios, the only perceived solution to prevent privacy violations is to opt out entirely, a course of action often dismissed as unrealistic due to the fear of missing out on the conveniences of staying connected [30].

Similarly, in Study B, although VAs' functionalities, such as listening and recording, were made visible through VoxMox, households questioned whether we had exaggerated the surveillance capacities of their VAs. Despite these concerns, none of the households chose to disconnect or unplug VoxMox and withdraw from the study. Instead, they continued to use it almost identically to their own devices, as revealed in our findings. Reflecting on our study A findings, users demonstrated apathy through a lack of concern and a persistent disregard for privacy policy updates, sometimes intentionally avoiding them. Such instances of apathy were rationalized as participants perceived themselves as "normal" and "not unique". In Study B, when users were prompted to reflect on similar instances when using VoxMox, which made the internal mechanisms of their VAs more visible, apathetic behavior persisted. For instance, participants found the LCD screen displaying total listening time 'creepy', contributing to a heightened sense of surveillance compared to their own VA, despite identical functionalities.

These observations underscore an existing privacy attitude known as privacy apathy, initially conceptualized by Hargittai et al. [30] and later adapted by Augustin et al. [6] into the context of intelligent voice-assisted agents. Privacy apathy suggests individuals abandon efforts and lose interest in privacy due to feeling powerless over their information. In our studies, privacy apathy also reveals how users habitually interact with VAs without critically evaluating privacy trade-offs. Unlike online privacy on social networks, privacy concerns with VAs can be more pervasive due to their physical presence, always-on nature, and sleek design, blending seamlessly into home environments. This may contribute to apathetic behavior, even when VAs deviate from expected patterns due to false activations. An increased dependence on VAs can also lead people to view them as indispensable personal assistants.

In the context of smartphone applications, Shklovski et al. [64] suggest that people's lack of response when they encounter unexpected data flows violating their privacy reflects learned helplessness. This is a resignation stemming from feeling powerless upon discovering how little control users have over the potential misuse of their data [24]. Since our provocation intentionally revealed the capabilities of the technology, we did not anticipate unforeseen reactions from our participants. Despite being prompted to reflect and made intentionally aware of data flows during interactions, participants did not change their apathetic attitudes not did they take privacy actions.

Individuals categorized as 'privacy unconcerned' according to Westin's privacy segmentation [82] exhibit a disregard for sharing personal data, minimize privacy issues, and endorse third-party data sharing despite warnings. However, when applying Westin's segmentation to contemporary data-centric technologies, such as

VAs, some privacy researchers [53, 59, 77] argue that contextual factors and misinformed views about privacy are often overlooked. Our findings reinforce this viewpoint, revealing that even when asked to consider privacy breaches and made aware of audio surveillance capacities, participants remained apathetic, particularly in scenarios where conveniences of VAs are deeply integrated into everyday life.

7.2 Implications to Breaking Privacy Apathy

In a state of privacy apathy, people often overlook the importance of establishing boundaries or exercising control over their personal data. But why does privacy apathy occur in the first place? Is it only due to convenience, justification of the status quo, or powerlessness? Upon reflection of our findings, it appears that our participants assume VAs primarily prioritize their best interests, given the seamless provision of voice-based conveniences and user-friendly plug-and-play design. Consequently, there is a lack of awareness and understanding regarding the privacy implications, in contrast to the familiarity with the provided conveniences.

Instances where privacy implications are overshadowed by VA conveniences are apparent in the indifference towards VA location and the disregard for privacy notices. Previous research in smart home privacy [28, 39, 85] suggests that primary tech-savvy users may have a tactical advantage in protecting themselves from privacy violations. However, in contrast, these users may only appear to make rational trade-offs between privacy and convenience. Instead, their rationality may be overshadowed by apathetic attitudes, as evidenced by SJT mechanisms: stereotyping (e.g., users show apathy when they overlook mistakes made by their VAs), rationalization of the status quo (e.g., users show apathy when justifying placing VAs in sensitive locations at home), and internalization of structural inequalities (e.g., users show apathy upon becoming aware of personal data shared with third parties).

Future studies should consider addressing privacy apathy through a comprehensive approach that includes analyzing privacy fatigue [6, 69], which incorporates cynicism and emotional exhaustion from feeling powerless. Although our provocation facilitated reflections, it did not provide users with active control. Therefore, we recommend that future studies using provotypes explore opportunities to provide users with explicit control (see, e.g., [63, 79]), which can foster the habit of coupling awareness and taking control as a means of breaking privacy apathy. In this regard, we suggest incorporating knowledge from previous work through concepts such as tangible privacy and perceptible assurance, which cater to inclusion for different household members who perceive privacy differently due to their varying mental models [2, 23, 83].

In study B, when the participants used VoxMox and saw more about how their own VAs work, looking back, we think that they may have used similar psychological mechanisms as seen in study A. This could have led them to make justifications and act apathetically toward privacy concerns. Based on the reflections of the participants, privacy apathy may potentially transform into engagement only when they personally experience a breach of privacy. Although provocation provided a medium to reflect apathetic attitudes, we believe that provocation also opened situations in which participants felt embarrassed as a consequence of their own actions. One such situation could be that when VoxMox made the inner workings of VAs more visible by engaging users with the aesthetic provocation of the overall appearance along with LED lights and also with the functional provocation of explicitly showing the duration of audio recordings. Participants expressed negative emotions such as feeling creeped out, while showing apathy at the same time. This interplay between expressing negative emotions and showing apathy resulted in participants suppressing embarrassing feelings. This suppression could be due to participants confronting their own choices or actions related to privacy protection, which they may have contemplated taking but deemed unnecessary or belated at that juncture. Although it may be considered outside the scope of this paper to delve in-depth into the topic of suppressing embarrassing emotions, a potential avenue to gain further insight could be exploring Dahl's theory of awkwardness [20].

Exploring embarrassing situations in shared physical spaces could present a promising avenue for future research with smart home devices in general. Smart home devices are characterized as multi-user devices with flexible usage boundaries, raising concerns about users' awareness of the device's surveillance capabilities [85]. Privacy apathy may also arise from potential hesitations regarding how others perceive privacy measures, which can hinder the adoption of protective actions. Previous research [28, 39] has demonstrated how primary users influence privacy perceptions within a household. We speculate that the fear of judgment and the perception of excessive caution by non-tech-savvy users could create resistance for tech-savvy primary users in implementing privacy measures. A constructive direction for future research could involve investigating the relationship between privacy apathy and embarrassing situations in social settings. We posit that this inquiry intersects with the concept of 'self-cringe' [20], where individuals experience embarrassment due to their own contributions to privacy vulnerabilities [47].

From a design perspective, we suggest that one approach could be to design for self-cringe experiences with the aim of stimulating more reflections and prompting proactive responses through explicit privacy controls. An extension of our provocation could move in the direction of advocating more visceral VAs [27, 62] that could involve transforming the traditionally amicable smart assistant persona into a more ominous one that always steers clear of passive privacy notices. This direction aims to elicit self-cringe experiences that could further heighten reflection and decisive actions that may work towards breaking privacy apathy. However, designers and researchers must exercise caution in determining the intensity of these self-cringe experiences, as excessive discomfort may arise. The ethical implications of deploying such designs should involve considerations on the impact on user's psychological well-being because excessive discomfort or embarrassment can potentially lead to stress. Furthermore, designers must consider the diverse range of users and their sensitivities to technology and acknowledge that some users may be more vulnerable that others [55]. Methodologically, designers must make users aware of the purpose and possible emotional impact of designs, ensuring that their participation is voluntary and informed along with the possibility to freely opt-out without any consequences.

7.3 Limitations

We acknowledge several limitations to the studies conducted. Firstly, observations made in households cannot necessarily be transferred to other cultures due to our limited demographics of mainly Danish participants. Second, the provotype in Study B was only deployed for one week in each household and the provotoype was also limited to only making the data flow in a VA more visible and not offering any explicit control options. This limitation hinders our ability to fully understand the long-term effects of privacy apathy and challenges our claims that participants remained indifferent even when provoked. Furthermore, it makes our speculations about the link between privacy apathy and embarrassing situations currently insufficient and warrants further investigation, particularly when we suggest that apathy arises from individuals' own contributions to privacy vulnerabilities. Third, our interviews comprised viewpoints mostly from primary users of VAs, and we believe that in the future including and engaging secondary users and bystanders, such as guests who can show different perceptions of privacy, would add further value to the implications of privacy apathy. Future studies are crucial to investigate the connection between negative emotions, such as embarrassment suppression, and privacy apathy. This understanding could potentially serve as motivation for individuals to steer clear of apathetic behavior towards privacy actions.

8 CONCLUSION

We investigated psychological and cognitive mechanisms that people use to rationalize and justify their privacy attitudes and behaviors when using VAs. The findings presented from the two studies illustrated a pervasive attitude of apathy toward privacy actions. Our contribution to the field of HCI is two-fold. Firstly, the identified instances through the lens of system justification theory and subsequently from the field studies conducted through the VoxMox provotype increase the empirical understanding of how people show privacy apathy despite being provoked to reflect by making the internal workings and data flows of their VAs more visible. Secondly, we highlighted the identified apathetic privacy attitudes by reflecting on our findings and also situating the identified apathetic instances in relation to the existing literature. We concluded by providing several implications on how future studies can break privacy apathy.

ACKNOWLEDGMENTS

This work was partly funded by the German Research Foundation (Deutsche Forschungsgesellschaft, DFG) through individual grant EC437/1-1.

We would like to thank Uldbjerg Jørgensen, Jesper Quist Jensen, Katrine Theilmann Gregersen, and Rasmus Thygesen Larsen for their valuable contributions to this research work.

REFERENCES

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS'19)*. USENIX Association, USA, 451–466.

[2] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 116 (oct 2020), 28 pages. https://doi.org/10.1145/3415187

[3] Naja Kathrine Kollerup Als, Julie Corlin Mikkelsen, and Dimitrios Raptis. 2022. The Troubling Cups: Making Trouble at Work about Inequalities in Pay.. In *Nordic Human-Computer Interaction Conference* (Aarhus, Denmark) *(NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 45, 12 pages. https://doi.org/10.1145/3546155.3546679

[4] Irwin Altman. 1975. The environment and social behavior: privacy, personal space, territory, and crowding. (1975).

[5] Noah Apthorpe, Pardis Emami-Naeini, Arunesh Mathur, Marshini Chetty, and Nick Feamster. 2022. You, Me, and IoT: How Internet-Connected Consumer Devices Affect Interpersonal Relationships. *ACM Trans. Internet Things* 3, 4, Article 25 (sep 2022), 29 pages. https://doi.org/10.1145/3539737

[6] Yannik Augustin, Astrid Carolus, and Carolin Wienrich. 2022. Privacy of AI-Based Voice Assistants: Understanding the Users' Perspective: A Purposive Review and a Roadmap for Elevating Research on Privacy from a User-Oriented Perspective. In *International Conference on Human-Computer Interaction*. Springer, 309–321.

[7] Shaowen Bardzell, Jeffrey Bardzell, Jodi Forlizzi, John Zimmerman, and John Antanitis. 2012. Critical Design and Critical Theory: The Challenge of Designing for Provocation. In *Proceedings of the Designing Interactive Systems Conference* (Newcastle Upon Tyne, United Kingdom) *(DIS '12)*. Association for Computing Machinery, New York, NY, USA, 288–297. https://doi.org/10.1145/2317956.2318001

[8] Eric P.S. Baumer. 2015. Usees. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 3295–3298. https://doi.org/10.1145/2702123.2702147

[9] Andrea J Bingham and Patricia Witkowsky. 2021. Deductive and inductive approaches to qualitative data analysis. *Analyzing and interpreting qualitative data: After the interview* (2021), 133–146.

[10] Laurens Boer and Jared Donovan. 2012. Provotypes for Participatory Innovation. In *Proceedings of the Designing Interactive Systems Conference* (Newcastle Upon Tyne, United Kingdom) *(DIS '12)*. Association for Computing Machinery, New York, NY, USA, 388–397. https://doi.org/10.1145/2317956.2318014

[11] Laurens Boer, Jared Donovan, and Jacob Buur. 2013. Challenging industry conceptions with provotypes. *CoDesign* 9, 2 (2013), 73–89.

[12] Virginia Braun, Victoria Clarke, Nikki Hayfield, Hannah Frith, Helen Malson, Naomi Moller, and Iduna Shah-Beckley. 2019. Qualitative story completion: Possibilities and potential pitfalls. *Qualitative Research in Psychology* 16, 1 (2019), 136–155.

[13] Ryan Calo. 2011. Against notice skepticism in privacy (and elsewhere). *Notre Dame L. Rev.* 87 (2011), 1027.

[14] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It Did Not Give Me an Option to Decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 555, 16 pages. https://doi.org/10.1145/3411764.3445691

[15] David Chatting, Nick Taylor, and Jon Rogers. 2021. Design for Reappearance in Smart Technologies. In *CSCW 2021 Workshop on Designing for Data Awareness*.

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

[17] Zhenfang Chen, Daragh Byrne, and Dina EL-Zanfaly. 2022. Google Home, Listen: Building Helper Intelligences for Non-Verbal Sound. In *Proceedings of the 14th Conference on Creativity and Cognition* (Venice, Italy) *(C&C '22)*. Association for Computing Machinery, New York, NY, USA, 619–622. https://doi.org/10.1145/3527927.3535202

[18] Naver Clova. [n.d.]. Naver Clova, Brown and Sally, howpublished = "https://linecorp.com/en/pr/news/en/2018/2219", year = 2023, note = "[Online; accessed 12-September-2023]".

[19] Naver Clova. [n.d.]. Naver Clova, Homepage, howpublished = "https://clova.ai/speech/en", year = 2023, note = "[Online; accessed 12-September-2023]".

[20] Melissa Dahl. 2018. *Cringeworthy: A theory of awkwardness*. Penguin.

[21] Christian Debes, Andreas Merentitis, Sergey Sukhanov, Maria Niessen, Nikolaos Frangiadakis, and Alexander Bauer. 2016. Monitoring Activities of Daily Living in Smart Homes: Understanding human behavior. *IEEE Signal Processing Magazine* 33, 2 (2016), 81–94. https://doi.org/10.1109/MSP.2015.2503881

[22] Audrey Desjardins, Timea Tihanyi, Freesoul El Shabazz-Thompson, Brock Craft, and Julia Saimo. 2023. THE INNER EAR: CAPTURING AND PHYSICALIZING HOME VIBRATIONS. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference* (Pittsburgh, PA, USA) *(DIS '23)*. Association for Computing Machinery, New York, NY, USA, 594–607. https://doi.org/10.1145/3563657.3596070

[23] Youngwook Do, Nivedita Arora, Ali Mirzazadeh, Injoo Moon, Eryue Xu, Zhihan Zhang, Gregory D. Abowd, and Sauvik Das. 2023. Powering for Privacy: Improving User Trust in Smart Speaker Microphones with Intentional Powering and Perceptible Assurance. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 2473–2490. https://www.usenix.org/conference/usenixsecurity23/presentation/do

[24] Nora A Draper and Joseph Turow. 2019. The corporate cultivation of digital resignation. *New media & society* 21, 8 (2019), 1824–1839.

[25] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS '17)*. USENIX Association, USA, 399–412.

[26] William Enck, Peter Gilbert, Seungyeop Han, Vasant Tendulkar, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. Sheth. 2014. TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. *ACM Trans. Comput. Syst.* 32, 2, Article 5 (jun 2014), 29 pages. https://doi.org/10.1145/2619091

[27] Christine Geeng and Anonymous Author. 2020. EGregor: An Eldritch Privacy Mental Model for Smart Assistants. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–9. https://doi.org/10.1145/3334480.3381827

[28] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300498

[29] Julia Hanson, Miranda Wei, Sophie Veys, Matthew Kugler, Lior Strahilevitz, and Blase Ur. 2020. Taking Data Out of Context to Hyper-Personalize Ads: Crowdworkers' Privacy Perceptions and Decisions to Disclose Private Information. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376415

[30] Eszter Hargittai and Alice Marwick. 2016. "What can I really do?" Explaining the privacy paradox with online apathy. *International journal of communication* 10 (2016), 21.

[31] Hilary Hutchinson, Wendy Mackay, Bo Westerlund, Benjamin B. Bederson, Allison Druin, Catherine Plaisant, Michel Beaudouin-Lafon, Stéphane Conversy, Helen Evans, Heiko Hansen, Nicolas Roussel, and Björn Eiderbäck. 2003. Technology probes: inspiring design for and with families. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Ft. Lauderdale, Florida, USA) *(CHI '03)*. Association for Computing Machinery, New York, NY, USA, 17–24. https://doi.org/10.1145/642611.642616

[32] Rikke Hagensby Jensen, Enrique Encinas, and Dimitrios Raptis. 2022. Spicing It Up: From Ubiquitous Devices to Tangible Things Through Provocation. In *Sixteenth International Conference on Tangible, Embedded, and Embodied Interaction* (Daejeon, Republic of Korea) *(TEI '22)*. Association for Computing Machinery, New York, NY, USA, Article 33, 15 pages. https://doi.org/10.1145/3490149.3502257

[33] John T Jost, Mahzarin R Banaji, and Brian A Nosek. 2004. A decade of system justification theory: Accumulated evidence of conscious and unconscious bolstering of the status quo. *Political psychology* 25, 6 (2004), 881–919.

[34] Frederike Jung, Kai von Holdt, Ronja Krüger, Jochen Meyer, and Wilko Heuten. 2022. I Do. Do I? – Understanding User Perspectives on the Privacy Paradox. In *Proceedings of the 25th International Academic Mindtrek Conference* (Tampere, Finland) *(Academic Mindtrek '22)*. Association for Computing Machinery, New York, NY, USA, 268–277. https://doi.org/10.1145/3569219.3569358

[35] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "Nutrition Label" for Privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages. https://doi.org/10.1145/1572532.1572538

[36] Julie A. Kientz, Shwetak N. Patel, Brian Jones, Ed Price, Elizabeth D. Mynatt, and Gregory D. Abowd. 2008. The Georgia Tech Aware Home. In *CHI '08 Extended Abstracts on Human Factors in Computing Systems* (Florence, Italy) *(CHI EA '08)*. Association for Computing Machinery, New York, NY, USA, 3675–3680. https://doi.org/10.1145/1358628.1358911

[37] Tore Knudsen. [n.d.]. Project Alias, Homepage, howpublished = "https://www.toreknudsen.dk/work/project-alias", year = 2023, note = "[Online; accessed 12-September-2023]".

[38] Marion Koelle, Katrin Wolf, and Susanne Boll. 2018. Beyond LED Status Lights - Design Requirements of Privacy Notices for Body-worn Cameras. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '18)*. Association for Computing Machinery, New York, NY, USA, 177–187. https://doi.org/10.1145/3173225.3173234

[39] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 41, 14 pages. https://doi.org/10.1145/3411764.3445598

[40] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 102 (nov 2018), 31 pages. https://doi.org/10.1145/3274371

[41] Natalia Lavado-Nalvaiz, Laura Lucia-Palacios, and Raúl Pérez-López. 2022. The role of the humanisation of smart home speakers in the personalisation–privacy paradox. *Electronic Commerce Research and Applications* 53 (2022), 101146. https://doi.org/10.1016/j.elerap.2022.101146

[42] Kun Liu, Kun Fu, Jing Yu Yang, and Ahmad Al Asady. 2023. A system justification theory of entrepreneurial attitudinal change during a crisis. *Entrepreneurship Theory and Practice* 47, 3 (2023), 893–923.

[43] Christoph Lutz, Christian Pieter Hoffmann, and Giulia Ranzini. 2020. Data capitalism and the user: An exploration of privacy cynicism in Germany. *New media & society* 22, 7 (2020), 1168–1187.

[44] Shrirang Mare, Logan Girvin, Franziska Roesner, and Tadayoshi Kohno. 2019. Consumer Smart Homes: Where We Are and Where We Need to Go. In *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications* (Santa Cruz, CA, USA) *(HotMobile '19)*. Association for Computing Machinery, New York, NY, USA, 117–122. https://doi.org/10.1145/3301293.3302371

[45] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proc. Priv. Enhancing Technol.* 2020, 2 (2020), 436–458.

[46] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You Just Can't Know about Everything": Privacy Perceptions of Smart Home Visitors. In *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia* (Essen, Germany) *(MUM '20)*. Association for Computing Machinery, New York, NY, USA, 83–95. https://doi.org/10.1145/3428361.3428464

[47] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376167

[48] Preben Mogensen. 1992. Towards a Provotyping Approach in Systems Development. *Scand. J. Inf. Syst.* 4, 1 (1992), 5.

[49] Adam D Moore. 2015. *Privacy rights: Moral and legal foundations*. Penn State Press.

[50] Aarthi Easwara Moorthy and Kim-Phuong L. Vu. 2015. Privacy Concerns for Use of Voice Activated Personal Assistant in the Public Space. *International Journal of Human–Computer Interaction* 31, 4 (2015), 307–335. https://doi.org/10.1080/10447318.2014.986642 arXiv:https://doi.org/10.1080/10447318.2014.986642

[51] Guillaume Nadon, Marcus Feilberg, Mathias Johansen, and Irina Shklovski. 2018. In the User We Trust: Unrealistic Expectations of Facebook's Privacy Mechanisms. In *Proceedings of the 9th International Conference on Social Media and Society* (Copenhagen, Denmark) *(SMSociety '18)*. Association for Computing Machinery, New York, NY, USA, 138–149. https://doi.org/10.1145/3217804.3217906

[52] Jaime L Napier, Anesu N Mandisodza, Susan M Andersen, and John T Jost. 2006. System justification in responding to the poor and displaced in the aftermath of Hurricane Katrina. *Analyses of social issues and public policy* 6, 1 (2006), 57–73.

[53] Helen Nissenbaum. 2009. Privacy in context. In *Privacy in Context*. Stanford University Press.

[54] Sandra Petronio. 2002. *Boundaries of privacy: Dialectics of disclosure*. Suny Press.

[55] James Pierce, Sarah Fox, Nick Merrill, and Richmond Wong. 2018. Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 139 (nov 2018), 24 pages. https://doi.org/10.1145/3274408

[56] Dimitrios Raptis, Rikke Hagensby Jensen, Jesper Kjeldskov, and Mikael B. Skov. 2017. Aesthetic, Functional and Conceptual Provocation in Research Through Design. In *Proceedings of the 2017 Conference on Designing Interactive Systems* (Edinburgh, United Kingdom) *(DIS '17)*. Association for Computing Machinery, New York, NY, USA, 29–41. https://doi.org/10.1145/3064663.3064739

[57] Jon Rogers, Loraine Clarke, Martin Skelly, Nick Taylor, Pete Thomas, Michelle Thorne, Solana Larsen, Katarzyna Odrozek, Julia Kloiber, Peter Bihr, Anab Jain, Jon Arden, and Max von Grafenstein. 2019. Our Friends Electric: Reflections on Advocacy and Design Research for the Voice Enabled Internet. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300344

[58] Alex Sciuto, Arnita Saini, Jodi Forlizzi, and Jason I. Hong. 2018. "Hey Alexa, What's Up?": A Mixed-Methods Studies of In-Home Conversational Agent Usage. In *Proceedings of the 2018 Designing Interactive Systems Conference* (Hong Kong, China) *(DIS '18)*. Association for Computing Machinery, New York, NY, USA, 857–868. https://doi.org/10.1145/3196709.3196772

[59] John S. Seberger, Marissel Llavore, Nicholas Nye Wyant, Irina Shklovski, and Sameer Patil. 2021. Empowering Resignation: There's an App for That. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 552, 18 pages. https://doi.org/10.1145/3411764.3445293

[60] John S. Seberger, Irina Shklovski, Emily Swiatek, and Sameer Patil. 2022. Still Creepy After All These Years:The Normalization of Affective Discomfort in App Use. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery,

New York, NY, USA, Article 159, 19 pages. https://doi.org/10.1145/3491102.3502112

[61] William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. 2020. Informing the Design of Privacy-Empowering Tools for the Connected Home. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376264

[62] William Seymour and Max Van Kleek. 2020. Does Siri Have a Soul? Exploring Voice Assistants Through Shinto Design Fictions. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3334480.3381809

[63] Sujay Shalawadi, Christopher Getschmann, Niels van Berkel, and Florian Echtler. 2024. Manual, Hybrid, and Automatic Privacy Covers for Smart Home Cameras. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference* (IT University of Copenhagen, Denmark) *(DIS '24)*. Association for Computing Machinery, New York, NY, USA, 3453–3470. https://doi.org/10.1145/3643834.3661569

[64] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2347–2356. https://doi.org/10.1145/2556288.2557421

[65] Michael Shorter, Bettina Minder, Jon Rogers, Matthias Baldauf, Aurelio Todisco, Sabine Junginger, Aysun Aytaç, and Patricia Wolf. 2022. Materialising the Immaterial: Provotyping to Explore Voice Assistant Complexities. In *Proceedings of the 2022 ACM Designing Interactive Systems Conference* (Virtual Event, Australia) *(DIS '22)*. Association for Computing Machinery, New York, NY, USA, 1512–1524. https://doi.org/10.1145/3532106.3533519

[66] Daniel J Solove. 2005. A taxonomy of privacy. *U. Pa. l. Rev.* 154 (2005), 477.

[67] Daniel J Solove. 2008. Understanding privacy. (2008).

[68] Daniel J Solove. 2012. Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.* 126 (2012), 1880.

[69] Daniel J Solove. 2021. The myth of the privacy paradox. *Geo. Wash. L. Rev.* 89 (2021), 1.

[70] Kevin M. Storer, Tejinder K. Judge, and Stacy M. Branham. 2020. "All in the Same Boat": Tradeoffs of Voice Assistant Ownership for Mixed-Visual-Ability Families. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376225

[71] Yolande Strengers and Jenny Kennedy. 2021. *The smart wife: Why Siri, Alexa, and other smart home devices need a feminist reboot.* Mit Press.

[72] Madiha Tabassum, Tomasz Kosiński, Alisa Frik, Nathan Malkin, Primal Wijesekera, Serge Egelman, and Heather Richter Lipford. 2020. Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 3, 4, Article 153 (sep 2020), 23 pages. https://doi.org/10.1145/3369807

[73] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. 2019. "I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 435–450. https://www.usenix.org/conference/soups2019/presentation/tabassum

[74] Nick Taylor, Jon Rogers, Loraine Clarke, Martin Skelly, Jayne Wallace, Pete Thomas, Babitha George, Romit Raj, Mike Shorter, and Michelle Thorne. 2021. Prototyping Things: Reflecting on Unreported Objects of Design Research for IoT. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference* (Virtual Event, USA) *(DIS '21)*. Association for Computing Machinery, New York, NY, USA, 1807–1816. https://doi.org/10.1145/3461778.3462037

[75] Christian Tiefenau, Maximilian Häring, Eva Gerlitz, and Emanuel von Zezschwitz. 2019. Making Privacy Graspable: Can we Nudge Users to use Privacy Enhancing Techniques? *arXiv preprint arXiv:1911.07701* (2019).

[76] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14)*. Association for Computing Machinery, New York, NY, USA, 129–139. https://doi.org/10.1145/2632048.2632107

[77] Jennifer M Urban and Chris Jay Hoofnagle. 2014. The privacy pragmatic as privacy vulnerable. In *Symposium on Usable Privacy and Security (SOUPS 2014) Workshop on Privacy Personas and Segmentation (PPS)*.

[78] Jojanneke Van der Toorn and John T Jost. 2014. Twenty years of system justification theory: Introduction to the special issue on "Ideology and system justification processes". , 413–419 pages.

[79] Rosa Van Koningsbruggen, Sujay Shalawadi, Eva Hornecker, and Florian Echtler. 2022. Frankie: Exploring How Self-Tracking Technologies Can Go from Data-Centred to Human-Centred. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia* (Lisbon, Portugal) *(MUM '22)*. Association for Computing Machinery, New York, NY, USA, 243–250. https://doi.org/10.1145/3568444.3568470

[80] Adeola Wale-Kolade and Peter Axel Nielsen. 2016. Apathy Towards the Integration of Usability Work: A Case of System Justification. *Interacting with Computers* 28, 4 (June 2016), 437–450. https://doi.org/10.1093/iwc/iwv016 _eprint: https://academic.oup.com/iwc/article-pdf/28/4/437/6771899/iwv016.pdf.

[81] Jayne Wallace, Jon Rogers, Michael Shorter, Pete Thomas, Martin Skelly, and Richard Cook. 2018. The SelfReflector: Design, IoT and the High Street. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3173574.3173997

[82] Alan F Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.

[83] Maximiliane Windl, Albrecht Schmidt, and Sebastian S. Feger. 2023. Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 70, 16 pages. https://doi.org/10.1145/3544548.3581167

[84] Sara Wolf, Benedikt Steinmüller, Frauke Mörike, Simon Luthe, and Jörn Hurtienne. 2023. The God-I-Box: Iteratively Provotyping Technology-Mediated Worship Services. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference* (Pittsburgh, PA, USA) *(DIS '23)*. Association for Computing Machinery, New York, NY, USA, 1710–1723. https://doi.org/10.1145/3563657.3596029

[85] Richmond Y. Wong, Jason Caleb Valdez, Ashten Alexander, Ariel Chiang, Olivia Quesada, and James Pierce. 2023. Broadening Privacy and Surveillance: Eliciting Interconnected Values with a Scenarios Workbook on Smart Home Cameras. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference* (<conf-loc>, <city>Pittsburgh</city>, <state>PA</state>, <country>USA</country>, </conf-loc>) *(DIS '23)*. Association for Computing Machinery, New York, NY, USA, 1093–1113. https://doi.org/10.1145/3563657.3596012

[86] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 59:1–59:24. https://doi.org/10.1145/3359161

[87] Jason C. Yip, Kiley Sobel, Xin Gao, Allison Marie Hishikawa, Alexis Lim, Laura Meng, Romaine Flor Ofiana, Justin Park, and Alexis Hiniker. 2019. Laughing is Scary, but Farting is Cute: A Conceptual Model of Children's Perspectives of Creepy Technologies. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300303

[88] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 159–176. https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

[89] Hui Zhang, Munmun De Choudhury, and Jonathan Grudin. 2014. Creepy but Inevitable? The Evolution of Social Networking. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Baltimore, Maryland, USA) *(CSCW '14)*. Association for Computing Machinery, New York, NY, USA, 368–378. https://doi.org/10.1145/2531602.2531685

[90] Shoshana Zuboff. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019.* Profile books.