Playing with Privacy: Exploring the Social Construction of Privacy Norms Through a Card Game

JENNY BERKHOLZ, University of Siegen, Germany
ANIQA RAHMAN, University of Siegen, Germany
GUNNAR STEVENS, University of Siegen, Germany and Bonn-Rhein-Sieg University of Applied Science, Germany

Investigating digital privacy behavior requires consideration of its contextual nuances and the underlying social norms. This study delves into users' joint articulation of such norms by probing their implicit assumptions and "common sense" surrounding privacy conventions. To achieve this, we introduce *Privacy Taboo*, a card game designed to serve as a playful breaching interview method, fostering discourse on unwritten privacy rules. Through nine interviews involving pairs of participants (n=18), we explore the decision-making and collective negotiation of privacy's vagueness. Our findings demonstrate individuals' ability to articulate their information needs when consenting to fictive data requests, even when contextual cues are limited. By shedding light on the social construction of privacy, this research contributes to a more comprehensive understanding of usable privacy, thereby facilitating the development of democratic privacy frameworks. Moreover, we posit *Privacy Taboo* as a versatile tool adaptable to diverse domains of application and research.

CCS Concepts: • **Security and privacy → Social aspects of security and privacy**; • **Human-centered computing → Collaborative and social computing theory, concepts and paradigms**.

Additional Key Words and Phrases: privacy, privacy judgments, privacy decisions, privacy order, privacy norms, card game, interview study, qualitative methods, negotiation, breaching experiment

ACM Reference Format:
Jenny Berkholz, Aniqa Rahman, and Gunnar Stevens. 2025. Playing with Privacy: Exploring the Social Construction of Privacy Norms Through a Card Game. *Proc. ACM Hum.-Comput. Interact.* 9, 1, Article GROUP23 (January 2025), 23 pages. https://doi.org/10.1145/3701202

1 INTRODUCTION

Digital privacy is a complex topic that has been well-researched for decades [16]. Several studies examine human privacy behavior and have revealed interesting phenomena such as the privacy paradox [28] or the privacy calculus model [9], which makes human behavior more explainable. While such approaches often assume humans as rationally acting beings, Nissenbaum provides the contextual integrity framework [45] to illuminate and analyze the deeper layers of information flow based on social norms beyond individual rationality. These norms are part of the social order and are continually shaped through ongoing negotiations [56]. We argue that privacy norms are the underlying principle behind the user's privacy decisions. Privacy norms are unwritten human core beliefs about privacy, which become apparent when articulating the privacy "common sense." Furthermore, like other norms, privacy norms are fluid. They are constituted and negotiated by social interaction. Yet, apart from studies on boundary regulations [41], research that addresses the

Authors' addresses: Jenny Berkholz, University of Siegen, Siegen, Germany, jenny.berkholz@uni-siegen.de; Aniqa Rahman, University of Siegen, Siegen, Germany, aniqa.rahman@student.uni-siegen.de; Gunnar Stevens, University of Siegen, Siegen, Germany and Bonn-Rhein-Sieg University of Applied Science, Sankt Augustin, Germany, gunnar.stevens@uni-siegen.de.

2573-0142/2025/1-ARTGROUP23
https://doi.org/10.1145/3701202

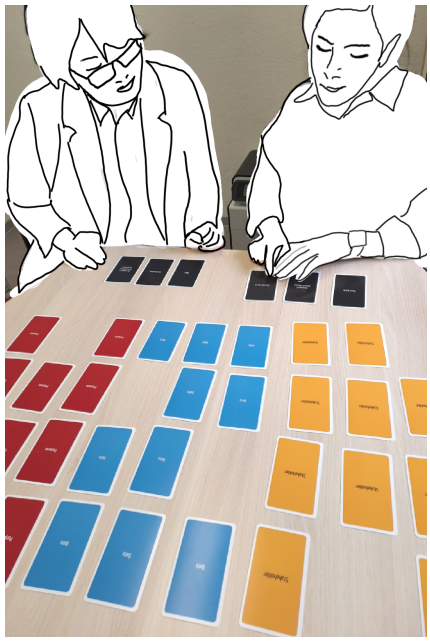

Fig. 1. This image captures a re-enacted interview scene featuring two individuals engaging in our card game, *Privacy Taboo*. The stylized depiction of the two participants conveys their discussion about the fictive scenario they have drawn (black cards). Spread out in front of them are additional cards, face down in yellow (stakeholder), blue (data), and red (purpose), yet to be explored.

joint negotiation process of privacy is scarce in Computer-Supported Cooperative Work (CSCW) and Human-Computer Interaction (HCI) research, with a few exceptions [22, 49]. Nevertheless, we demonstrate that research on digital privacy norms can contribute to a holistic understanding of usable privacy.

To understand these inherent privacy judgments, we draw inspiration from Garfinkel's significant work on breaching experiments, which uncover unwritten norms and rules by deliberately violating them [15]. We pursue a more fictitious and less invasive approach by adapting a playful framework through the creation of our card game *Privacy Taboo*. The game functions as a stimulus for conversation between the participants and an alternative interview method, absent of specific gamification guidelines or educational aims. Section 3.1 describes the rationale behind our design decisions, and section 3.2 provides a detailed description of the game's rules. In brief, *Privacy Taboo* operates as follows: it comprises three categories of cards – stakeholder, data, and purpose, of which the participants draw one card each. The combination of the three cards results in a scenario, for example: "A *Local charity organization* (stakeholder) requests your *Geolocation* (data) to *sell the data* (purpose)" (see figure 3). The participants mutually discuss their thoughts and feelings about the drawn scenario and describe whether they would consent to sharing their personal information. In each round, participants exchange one card to draw different combinations. With this study design, we aim to find out about the tacit distinctions in decision-making to answer our research question *How do people negotiate digital privacy norms based on our card game?*

Through this approach, we recognized that the participants negotiated the vagueness of privacy norms collectively, for example, by pointing out certain doubts to each other or sharing personal

Fig. 2. This image shows the back side of three cards, each from one of the decks. The yellow card contains the term *Stakeholder*, the blue card has the inscription *Data*, next to the red card labeled *Purpose*.

Fig. 3. This image shows the front side of three cards, each from one of the decks. The first card from the stakeholder deck shows *Local charity organization*, the second card shows the data *Geolocation*, and the last one is labeled *to sell the data* as a purpose.

experiences from the past. We also found that a certain "gut feeling" was significant for decision-making, which is an intriguing factor for embodied knowledge [39], a manifestation of norms. Further, participants precisely articulated their information needs, and the majority could make reflected decisions, even though the three cards provided limited context or depicted less anticipated scenarios or more dystopian ones [59].

Overall, this study presents a card game method that is transferable to different application fields of HCI and CSCW research and can contribute to a greater understanding of underlying norms and rules. It playfully encourages participants to articulate the subtle differences in decisions, which ultimately fosters the comprehension of the social construction of privacy more deeply. Furthermore, we indicate that citizen assemblies are a democratized venue for privacy debates and negotiations to address power imbalances. This study contributes to a holistic understanding of usable privacy, transferring design implications for personal information management systems (PIMS).

In the following, we investigate the state of the art regarding digital privacy and norm negotiation, describing our methodology, presenting our findings, and discussing them. This is followed by limitations, future work, and a conclusion.

2 STATE OF THE ART

In HCI and CSCW research, the design and understanding of usable privacy and security are essential and well-researched areas [16]. However, privacy has a long research tradition outside the digital world by legal, social, and political scholars [55]. Formerly, privacy was defined as early as 1890 by Warren and Brandeis as "the right to be let alone" [29]. This definition is still relevant, but a lot has changed socially and technologically since then. As a result, definitions of privacy face challenges amid the constantly evolving digital landscape and emerging phenomena that continually shift boundaries. The legal and scientific communities continuously redefine privacy, a process shaped by testing the boundaries of what is deemed appropriate, thereby contributing to the fabric of social order and norms. The following two chapters address the various theories and approaches around digital privacy and norms.

2.1 Digital Privacy

In the 1960s, Westin [62] identified different privacy functions and states, considering the inherent challenges and consequences of technologies and their surveillance potential. Furthermore, he elaborated on the underlying societal norms of privacy by considering privacy an inherent human right that depends on the society and culture in which one lives. He writes that individuals are continually engaged in a personal adjustment process to balance the desire for privacy and disclosure to others against the background of social norms set by the society in which they live [62]. His theory was followed by Altman's privacy regulation theory [2], which dealt with the social sphere of boundary control between individuals and how they conceal and disclose their information to each other. Altman wrote that privacy is, among other things, a dynamic and fluid process of constant regulation. While Westin and Altman's theories describe initial approaches regarding surveillance through technologies, later work such as that of Solove [55] clearly outlines the abusive forms of information processing, information dissemination, and invasion. However, many approaches stick to paradigms, which place the individual in the foreground rather than a symbiotic relationship between the individual and society. Similarly, this applies to the privacy calculus model [9]. This model demonstrates that people base their actions on rational and profit-oriented considerations. They showed that people weigh the advantages and disadvantages of a particular privacy action against each other and decide according to their interests, even if this decision may eventually be harmful to their privacy. In this context, individuals are acting in terms of a homo oeconomicus [17]. A concrete example of such a case is the use of privacy-infringing messenger apps. According to the model, a person willingly uses a messenger app with privacy deficiencies when their close contacts use it since the benefit of having contact with friends outweighs the privacy weakness [17]. This approach aligns with the privacy paradox [28], which describes the paradoxical behavior of people caring about their privacy but acting the opposite.

Conversely, Nissenbaum follows an alternative approach to capture social facets beyond rationality with her contextual integrity (CI) framework. She provides a structure for analyzing privacy as embedded and dependent on contextual social norms. She argues that within a particular social context, privacy entails an *appropriate flow of information* governed by norms [53]. Hence, privacy is not defined as minimizing or preventing data flow. Rather, it is determined by whether data transmission between the actors is deemed appropriate [45, 53]. Context-relative informational norms are an integral aspect of the CI framework and are constituted of four parameters: *(1) context, (2) actors, (3) attributes, and (4) transmission* [45]. However, Nissenbaum explains that "when we mind that information about us is shared, we mind not simply that it is being shared but that it is shared in the wrong ways and with inappropriate others. Although most of the time these requirements are tacit and the states of all parameters need not be tediously spelled out, in controversial cases,

elliptical expressions of people's expectations can be taken too literally and serve as sources of common misunderstandings" [45]. This statement is an interesting argument for our study since we create scenarios based on three elements: stakeholder, data, and purpose, which are the usual information users encounter when confronted, e.g., with cookie banners. Therefore, we expand the CI approach by broadening the view of joint social negotiation of implicit social rules and their articulation without taking them "too literally". In the following section, we will elaborate on the previous terminology.

2.2 Negotiation and Social Norms

In technology-related research, the development of privacy norms [22, 49] has been rarely investigated. However, negotiation overall is commonly discussed in connection to boundary work [30], as in Mols and Pridmore [41]. They researched spouses' "boundary-sculpting practices" around the disclosure of the blue check mark in WhatsApp and how they negotiate interpersonal rules. Again, the context dependency mentioned before is of immense importance for boundary-sculpting, for example, by regulating professional and personal life boundaries [44]. Furthermore, Tene and Polonetsky [60] highlight the importance of context and appropriateness for technologies by investigating how certain features embedded in a specific context become "creepy" and thereby shift social norms. They describe that the 2012 app "Girls Around Me" gained significant criticism by displaying the location and information of "girls" who were in a user's geographical vicinity and logged into their social networks. At that time, however, the app legally did not violate any regulations since the surface data was publicly available. Still, the context made this app "creepy" and disrupted the social norms. Later, major social networks removed the app from their APIs. The authors describe that "it was not illegal; it was distasteful" [60]. This example clearly illustrates how the public discourse has shaped the norm by categorizing it as inappropriate. McDonald and Crandall [38] point out that norms are flexible and behavior change can occur from changes in norms without changing individual beliefs. Individuals can also rebel against norms and regulations and thus change social structures and culture, as these are impermanent [38]. Rebellion, in particular, can be very exciting to investigate concerning power imbalances between users and platforms [4, 40]. Although Goffman [19] did not yet consider the negotiation of norms in this way, his studies were also concerned with the relationships between the oppressed and the oppressor in total institutions and their negotiations of balancing constraint and freedom.

In the humanities, the negotiation of social order and norms has been addressed particularly by Strauss [56], who states that social worlds are mutually constituted in negotiations taking place in arenas [56, 57]. Negotiations re-frame the subject and power in their more fluid and discursive forms [14]. Similarly, Garfinkel [15] considers that breaching the social norm makes them visible. He states that norms could be articulated by analyzing how others react to a sudden break of social norms and further ethnographic reflection. Therefore, he instructed breaching experiments; one experiment included revealing a hidden tape recorder after a private conversation. The reaction of the counterpart then illustrated the social norm, arguing that it was a breach of trust and that one should inform someone about recording a conversation beforehand [15].

We incorporate the aforementioned ideas into our study and emphasize that privacy is a fluid concept, subject to negotiation, and follows unwritten rules. It is embedded within contexts that render certain actions appropriate or inappropriate. To make these underlying norms visible, they must be breached and can be reflected upon through their articulation. Therefore, similar to Garfinkel [15], we aim to breach situations. We do this based on fictitious scenarios created through cards to protect the participants without harming their actual privacy. In the following section, we will explain our card game design process and the methodology of our study design.

3 METHODOLOGY

3.1 Card Game Design Process

Aiming to design a card game as a playful version of a breaching experiment, the authors brainstormed how such a game could be structured. We then decided on the categories of stakeholder, data, and purpose since users encounter this information when confronted with cookie banners or when downloading an app. To determine the cards' content, we drew from our everyday experiences and collectively compiled stakeholders, the data they requested, and their stated purposes. Additionally, we gathered folk theories [54] that we encountered in conversations with friends and family and in public discourse. We must highlight that this procedure was rather an auto-ethnographic approach [50] based on the authors' experiences than a standardized empirical survey. However, with this approach, we pursue an initial exploratory approach close to users' everyday experiences.

Our compilation resulted in a diverse collection of stakeholders, ranging from trivial entities like "A family member" to companies (e.g., Netflix) and public institutions (e.g., the government). For the data, we included personal information (e.g., home address) and technological access requests (e.g., access to your microphone), acknowledging that the latter category is not data per definition but is counted under the umbrella term *data* in this study. Furthermore, we decided to use similarly vague terminology, as found with cookie banners, that just shows a broad purpose (e.g., advertisement purpose) without specifying how they utilize the data [31]. Additionally, we included a more provocative card gathered from folk theories [54] suggesting that stakeholders might disclose personal data to the Secret Services and one card that does not specify the purpose, prompting participants to speculate about it.

After careful joint discussion, we settled on 12 cards per category, resulting in a total of 36 cards (for an overview see table 1). We then created and printed the deck using a card manufacturer's website. It is essential to emphasize that this game is not structured according to a win-or-lose scheme but is solely aimed at stimulating reflective conversation about privacy practices and articulating norms. Therefore, we do not adhere to scientific gamification principles; the material structure solely resembles a typical card game. However, there is significant scientific work on card games for educating and raising awareness of digital privacy and its design [26, 32, 51].

Following the aforementioned considerations, we established the game's rules by testing different variants until agreeing on the final form. To capture the subtle distinctions in people's privacy judgments, we decided to let participants exchange the different categories one by one to make assumptions about the different effects on people's attitudes. Furthermore, we determined the number of participants. As we aimed to gain insights into the joint negotiation of privacy norms, we concluded that two people per play, or interviews, would be optimal since individual participants would not have a discussion partner. More than two participants could result in an overwhelming and less intimate setting, eventhough it would be possible [5, 42].

It is important to emphasize that the scenarios drawn with the cards are sometimes dystopian, nonsensical, or rather unanticipated. This is not a weakness, but we find these scenarios particularly intriguing. Such borderline cases stimulate personal reflection, elicit judgments differently, and encourage an articulation of the underlying norms. We want to highlight that integrating hypothetical scenarios is a solid approach to avoid exposing people to certain privacy risks [10, 11]. Therefore, we have established the following rules, which allow for playing similar scenarios in constantly changing combinations; for a visual representation, see figure 4.

3.2 *Privacy Taboo* Rules

The researcher shuffles the cards and arranges them by evenly spreading them from the deck into stakeholder, data, and purpose categories (as illustrated in Figure 1). They explain the rules to the

Table 1. This table provides an overview of the content of the 36 different cards in *Privacy Taboo*. The cards are divided into three categories: stakeholder, data, and purpose, each containing twelve cards. The cards have been shuffled after every session. The order presented here is randomly selected and was not the initial order of the game.

Stakeholder	Data	Purpose
A family member	Your browser history	to optimize functionality
Facebook (Meta)	Access to your webcam	to give you a 5 percent discount
The government	Access to your microphone	to store the data
ChatGPT (OpenAI)	Access to your contact list	to train an AI
Your insurance	Images in your gallery	for crime prevention
The university	Geolocation	to sell the data
Amazon	Bank account status	to understand you better
Netflix	Your smartphone's type	Advertisement
Uber	Your home address	to create a personalized experience
Local charity organization	Social media handle	to send to the Secret Service
Food delivery service	Health data	it is mandatory to use the service
Your bank	Relationship status	What do you think is the reason?

participants and address any remaining questions participants may have. The card game proceeds as follows:

- **Setup**: Each participant draws one card from each category (stakeholder, data, purpose) and places them face-up on the table in the same order as stakeholder, data, and purpose. Meaning that each of the two participants has three cards in front of them, resulting in six cards in total.
- **Scenario Discussion**: The researcher reads the drawn scenarios aloud and initiates a discussion by asking questions about the combinations, starting with one scenario and then the other. The opening question is always "How does this combination make you feel?", to stimulate an open discussion, followed by spontaneous questions and turn-takings between the participants. The closing question is always "Would you finally consent to this request?" Both participants have to answer the questions about both scenarios. During the discussion phase, participants share their thoughts and feelings about the scenarios or talk about personal experiences. This discussion does not need to follow a strict structure (e.g., Person A speaks first, then Person B) but can flow more naturally as a conversation.
- **New Stakeholder Card**: Participants draw and place a new stakeholder card on top of the previous one. The researcher reads the new scenario and prompts discussion, focusing on how the scenario has changed by introducing the new card. Again following the opening and closing questions.
- **Revealing Former Stakeholder, Drawing New Data**: Participants remove the previously drawn stakeholder card to reveal the former one from the first scenario. They put the second stakeholder card aside, as it is not needed anymore. Then, they draw a new data card to put on top of the former one. The researcher again facilitates discussion by asking questions and encouraging participants to share personal examples or ideas.
- **Revealing Former Data, Drawing New Purpose**: Continuing from the previous steps, participants remove the previously drawn data card to reveal the former one. Then, they draw a new purpose card. The researcher guides discussion similar to earlier steps.

- **Bonus Round (Optional)**: If participants desire an additional round with new cards, they can remove the *old* cards to the side and draw a new set of three cards. They continue the same discussion pattern as in the other scenarios.

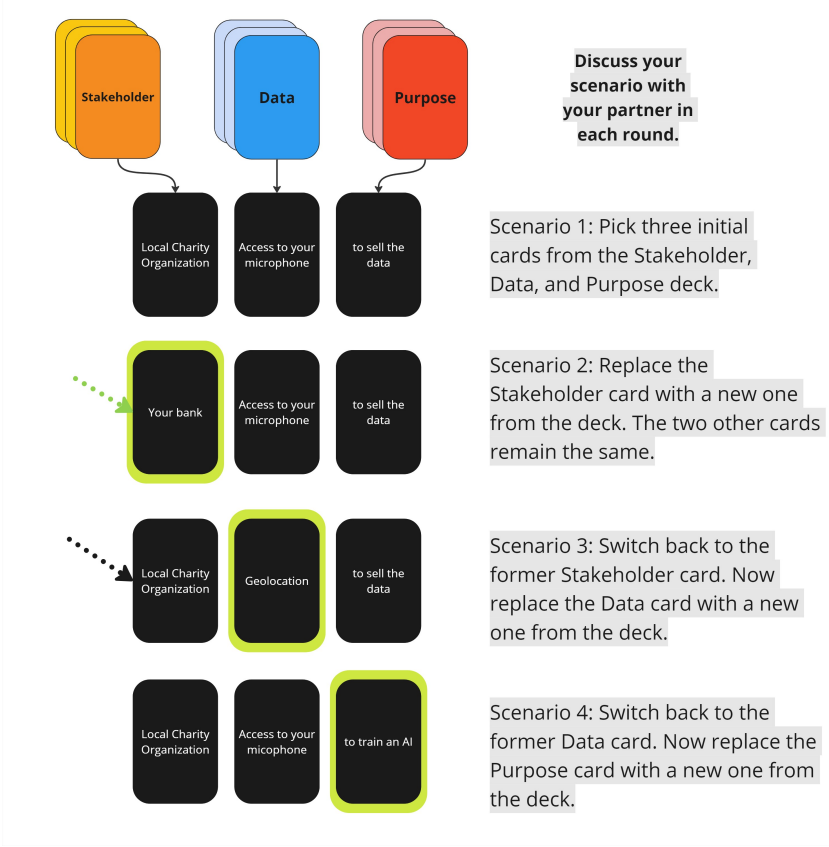

Fig. 4. This figure illustrates the rules of *Privacy Taboo*. At the top are the three decks of cards: stakeholder, data, and purpose. Below them are the four different steps, representing scenarios, that the participants follow. For the first scenario, the participant selects one card from each deck (demonstrated here as *Local charity organization – Access to your microphone – to sell the data*). In the second step, the participant replaces the initial stakeholder card with a new one from the deck (indicated with a green background). The other two cards remain the same, resulting in an example scenario of *Your bank – Access to your microphone – to sell the data*. For Scenario 3, the participant returns the former stakeholder card (*Local charity organization*, and discards *Your bank*). Then, they replace the data card with a new one from the deck, resulting in an exemplified scenario of a *Local charity organization – Geolocation – to sell the data*. Finally, for Scenario 4, the participants return the former data card and replace the purpose card with a new one from the deck (*Local charity organization – Access to your microphone – to train an AI*). Each participant follows this procedure so that two scenarios are discussed mutually in each round. The researcher stimulates the discussion between participants about the two scenarios in each step.

3.3 Recruitment of Participants and Interview

We determined that the primary target audience for this game is laypeople who regularly use the internet. Yet, we also envision that individuals with lower digital literacy and vulnerable groups

benefit from reflecting on their data through the card game under the guidance of an expert. Therefore, our recruitment targeted persons without extensive expertise in usable security or privacy, ensuring that technical background knowledge did not heavily influence their privacy attitudes. Yet, we required them to have a certain level of digital experience, such as regular smartphone use. Since we did not pursue an educational purpose, we had no further exclusion criteria, as data privacy and confidentiality concern everyone.

Furthermore, our goal was to recruit 18 participants to achieve initial saturation. This was confirmed during the course of conducting the interviews, as patterns began to emerge after approximately five interviews. We launched a public social media call announcing a scientific interview study, including a card game concerning digital privacy. Then, we scheduled appointments with the people who contacted us. Some participants brought someone they knew to the meeting, such as their flatmates or spouses. For those who did not bring someone, we arranged pairs and asked for their consent to interview them with an unfamiliar person. The rationale behind this was to observe if there were differences in the negotiation process depending on the participants' familiarity. This resulted in interviews with people who knew each other very well (interviews 1, 4, 5, 7, and 9) and those who barely knew each other or not at all (interviews 2, 3, and 8). We conducted 9 interviews with two people each, resulting in the IDs P1-P18 (see Table 2). The audio recordings of the interviews totaled 08:18:07 hours, meaning the interviews lasted an average of 55 minutes. All participants agreed to audio recording, transcription, and publication of written excerpts of the sessions. They received compensation of 10 Euros for their participation, which is in line with the ethical requirements of our home university. The anonymized transcripts were saved on a GDPR-compliant server verified by the university.

Before and after conducting the game, we had a pre- and post-interview phase. In the pre-phase, we introduced ourselves and the participants to each other in cases where they did not know each other. We introduced the game and asked some ice-breaker questions, such as their thoughts on data protection overall and their views on cookie banners, to create a relaxed atmosphere and sensitize them to the topic. Furthermore, we asked the participants to engage in discussions respectfully and to refrain from harshly judging others' privacy choices. After playing the game, in our post-interview phase, we asked the participants about their impressions of the game and whether they had any unanswered questions or feedback. We also emphasized the importance of data protection if we noticed during the game that they seemed too lax with their permissions and informed them about various privacy practices from our research on this topic. Nevertheless, our study does not claim to be educational, although we have endeavored to educate the participants to the best of our ability.

3.4 Analysis Procedure

We employed a thematic analysis of the transcripts to interpret our dataset, as outlined by Braun and Clarke [8]. To ascertain open-ended insights from the data, we embarked on the grounded approach [58]. Initially, the primary interviewer presented the key findings to the remaining authors, outlining notable differences, similarities, and overarching impressions gleaned from the nine interviews. Subsequently, two authors independently coded the transcripts using MAXQDA software, engaging in iterative discussions to reconcile similar codes and identify overarching themes collaboratively. This process underwent refinement through two additional sessions to solidify the identified themes.

In parallel, we conducted a quantitative examination of the various combinations during a dedicated session to ensure that we did not overlook significant insights. However, it's essential to underscore our primary aim of investigating tacit human attitudes so that a qualitative evaluation is more fitting than a quantitative approach. While we did play through 67 combinations, a quantitative

Table 2. This table presents detailed information about our 18 participants, including the number of interviews (1-9), their ID (P1-P18), age (ranging from 21 to 57), gender (10 female/8 male), occupation (e.g., employee), and their relationship with each other (e.g., married couple).

Interview	ID	Age	Gender	Occupation	Relationship
1	P1	23	f	student and employee	co-workers and friends
	P2	24	f	employee	
2	P3	30	m	employee	strangers
	P4	33	f	employee	
3	P5	28	m	employee	acquaintance
	P6	25	f	employee	
4	P7	32	m	photographer	married couple
	P8	27	f	teacher	
5	P9	29	m	employee	couple
	P10	31	f	employee	
6	P11	30	m	employee	friends
	P12	21	f	journalist	
7	P13	57	m	employee	married couple
	P14	54	f	employee	
8	P15	28	m	student	strangers
	P16	27	m	employee	
9	P17	30	f	student	flatmates
	P18	24	f	student	

evaluation would be plausible. However, we saw that a quantitative lens could not uncover the "hidden" assumptions surrounding individuals' privacy.

The themes we identified through our thematic analysis are further expounded upon in Chapter 4, wherein the sub-chapters are named after the main themes.

4 FINDINGS

4.1 Decision-Making

Overall, we noted a distinct dualism between the considerations of functional-technological aspects and emotionally driven factors in the decision-making process. Through our observations, we discerned an interplay of different influences shaping participants' decisions, beyond singular reasons.

Some participants displayed a strong inclination towards assessing the technological merits of the request, granting consent only if it offered tangible, functional benefits. Initially, these individuals expressed skepticism towards the game, noting potential deviations from their real-life decision-making due to time constraints when downloading apps or browsing websites. We then highlighted that our game serves as a platform to explore decision-making beyond time pressure constraints to investigate the multifaceted factors at play in privacy-related choices. During the study, it emerged multiple times that individuals generally desire more time for decision-making in their everyday lives. For instance, during Interview 1, participants discussed a delaying boundary practice where, in a dating context, they preferred disclosing their Instagram username over their phone number to a stranger. This strategy afforded them time and physical distance to evaluate their interest in the person and control profile access. Similarly, we observed that timely stress levels outside the game significantly influenced the decision-making process. As articulated by

P14, it causes her stress to use her smartphone or download an app, which can lead her to hasty decision-making without thorough consideration of privacy implications.

4.1.1 Gut Feeling. Overall, participants expressed a desire for more information about the requests in many scenarios, although less frequently than we expected based on the CI framework [45]. When they did seek additional contextual information, we inquired about the specific information they sought to make a decision and how they envisioned a scenario with richer context. They often mentioned consulting the stakeholder's website or seeking advice from friends and family who may have had similar experiences. However, we observed that the reasons for accepting or declining a request were often rooted more in an intuitive, embodied knowledge [39], such as "gut feeling" which we interpret as a "competence-to-act" [18]. Nevertheless, there were instances where they consciously went against their intuitive gut feelings, which was unexpected, especially since we discussed fictional scenarios without real consequences. This suggests that participants took the game seriously and aimed to respond realistically. For example, P13's response to a scenario where the university requested his social media handle was revealing: "I would probably agree with a bad gut feeling..." (P13). He consented because, for him, the university was a trustworthy stakeholder. Similarly, P5 consented to a scenario involving ChatGPT despite feeling a "stomach ache," as he relied on the service regularly and was unwilling to give it up.

4.1.2 Resignation. This action against their intuition also led to feelings of resignation and frustration, evident in the participants' arguments. The feeling of powerlessness among users emerged as a prominent theme, with some expressing sentiments such as feeling "transparent; everyone knows what they want to know anyway" (P3). Many felt they had no real freedom of choice, leading to responses like "take everything and leave me alone" (P2). P5 provided a more detailed explanation when discussing a scenario where the university requested webcam access, despite his discomfort: "Of course, I would allow it. You swallow the bitter pill even if you're not in favor of it, but then the higher power is the university, and then you say yes...then that's secondary" (P5). The metaphor of swallowing a "bitter pill" highlights the internal conflict participants faced when acting against their own preferences. Similarly, with the stakeholder card "Uber", we observed instances where the urgency of using a service, especially late at night, compelled individuals to accept requests they were uncomfortable with. Additionally, there was a notable skepticism about refusing requests from the government, as many assumed that they obtained their data "anyhow" regardless of their consent (P11).

4.1.3 Rebellion. In contrast to this sense of resignation, we also observed users' attempts to reclaim their autonomy by expressing rebellion or defiance when faced with certain scenarios. For instance, when presented with a request from Netflix for access to their phone gallery, one participant's response was simply "screw them" (P16). We noted that requests for access to images seemed to breach a taboo, eliciting immediate and unhesitating reactions from participants. This sentiment was echoed by P15 in this scenario, who explicitly stated that he would switch to another provider in response to such a request, underscoring the power disparity between users and major platforms. Similarly, when confronted with a request from the university for access to images, another participant expressed strong feelings using an offensive tone in German: "I would then revolt and choose the path of confrontation; what the hell is the university doing with my images in the gallery? I would challenge the ethics committee on what that is supposed to be for. Then I would look for an alternative" (P5). Interestingly, in a previous scenario P5 had indicated discomfort when the university requested access to his webcam. This suggests that the request for access to "images in the gallery" represents a threshold violation, being an "intrusion into the soul" (P5). We explore the themes of rebellion and power imbalances more deeply in section 4.4.2.

4.1.4 Fear and Precaution. Another prominent theme we identified is decision-making based on fear, particularly fear of negative consequences or misinterpretations stemming from the data provided. This fear was notably evident when participants drew the government as a stakeholder or in any combination with the card "Images in your gallery." For example, P13 approached these scenarios cautiously, noting that images can carry different meanings when taken out of context. He further expressed concern about memes in his gallery that he disagrees with but were sent to him, fearing they may be misconstrued as his own views. This apprehension was exacerbated when combined with the purpose card "to understand you better," leaving many participants feeling uneasy. In contrast, we also observed instances where skepticism or fear were lacking where they might have been warranted. For instance, P2 expressed no concerns about sharing her geolocation with a Secret Service, stating she had "nothing to hide" (P2). While we did not intervene during the interview, we addressed data protection concerns in the post-interview phase to raise awareness among participants. Moreover, we noted uncertainty triggered by the cards "to train an AI" and "ChatGPT", as participants struggled to assess the implications caused by the technology's novelty. This highlights the evolving nature of privacy norms in regard to AI, which are still in development, and individuals are undergoing an adjustment process [62].

4.1.5 Confusion and Curiosity. Some prompts confused the participants, such as the uncommon combination of "*Food delivery service* requests *Social media handle* for *crime prevention*," being a less anticipated, dystopian scenario under German regulations. Interestingly, P2 accepted this request out of confusion, as she stated. This observation is intriguing because the game does not impose any compulsion to accept a request. Thus, she imagined herself in such a scenario and aimed to provide a realistic response. However, confusion was a relatively rare occurrence, and in most cases, the participants understood the context well enough to provide an informed decision.

Participants were also occasionally puzzled by the terminology of the data card "Your smartphone's type," but after we clarified its meaning in terms of brand and model, most found it to be less intrusive than other data. During the post-interview reflection, we emphasized that such data could also be critical in examining personal information. Furthermore, the "Relationship status" card frequently sparked confusion but piqued curiosity. Compared to other data, it initially appears not commonly requested in everyday life, even though this is highly dependent on the cultural and governmental environment in which one lives. However, P2 and P9 sometimes gave approval to a request out of curiosity, to see how a platform or algorithm could utilize certain information.

4.1.6 Role Conflict. Furthermore, the participants were aware of their conflicting roles in both personal and professional contexts. For instance, P16 explained that he would consent to access contacts in many scenarios as a private individual but not in a work context. He mentioned having numerous work-related contacts stored on his company cell phone, which he would not be willing to share. This statement vividly illustrates the distinction between norms in different contexts. Additionally, we observed that the participants' professions significantly influenced their evaluation of the scenarios. For example, P7, speaking from his perspective as a professional photographer, discussed the potential publication of his work, while P1 mentioned that certain combinations could be intriguing for marketing purposes for her company, even if she herself would not agree to them in her private capacity.

The somewhat unusual stakeholder card "A family member" prompted discussions about the various roles individuals assume within a family. As we were unaware of the family circumstances of the participants, we kept this card intentionally generic, allowing participants to select a specific family member by themselves. Most opted for a parent. The discussions about role changes as a son or daughter were particularly interesting in this context. However, there were limits to the trust placed in family members, for instance in combination with the access to the webcam only under

conditions that they would tell them the time when they access it. Despite somewhat unreasonable scenarios (e.g., Grandmother wants to train an AI), the family card was generally viewed as amusing and showed an overall trust for this stakeholder.

4.2 Deliberation Process

In addition to scenarios where participants could quickly determine whether or not to consent, most cases involved a deliberation process. Oftentimes, a dilemma arises when the purpose behind a request seems altruistic, as seen in the context of health data. Participants frequently debated whether sharing health data for medical purposes, such as cancer research, could benefit others. However, concerns about potential discrimination also surfaced, particularly evident in interview 4. For example, discussions revolved around whether the analysis of health data by entities like the university could enhance accessibility or lead to discrimination. Ultimately, opinions on such scenarios were mixed, indicating that an apparently "good cause" alone was insufficient to justify sharing personal data. Participants expected high credibility from certain stakeholders, such as "Local charity organizations", and preferred to share only anonymous data.

Another purpose that underwent significant scrutiny was crime prevention. While participants recognized the ostensibly positive intention, they expressed apprehension about the potential negative consequences of sharing their data. They emphasized the importance of context in making their final decision and typically opted not to consent to crime prevention scenarios. Humorous comments and anecdotes, such as accidentally purchasing items associated with a crime and subsequent arrest, were common during discussions.

Privacy calculus [9] and deliberation also played a role, particularly with the purpose card "to give you a 5 percent discount." Some participants even used calculator apps to assess the potential savings, e.g., on their insurance premiums. However, many participants desired a higher discount percentage before consenting. Surprisingly, participants often expected to receive a portion of the profits from the platforms or institutions when drawing the purpose card "to sell the data," although this expectation is not true to life. Thus, they weighed the potential monetary gain against the perceived risks, demonstrating a rational economic approach to decision-making [9, 17].

4.2.1 Transmission to Third Parties. In particular, the data cards "Images in your gallery" and "Access to your contact list" sparked lively discussions concerning sharing others' data. For instance, some participants initially overlooked the fact that granting access to their contact list also meant disclosing the data of family and friends, such as when downloading an app. In such instances, one participant often alerted their partner to this concern, leading to a shocked reaction upon realization. They expressed feelings of shame and embarrassment, especially upon recognizing they may have inadvertently shared friends' and family members' data previously, assuming a sense of guilt. These intense feelings of shame underscored a deeply ingrained social norm against sharing others' data, portraying it as socially discouraged or taboo.

Similar dynamics emerged with the data category "Images in your gallery," as participants swiftly changed their decision when their game partners reminded them that granting access means also exposing photos of other individuals and bystanders. This prompted them to retract their fictive consent. This phenomenon aligns with Nissenbaum's CI Framework, which emphasizes the significance of sharing data with third parties [45].

In most cases, granting access to the contact list was rejected, except when combined with the purpose "to create a personalized experience." Participants explained that many social media apps require access to the contact list to facilitate connections with real contacts, prioritizing functionality over privacy concerns.

A contrasting perspective on data sharing was evident in P14's approach, who felt guilty when refusing cookies or other requests on a platform where she was a user. She viewed data sharing as an exchange, where she provides her data in return for the platform's service. This perspective aligns with a Mauss'ian logic of gifting [37]. For her, her data holds a specific value that is interesting for others. Unlike others who experienced frustration, anxiety, or feeling overwhelmed, P14 assumed guilt and responsibility in the "gifting" process, attributing agency to the stakeholder.

4.2.2 Advertisement. Another intriguing point that emerged, not only explicitly discussed in the context of the "Advertisement" purpose card but recurring throughout all interviews, was the trade-off between personalized and non-personalized advertising. While some participants viewed personalized advertising as "good" and desirable, others found it "creepy," expressing discomfort with algorithms knowing them too well (P9), and therefore preferring to reject such requests. We observed that personalized advertising walks a fine line, easily transitioning from being perceived as helpful to intrusive surveillance. For instance, P1 described geolocation-based customized advertising as hitting a pain point. Furthermore, advertisement was cited as a probable reason when participants drew the purpose card: "What do you think is the reason?" This suggests a tacit acceptance of advertising as a legitimate reason for data collection. Overall, while advertising as a purpose falls within social norms, a delicate balance exists, as illustrated by the fine line participants perceived in the context of personalized advertising.

4.3 Mediation and Trust through Public Discourses

During the study, we observed the significant influence of various intermediaries on social norms, as participants frequently cited them in their explanations. They primarily referenced movies, documentaries, and media reports, which led us to infer that these sources contribute to the construction of social norms, aligning with Bourdieu's concept of taste-makers [7, 34].

For instance, after drawing the "Uber" stakeholder card, P2 mentioned a movie she had watched about a "fake Uber driver," using it to justify her skepticism and refusal to consent. Furthermore, we noted that, with the "Uber" card, the request was often associated directly with an individual, namely the driver, rather than the company itself. This suggested that different standards applied here compared to, for example, Amazon. While participants theoretically interact with individuals through Amazon's delivery service, their argumentation focused more on the company itself. Nonetheless, participants perceived faceless entities or AI accessing their data as equally threatening. This phenomenon demonstrated a form of personification of the technology [43], although not as direct as with Uber drivers. Moreover, we found that participants were willing to give large companies like Amazon the benefit of the doubt. They believed these companies adhered to social norms, assuming they would not risk a public scandal by misusing data, as it would tarnish their reputation (P16).

Additionally, peer groups and social networks served as mediators of privacy norms. For instance, P2's teacher advised her to be careful with personal images on the internet due to potential misuse by others. Family and friends also played a significant role, as participants recounted anecdotes from them to justify their reasoning. For example, P17 described how she handles data protection topics carefully, considering herself "old-fashioned." When we asked her to clarify what she means by "old-fashioned," she explained that she learned from her mother to be cautious with her personal information and considers it to be not up-to-date anymore due to the integration of social media in her everyday life.

4.4 Negotiation of Social Norms

Another major element within the framework of collaborative creation and reinforcement of social norms was negotiation, which took place on multiple levels. Firstly, negotiation occurred between the participants themselves as they collectively navigated the boundaries of what is considered acceptable. Secondly, negotiation was evident between participants and platforms, aimed at addressing power imbalances and devising coping strategies.

4.4.1 Mutual Reflection. It was intriguing to observe how participants recognized differences in their interpretations of the scenarios and then discussed them until they achieved mutual understanding. This phenomenon was particularly noticeable among individuals familiar with each other, as they also engaged in mutual correction. For instance, in interview 1, P1 stated that she had disabled location sharing on her phone and would decline the request for geolocation in a drawn scenario. However, P2 interjected, pointing out that she always had her geolocation activated, as they both use a tracking app to monitor their safe arrival home in the evening. "P1: [...] I've turned that off everywhere. So, I definitely wouldn't agree. P2: Um, may I interrupt? That's not true. I can see where you are all the time [...]." This exchange prompted P1 to realize that the mental model of her privacy practices was inaccurate. A similar interaction occurred between P7 and P8, who reminded each other that they had activated the microphone necessary for recording Instagram stories, although they were not consciously aware of it. Even participants who were not acquainted with each other pointed out gaps in each other's knowledge; for example, P4 was unaware that the Meta stakeholder card also encompassed the use of Instagram. Participants often reconsidered their initial opinions after these discussions, exchanges, and negotiations. At times, it was explicitly expressed that there was still uncertainty, and they remained open to the arguments of others, as seen in P10's response to P9: "But maybe you can still change my mind, depending on what you say." Most norm negotiations occurred within these interpersonal interactions and reflective processes. Additionally, we observed boundary work [41] through coping strategies employed by participants when interacting with major platforms [40].

4.4.2 Coping with Power Imbalances. "If they don't want to disclose what they need my data for because they think I would say 'no' – I'll probably refuse anyway." (P7). As discussed earlier, this quote effectively captures the defiance and protest exhibited by the participants, showcasing their response to opaque data requests. Moreover, when confronted with power imbalances based on dependency on the platforms, participants emphasized their everyday privacy protection practices, such as covering their webcam [33]. Thus, when confronted with the data card "Access to your webcam," the predominant response was that they would accept it under the condition of covering the camera. P14 also mentioned habitually holding her smartphone in a specific manner to keep the camera permanently covered by her thumb. She demonstrated this cumbersome hand position to us, illustrating a tangible inconvenience. These boundary sculpting practices [41] are intended to assert control over one's data. Other measures, including using a VPN or seeking alternative providers, challenged the power imbalance. Participants expressed a need for more functional information for certain requests, such as how stakeholders access personal information. For instance, P9 distinguished between manually entering his "home address" (data card) and simply pressing an *ok* button or accepting a geolocation query having a distinct effect on him. Similarly, when P3 drew the card "to store the data," the reliability of the server or storage medium was pertinent to him. Regarding advertising, which we previously discussed, P8 expressed an act of protest by refraining from clicking on personalized advertisements: "When the ads are heavily customized to me and are about the things I am talking about or something, that is sometimes scary. And for me, it is sometimes almost a boycott not to click on these advertisements." (P8) These statements reflect a

desire to have agency over one's information. However, P5 described the paradox he sometimes faces, initially considering his "little" data as insignificant in the vast pool of big data but also recognizing the importance of individual actions [6].

5 DISCUSSION

In the following section, we will discuss our findings in light of our research question by reflecting on *Privacy Taboo* as a method, democratization, public infrastructures, and design implications, particularly for Personal Information Management Systems (PIMS).

5.1 *Privacy Taboo* as a Method

Privacy Taboo provided a captivating lens through which to observe norm formation across multiple levels. Participants engaged in negotiation, adjusting their opinions collectively while highlighting various aspects of privacy to each other [41, 62]. Using coping strategies and rebellion against power imbalances added an intriguing dimension [4, 38]. Moreover, we found that participants often drew upon media and mediators, such as teachers and parents, to articulate norms and convey competencies.

Our study contributes to the existing literature by validating established assumptions and uncovering novel insights. Notably, our findings support Nissenbaum's contextual integrity (CI) framework [45], as participants expressed information needs essential for CI to assess a situation effectively. In scenarios involving incentives like "to give you a 5 percent discount," individuals exhibited behavior aligned with the homo oeconomicus and calculus models, setting personalized thresholds about the exact number of money they want to save [9, 17]. The paradoxical nature of privacy also emerged, with some participants being confused with some requests. They also described inquiries including AI as "creepy," reflecting the still evolving norms in this domain, thus not providing a frame of orientation [28, 60]. Furthermore, advertisement seems to be partly covered by the social norm, but can cross a fine line easily.

Overall, participants demonstrated "competence-to-act" [18] in decision-making, whether accepting or declining requests or seeking further information. They displayed an ability to reflect on an abstract level, recognizing normative requirements associated with different roles, such as in the professional or personal context [44]. Despite occurring intuitively as a manifestation of embodied knowledge [39], these observations underscore the deeply entrenched social norms surrounding privacy.

It is crucial to note that decisions made in the game may not necessarily reflect real-life behavior. However, this aspect is precisely what makes the game compelling. It encourages individuals to consciously reflect on their preferences, engage in discussions, and scrutinize their practices, ultimately contributing to norm formation.

In addition to more probable scenarios, the game shows scenarios of privacy dystopia, for example, the government demanding access to the microphone [59]. Such dystopian scenarios are not regularly found in democratic societies but are not impossible in the future or in other societies. They contributed to an animated discussion as the participants jointly brainstormed about the possible consequences of such surveillance or derived self-explanations of its misuse based on their current experiences. Therefore, we also find the statements on such scenarios relevant, as they reveal insights into the need for informational self-determination and digital sovereignty. They also sensitize the participants to the consequences of scenarios that are currently prevented by German laws and regulations.

We emphasize that perceptions of privacy are deeply rooted in the cultural and socio-political environment in which one lives, shaping users' internalized norms [62]. Consequently, our German sample likely has different views on privacy compared to users from other countries, particularly

since privacy has been inscribed into German law since the population census decision in the 1980s [23]. Thus, the breach of norms and taboos is influenced by this and manifests differently as dystopian scenarios in every culture. For example, our study participants frequently mentioned and feared China's social credit system [13] and named it a dystopian real-life example they hope German law will prevent. However, as political and cultural developments are in constant flux, the media discourses surrounding dystopia will continue to evolve, and we cannot foresee the shift of norms in the future.

Furthermore, we see *Privacy Taboo* as adaptable to various domains, including, for instance, the smart home context, where stakeholder cards could be exchanged with providers like Amazon's Alexa or smart kitchen technologies. The game could also be applied to privacy studies in familial or partnership contexts, facilitating discussions about personal boundaries with different purposes. We can even envision its use beyond the scientific framework in real-life relationships, where partners can playfully explore their personal boundaries, especially considering that each family operates within a unique set of rules and values.

Nevertheless, our sample consisted mainly of laypeople who showed keen interest and awareness of privacy matters and were open to reflecting on their privacy needs. They tended to reject requests as much as possible, defying perceived loss of autonomy. Based on this, we assume that potential players should not have a defensive attitude toward social exchange and should be open to discussing topics around data protection. The card game can be effectively used in schools and public institutions to engage a broader audience that actively uses the Internet. The game is designed to be adaptable to various contexts, thereby reaching different target groups. However, for individuals in more precarious digital environments, such as those with censored Internet access, the game in its current form may be less appealing due to their restricted digital autonomy. In such cases, the cards must be adapted to meet the specific needs of vulnerable groups or activists.

Moreover, we learned from the post-interview feedback that some cards exerted disproportionate influence, overshadowing others. For example, "Access to your webcam" or "to send to the Secret Service" significantly dominated the game, making participants feel relieved when these cards were replaced. We assume that these reactions are due to the dystopian portrayal of them in media and films. They represent a significant loss of control over one's own data, as it is uncertain when or how a third party might access it. These highly contrasting cards and the strong reactions they provoke demonstrate a breach of norms, which was the primary interest of our study. In future studies, it would be interesting to observe which reactions occur with a more balanced set of cards that do not include the more provocative cases. This approach might encourage participants to consider the consequences of their decisions in greater detail, but would perhaps take them more negotiation with others to make an informed consent.

Lastly, we were pleasantly surprised to receive feedback from all participants during the post-interview phase, indicating the game's effectiveness in facilitating discussions about privacy-related topics. Despite deviating from gamification guidelines, the participants expressed that the game fostered engagement and enjoyment.

5.2 Democratization and Public Infrastructure

Through our study, we have recognized the importance of public discourses on privacy topics and the value of exchanging ideas and engaging in collective discourse. We found that simply reflecting together on these topics through the card game can sharpen people's opinions and perceptions by, for example, highlighting information gaps without being patronizing about shortcomings. As we have seen in interview 1, when P2 mirrored the privacy practices of P1, deconstructing her mental model, which would be difficult to do by oneself. Building on this, we would encourage consumer

centers or public institutions to organize gaming sessions moderated by knowledgeable individuals, fostering dialogue and raising awareness between familiar and unfamiliar people.

Another concept that could genuinely contribute to the democratization of privacy decisions through a public body is a form of citizen assembly, as suggested by P9 during the game. Such an assembly, following the example of the German citizen assembly [1], could agree on a privacy label similar to a nutrition label [27]. In the future, we want to explore this idea further. We believe that a citizen's assembly tasked with establishing common standards for data protection could be an effective way to stimulate diverse discourse, under the condition that it is composed of a diverse sample of individuals. Moreover, by simulating scenarios similar to our card game, awareness can be raised and further insights provoked. This approach would ensure that even governmental entities, which significantly influence norm formation, support the constant regulation process [2] in a democratic way.

Nevertheless, digital privacy is not equally accessible to everyone; it remains a luxury for those who can afford to protect it, both materially and immaterially [21]. This disparity is a consequence of social inequality, where many lack the resources to invest in expensive VPNs or do not have sufficient access to digital literacy [47]. While we consider privacy and the protection of personal data from third parties a fundamental human right, we acknowledge that cultural perspectives on this matter can vary [52, 61]. Vulnerable groups, in particular, require support [48]; they should be provided with the tools and knowledge necessary for safeguarding their privacy, as the lack thereof can lead to discrimination and stigmatization [36]. Our card game offers a low-threshold opportunity to create a hypothetical space for everyone, enabling them to reflect on their privacy needs beyond commercial interests. The game is intended to address all social classes and demographics.

5.3 Design Implications

Our study aims not to determine design implications but to foster a deeper understanding of privacy dynamics [12]. However, our findings stimulated some thoughts toward design considerations regarding privacy assistive tools that we want to share. We see the card game as a valuable tool to integrate into a Personal Information Management System (PIMS) [1] by leveraging scenario-building to gain better insights into users' privacy preferences. As such, a digital version of *Privacy Taboo* would be the basis of a personal privacy assistant to discern users' explicit privacy preferences across various contexts and situations. This concept aligns well with Nissenbaum's CI framework [45].

One challenge for such an assistant is ensuring that it handles users' data responsibly by being GDPR-compliant and adhering to ISO/IEC 27001 standards [24]. Ideally, it should be a robust, decentralized system that follows open-source guidelines and is not profit-oriented. We do not intend for the assistant to shift the obligations to the users to protect their privacy. Still, governmental regulations are the primary means of preventing data misuse. Strengthening autonomy is, therefore, only a part of the solution [25]. In addition, we also see a challenge in the design of an assistant for vulnerable groups [48], as even tech-savvy people often find it challenging to regulate their data via PIMS [3, 25]. In contrast to the physical card game, a digital counterpart presents more apparent barriers to use. Therefore, future studies require co-design approaches that involve users closely in the design process and consider specific contexts of use.

Additionally, given our observation that time significantly influences data request decisions, the system should address this factor. It could prompt users to take their time when making decisions, perhaps encouraging them to consult friends and family for advice. Moreover, the system could facilitate a platform for users to exchange privacy-related questions and concerns. However,

[1] https://www.buergerrat.de/en/

we acknowledge that this is a difficult design provocation since we also know that people get annoyed by notifications when stressed, but we see potential in a more mindful way of using the internet [35]. Additionally, a PIMS could address the limitations of our study and fulfill a clearer educational mandate. While we provided clarification during post-interviews and addressed problematic agreements, the long-term use of such a system could better address these issues. For instance, requests perceived as less invasive, such as relationship status, social media handles, and smartphone types, were often deemed harmless and consented to. Here, a PIMS could educate users about the potential implications of seemingly innocuous agreements and their potential for profiling or misuse in *dark patterns* [20].

For a functional version of the game within a usable PIMS, we would still incorporate the rather dystopian or extreme combinations alongside the more realistic ones. Both types are essential to highlight privacy norms or misconceptions and help users become more aware of their privacy needs. Yet, we propose that the dystopian cards be included in a demo version of the PIMS, as they are unsuitable for training the assistant in more realistic contexts.

In summary our findings are important for further future design efforts. We showed that the "Images in your gallery" card represented a strong taboo. Furthermore, the fear of being misunderstood significantly influenced participants' behavior [45]. Likewise, a recurring fear throughout the study was inadvertently sharing family and friends' data. These findings warrant further investigation and consider how such norms can be effectively addressed in responsible designs.

6 FUTURE WORK AND LIMITATIONS

Given its exploratory nature, our study presents several limitations that need to be considered. The findings are primarily based on one-time interview sessions, and we did not explore how the continuous integration and appropriation of the card game might influence individuals' privacy behavior over time. In future studies, we aim to investigate whether prolonged game use can enhance skills and increase privacy awareness. One avenue for exploration could involve providing the game to initiatives focused on teaching digital literacy to assess its efficacy in this context.

While our study provides valuable insights into individuals' tacit privacy attitudes, it is essential to acknowledge its heuristic nature [46]. Further research is necessary to understand fully how norms and rules are constructed. Given the interdependence of culture and privacy norms, we must emphasize that our study involved a sample influenced by the German cultural context. Consequently, the results may vary in other cultural contexts and governmental regulations, highlighting the need for cross-cultural studies.

Additionally, we must acknowledge that our sample primarily comprised individuals with whom we had some degree of connection through social media. While this could introduce bias into our data, we perceive it as a benefit, as it fostered a more intimate atmosphere for this rather delicate topic. However, future studies should aim to diversify the sample further to guarantee a broader representation, particularly targeting older adults, children, and teenagers who may approach privacy requests differently.

7 CONCLUSION

In conclusion, our study provides insights into how pairs articulate and negotiate privacy norms in various scenarios. We observed instances where participants grappled with feelings of powerlessness and power imbalances yet demonstrated a willingness to rebel or employ coping strategies in cases of significant norm violation. This suggests the presence of boundaries that participants were unwilling to cross, highlighting their agency in privacy decision-making. Furthermore, our observations revealed the importance of collective articulation and deliberation in shaping individuals' understanding of their privacy norms. Participants engaged in extensive discussions, particularly in

ambiguous scenarios involving potential moral dilemmas, demonstrating a conscientious approach to privacy decision-making.

Despite the card game's open-ended nature, we found that it provided an engaging experience that prompted reflection and contemplation among participants. We also noted the influence of mediators such as media and social environments on individuals' construction of privacy norms, underscoring the role of the public in creating a democratic forum for privacy education and discussion. Regarding design implications, we see the potential for scenario building in Personal Information Management Systems (PIMS) to assess users' privacy preferences better and consider the aspect of time in the process of decision-making. Besides the exploration of more realistic scenarios, the game also fosters discussion on dystopian scenarios, animating the participants to reflect on surveillance consequences and the importance of informational self-determination and legal protections. Moreover, we argue that the card game is adaptable to various use cases and has the potential for a broader application in diverse research contexts, seeking a holistic understanding of user preferences. In this way, our study contributes to the field of usable privacy in Computer-Supported Cooperative Work (CSCW) and Human-Computer Interaction (HCI). It offers a low-threshold exploratory approach to understanding user behavior and preferences in privacy-related contexts.

ACKNOWLEDGMENTS

This research was funded by the German Federal Ministry of Education and Research (BMBF) under the project BeDeNUTZ (project number: 16KIS1892). We would like to thank the BMBF for its support.

REFERENCES

[1] Serge Abiteboul, Benjamin André, and Daniel Kaplan. 2015. Managing your digital life. Commun. ACM 58, 5 (2015), 32–35.

[2] Irwin Altman. 1977. Privacy regulation: Culturally universal or culturally specific? Journal of social issues 33, 3 (1977), 66–84.

[3] Nicolas Anciaux, Philippe Bonnet, Luc Bouganim, Benjamin Nguyen, Philippe Pucheral, Iulian Sandu Popa, and Guillaume Scerri. 2019. Personal data management systems: The security and functionality standpoint. Information Systems 80 (2019), 13–35.

[4] Denise Anthony, Celeste Campos-Castillo, and Christine Horne. 2017. Toward a sociology of privacy. Annual review of sociology 43 (2017), 249–269.

[5] Ralf Bohnsack. 1999. Gruppendiskussionsverfahren. VS Verlag für Sozialwissenschaften, Wiesbaden. 123–142 pages.

[6] Göran Bolin and Jonas Andersson Schwarz. 2015. Heuristics of the algorithm: Big Data, user interpretation and institutional translation. Big Data & Society 2, 2 (2015), 2053951715608406.

[7] Pierre Bourdieu. 1984. Distinction: A social critique of the judgement of taste. Harvard university press, Cambridge, MA, USA.

[8] Virginia Braun and Victoria Clarke. 2012. Thematic Analysis. American Psychological Association, Washington, DC. 57–71 pages.

[9] Tamara Dinev and Paul Hart. 2006. An extended privacy calculus model for e-commerce transactions. Information systems research 17, 1 (2006), 61–80.

[10] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Lorrie Faith Cranor, and Vincent Koenig. 2021. A systematic literature review of empirical methods and risk representation in usable privacy and security research. ACM Transactions on Computer-Human Interaction (TOCHI) 28, 6 (2021), 1–50.

[11] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Vincent Koenig, and Lorrie Faith Cranor. 2023. Empirical Research Methods in Usable Privacy and Security. In Human Factors in Privacy Research. Springer International Publishing Cham, Switzerland, 29–53.

[12] Paul Dourish. 2006. Implications for design. In Proceedings of the SIGCHI conference on Human Factors in computing systems. Association for Computing Machinery, New York, NY, USA, 541–550.

[13] Severin Engelmann, Mo Chen, Felix Fischer, Ching-yu Kao, and Jens Grossklags. 2019. Clear sanctions, vague rewards: how China's social credit system currently defines" good" and" bad" behavior. In Proceedings of the conference on fairness, accountability, and transparency. ACM, New York, NY, USA, 69–78.

[14] Michel Foucault. 1979. Power, Truth, Strategy. Feral Publications, Sydney.

[15] Harold Garfinkel. 1964. Studies of the routine grounds of everyday activities. Social problems 11, 3 (1964), 225–250.

[16] Simson Garfinkel and Heather Richter Lipford. 2014. Usable security: History, themes, and challenges. Morgan & Claypool Publishers, San Rafael, California.

[17] Nina Gerber and Alina Stöver. 2023. From the Privacy Calculus to Crossing the Rubicon: An Introduction to Theoretical Models of User Privacy Behavior. In Human Factors in Privacy Research. Springer International Publishing Cham, Switzerland, 11–25.

[18] Silvia Gherardi. 2008. Situated knowledge and situated action: What do practice-based studies promise. In The SAGE handbook of new approaches in management and organization. Sage London, Limited, United Kingdom, 516–525.

[19] Erving Goffman. 1961. The Underlife of a Public Institution: A Study of Ways of Making Out in a Mental Hospital. In Asylums: Essays on the Social Situation of Mental Patients and Other Inmates. Anchor Books, New York, NY, 172–320.

[20] Colin M Gray, Cristiana Santos, and Nataliia Bielova. 2023. Towards a preliminary ontology of dark patterns knowledge. In Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, 1–9.

[21] Eszter Hargittai. 2018. The digital reproduction of inequality. In The inequality reader. Routledge, New York, NY, USA, 660–670.

[22] Christine Horne, Brice Darras, Elyse Bean, Anurag Srivastava, and Scott Frickel. 2015. Privacy, technology, and norms: The case of smart meters. Social science research 51 (2015), 64–76.

[23] Gerrit Hornung and Christoph Schnabel. 2009. Data protection in Germany I: The population census decision and the right to informational self-determination. Computer Law & Security Review 25, 1 (2009), 84–88.

[24] ISO. 03.08.2024. ISO/IEC 27001:2022. https://www.iso.org/standard/27001

[25] Heleen Janssen, Jennifer Cobbe, and Jatinder Singh. 2020. Personal information management systems: a user-centric privacy utopia? Published in Internet Policy Review (18 December 2020) 9, 4 (2020), 1–25.

[26] Patrick Jost and Andreas Künz. 2021. Cards and roles: Co-designing privacy serious games with an online role-playing boardgame. In Games and Learning Alliance: 10th International Conference, GALA 2021, La Spezia, Italy, December 1–2, 2021, Proceedings 10. Springer International Publishing, Switzerland, 187–197.

[27] 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. ACM, New York, NY, USA, 1–12.
[28] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security 64 (2017), 122–134.
[29] Irwin R Kramer. 1989. The Birth of Privacy Law: A Century Since Warren and Brandeis. Catholic University Law Review 39 (1989), 703.
[30] Christian Licoppe. 2004. 'Connected' presence: The emergence of a new repertoire for managing social relationships in a changing communication technoscape. Environment and planning D: Society and space 22, 1 (2004), 135–156.
[31] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In Proceedings of the 2012 ACM conference on ubiquitous computing. ACM, New York, NY, USA, 501–510.
[32] Ewa Luger, Lachlan Urquhart, Tom Rodden, and Michael Golembewski. 2015. Playing the legal card: Using ideation cards to raise data protection issues within the design process. In Proceedings of the 33rd Annual ACM conference on human factors in computing systems. ACM, New York, NY, USA, 457–466.
[33] Dominique Machuletz, Stefan Laube, and Rainer Böhme. 2018. Webcam covering as planned behavior. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. ACM, New York, NY, USA, 1–13.
[34] Jennifer Smith Maguire and Julian Matthews. 2010. Cultural intermediaries and the media. Sociology Compass 4, 7 (2010), 405–416.
[35] Teale W Masrani, Jack Jamieson, Naomi Yamashita, and Helen Ai He. 2023. Slowing it down: Towards facilitating interpersonal mindfulness in online polarizing conversations over social media. Proceedings of the ACM on Human-Computer Interaction 7, CSCW1 (2023), 1–27.
[36] Tobias Matzner, Philipp K Masur, Carsten Ochs, and Thilo von Pape. 2016. Do-It-yourself data protection—Empowerment or burden? Data protection on the move: Current developments in ICT and privacy/data protection 24 (2016), 277–305.
[37] Marcel Mauss. 1997. Soziologie und Anthropologie. 2. Gabentausch; Soziologie und Psychologie; Todesvorstellungen; Körpertechniken; Begriff der Person. Fischer-Taschenbuch-Verlag, Wiesbaden.
[38] Rachel I McDonald and Christian S Crandall. 2015. Social norms and social influence. Current Opinion in Behavioral Sciences 3 (2015), 147–151.
[39] Maurice Merleau-Ponty. 2012. Phenomenology of perception (DA Landes, trans.).
[40] Anne Mollen and Frederik Dhaenens. 2018. Audiences' coping practices with intrusive interfaces: Researching audiences in algorithmic, datafied, platform societies. In The future of audiences: A foresight analysis of interfaces and engagement. Springer International Publishing AG, Switzerland, 43–60.
[41] Anouk Mols and Jason Pridmore. 2021. Always available via WhatsApp: Mapping everyday boundary work practices and privacy negotiations. Mobile Media & Communication 9, 3 (2021), 422–440.
[42] David L Morgan, Jutta Ataie, Paula Carder, and Kim Hoffman. 2013. Introducing dyadic interviews as a method for collecting qualitative data. Qualitative health research 23, 9 (2013), 1276–1284.
[43] Thao Ngo, Johannes Kunkel, and Jürgen Ziegler. 2020. Exploring mental models for transparent and controllable recommender systems: a qualitative study. In Proceedings of the 28th ACM Conference on User Modeling, Adaptation and Personalization. Association for Computing Machinery, New York, NY, USA, 183–191.
[44] Christena E Nippert-Eng. 1996. Home and Work: Negotiating Boundaries Through Everyday Life. Chicago: Univ.
[45] Helen Nissenbaum. 2009. Privacy in context: Technology, policy, and the integrity of social life. In Privacy in Context. Stanford University Press, USA.
[46] Ulrich Oevermann. 2013. Objektive Hermeneutik als Methodologie der Erfahrungswissenschaften von der sinnstrukturierten Welt. In Reflexive Wissensproduktion. Springer, Wiesbaden, Germany, 69–98.
[47] Zizi Papacharissi. 2010. Privacy as a luxury commodity. First Monday 15, 8 (2010).
[48] Stanislaw Piasecki, Jiahong Chen, and Derek McAuley. 2022. Putting the Right P in PIMS: Normative Challenges for Protecting Vulnerable People's Data through Personal Information Management Systems. European Journal of Law and Technology 13, 3 (2022).
[49] Nicholas Proferes. 2022. The development of privacy norms. In Modern Socio-Technical Perspectives on Privacy. Springer International Publishing, Cham, 79–90.
[50] Amon Rapp. 2018. Autoethnography in human-computer interaction: Theory and practice. In New Directions in Third Wave Human-Computer Interaction: Volume 2-Methodologies. Springer, Heidelberg, Germany, 25–42.
[51] Kate Raynes-Goldie and Matthew Allen. 2014. Gaming Privacy: A Canadian Case Study of a Co-Created Privacy Literacy Game for Children. Surveillance & Society 12, 3 (2014), 414–426.
[52] Mennatallah Saleh, Mohamed Khamis, and Christian Sturm. 2018. Privacy invasion experiences and perceptions: a comparison between Germany and the Arab world. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems. ACM, New York, NY, USA, 1–6.

[53] Yan Shvartzshnaider, Nicholas Apthorpe, Nicholas Feamster, and Helen Nissenbaum. 2019. Going Against the (Appropriate) Flow: A Contextual Integrity Approach to Privacy Policy Analysis. In Proceedings of the AAAI Conference on Human Computation and Crowdsourcing, Vol. 7. The AAAI Press, Washington, DC, USA, 162–170.
[54] Ignacio Siles, Andrés Segura-Castillo, Ricardo Solís, and Mónica Sancho. 2020. Folk theories of algorithmic recommendations on Spotify: Enacting data assemblages in the global South. Big Data & Society 7, 1 (2020), 2053951720923377.
[55] Daniel J Solove. 2005. A taxonomy of privacy. U. Pa. l. Rev. 154 (2005), 477.
[56] Anselm Strauss. 1978. Negotiations: Varieties, contexts, processes, and social order. Vol. 114. Jossey-Bass San Francisco, San Francisco.
[57] Anselm Strauss. 2017. Psychiatric ideologies and institutions. Routledge, London.
[58] Anselm Strauss and Juliet M Corbin. 1997. Grounded theory in practice. Sage, Thousand Oaks.
[59] Theresa Jean Tanenbaum, Marcel Pufal, and Karen Tanenbaum. 2016. The limits of our imagination: design fiction as a strategy for engaging with dystopian futures. In Proceedings of the Second Workshop on Computing within Limits. Association for Computing Machinery, New York, NY, USA, 1–9.
[60] Omer Tene and Jules Polonetsky. 2013. A theory of creepy: technology, privacy and shifting social norms. Yale JL & Tech. 16 (2013), 59.
[61] Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2018. Examining security and privacy research in developing regions. In Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies. ACM, New York, NY, USA, 1–14.
[62] Alan F Westin. 1968. Privacy and freedom. Washington and Lee Law Review 25, 1 (1968), 166.

Received May 2024; revised August 2024; accepted October 2024