Immersive Invaders: Privacy Threats from Deceptive Design in Virtual Reality Games and Applications

HILDA HADAN, Stratford School of Interaction Design and Business, University of Waterloo, Canada
MICHAELA VALIQUETTE, Human-Computer Interaction, Carleton University, Canada
LENNART E. NACKE, Stratford School of Interaction Design and Business, University of Waterloo, Canada
LEAH ZHANG-KENNEDY, Stratford School of Interaction Design and Business, University of Waterloo, Canada

Virtual Reality (VR) technologies offer immersive experiences but collect substantial user data. While deceptive design is well-studied in 2D platforms, little is known about its manifestation in VR environments and its impact on user privacy. This research investigates deceptive designs in privacy communication and interaction mechanisms of 12 top-rated VR games and applications through autoethnographic evaluation of the applications and thematic analysis of privacy policies. We found that while many deceptive designs rely on 2D interfaces, some VR-unique features, while not directly enabling deception, amplified data disclosure behaviors, and obscured actual data practices. Convoluted privacy policies and manipulative consent practices further hinder comprehension and increase privacy risks. We also observed privacy-preserving design strategies and protective considerations in VR privacy policies. We offer recommendations for ethical VR design that balance immersive experiences with strong privacy protections, guiding researchers, designers, and policymakers to improve privacy in VR environments.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**; • **Human-centered computing → Virtual reality**; **Empirical studies in HCI**; • **Applied computing → Computer games**.

Additional Key Words and Phrases: User Privacy, Dark Patterns, Deceptive Design, Virtual Reality, Games User Research

ACM Reference Format:
Hilda Hadan, Michaela Valiquette, Lennart E. Nacke, and Leah Zhang-Kennedy. 2025. Immersive Invaders: Privacy Threats from Deceptive Design in Virtual Reality Games and Applications. *Proc. ACM Hum.-Comput. Interact.* 9, 7, Article CSCW431 (November 2025), 54 pages. https://doi.org/10.1145/3757612

1 Introduction

Deceptive Design (formerly "dark patterns")[1] refers to design practices that distort or impair users' ability to make informed decisions, regardless of the design intent [8, 12, 77]. Users face privacy harms when deceptive tactics, such as bad defaults, mandatory registrations, and social pyramid, impair their decision-making and lead to unintended data disclosures [8, 48, 54, 101]. Deceptive designs

[1]We follow the ACM Diversity and Inclusion Council's guideline for inclusive language and adopt the term "deceptive design" instead of "dark patterns" in our study. See: https://www.acm.org/diversity-inclusion/words-matter

Authors' Contact Information: Hilda Hadan, hhadan@uwaterloo.ca, Stratford School of Interaction Design and Business, University of Waterloo, Waterloo, Canada; Michaela Valiquette, michaelavaliquette@cmail.carleton.ca, Human-Computer Interaction, Carleton University, Ottawa, Canada; Lennart E. Nacke, lennart.nacke@acm.org, Stratford School of Interaction Design and Business, University of Waterloo, Waterloo, Canada; Leah Zhang-Kennedy, lzhangke@uwaterloo.ca, Stratford School of Interaction Design and Business, University of Waterloo, Waterloo, Canada.



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.
© 2025 Copyright held by the owner/author(s).
ACM 2573-0142/2025/11-ARTCSCW431
https://doi.org/10.1145/3757612

are particularly problematic in social computing, where issues such as data consent interactions and social engineering techniques raise concerns about data ethics and privacy [8, 47, 53].

As a new medium for gaming and social interaction, Virtual Reality (VR) opens a new frontier for manipulative tactics through immersive visual, audio, and haptic feedback that disconnects users from the real world [122]. VR's spatial and realistic displays can enhance the subtlety of deceptive designs [55, 69], making it harder for users to critically assess content [22]. VR simulations using bodily sensor data enable hyper-personalized deceptive tactics [13, 86]. Additionally, VR-enabled social experiences also introduce challenges to maintaining user privacy [80].

Although academic researchers and government agencies are actively regulating deceptive designs [31, 50, 97, 101] and sanctioning companies for invading user privacy with deceptive practices [20, 36, 98, 128], these efforts primarily address issues in the 2D mobile and computer platforms (e.g., [12, 50, 87, 88]). Research on deceptive practices in VR and their privacy implications remains limited (e.g., [55]), and deceptive game design studies have largely focused on temporal and monetary manipulations, neglecting privacy issues (e.g., [57, 68, 103]). As commercial games and social applications increasingly shift to VR, it becomes crucial to understand how deceptive practices evolve in immersive technology and the implications for user privacy.

Our research examines the manifestation of deceptive designs in the privacy communication and interaction mechanisms of top-rated commercial VR applications. This is particularly important since users often lack awareness of VR's data collection capabilities [59]. Our research objective is to explore how these designs obscure or distort users' understanding of privacy information and impair their privacy decisions. We also explore privacy-enhancing VR designs, which we referred to as "bright patterns"[2] that support users' ability to make informed privacy decisions and better understand privacy information [51, 114, 130]. Such insights are essential for developing VR safeguards that contribute to safer and privacy-respecting VR gaming and social interaction environments. With this objective in mind, we focus on two primary research questions (RQs):

RQ1: To what extent do commercial VR games and applications implement deceptive and "bright patterns" that might influence users' privacy decisions?

RQ2: What specific data practices and privacy risks are concealed by or made more manageable through design strategies in VR games and applications?

To answer these RQs, we examined the privacy communication and interaction mechanisms of 12 top-rated VR games and apps, along with their data practices described in their privacy policies (see Section 3.1). These titles were selected for their popularity, market impact, and diverse genres and functionalities. Therefore, they represent the most highly recommended[3], top-rated[4], and widely downloaded products on major VR platforms[5]. The genres of the 12 games and applications selected range from puzzle and adventure games to applications for productivity, fitness, and social interaction. We refer to the former as "games" and the latter as "apps", which are applications that offer playful experiences but do not necessarily rely on core game elements or demonstrate game characteristics [25, 76]. This diverse selection, which we hereby refer to as "VR games and apps,"

[2]We adopt the term "bright patterns" from the literature [51, 114, 130] to prioritize clarity for this specific class of that literature frequently referred to as the user empowerment alternative to deceptive design. We follow this terminology rather than introducing a new term to prevent confusion, as there is currently no standardized terms in any legislation to describe this kind of design patterns.

[3]Recommended Games—PCVR, Quest & PSVR. https://www.reddit.com/r/VRGaming/comments/ymsewg/recommended_games_pcvr_quest_psvr/

[4]Meta Quest Store. https://www.meta.com/experiences/

[5]VR Space. (2024, February 14). *The 50 most downloaded VR games of all time.* VR Space. https://vr.space/news/the-50-most-downloaded-vr-games-of-all-time/

provides a broad overview of privacy practices in various VR use cases and allows us to identify deceptive practices affecting a large number of users in various VR contexts.

Building on prior deceptive design and privacy research [9, 48, 60, 67], we used a two-phased methodology. First, we conducted an autoethnographic evaluation of 12 VR games and apps. Then, we contrasted these findings with the data practices outlined in the applications' privacy policies derived through thematic analysis. This two-phased approach enabled us to identify discrepancies between the privacy information presented to users, the ways user-facing privacy mechanisms influence decision-making, and the actual privacy issues disclosed in the publisher's data practices.

Our research findings make three main **contributions**: *First*, we show that while deceptive design patterns in the registration and subscription processes, consent interactions, privacy settings, quality-of-life (QoL) features, and notification mechanisms in VR games and apps still heavily rely on 2D interfaces in VR, their presence in the privacy communication and interaction mechanisms of VR games and apps demonstrates how traditional manipulative tactics are being adapted in immersive environments. These tactics are further amplified by VR-unique features, with increased harm to users' privacy. *Second*, our analysis of privacy policies shows that convoluted and complex policies, already a known usability issue on mobile and web platforms, continue to plague users in VR, obscure their understanding, and hinder their privacy decision-making. We found that substantial data transmissions are not transparently communicated through VR design mechanisms, with many relying on submissive consent practices. Some lacked privacy settings entirely, which further increases users' confusion and unawareness of privacy risks. These findings emphasize the need for transparent and usable privacy communication, both in design mechanisms and policy construction. *Third*, we identified privacy-enhancing VR design strategies and protective considerations in privacy policy that can serve as a foundation for more effective privacy communication and interaction in VR games and apps. Based on these results, we make recommendations for the ethical design of VR games and apps that balance immersive experiences with strong privacy protections to guide VR researchers, designers, and policymakers in creating privacy-preserving VR games and apps and crafting clearer privacy policies for this evolving technology.

2 Related Work

2.1 Deceptive Design and Its Privacy Implications

Deceptive Designs exploit both people's internal cognitive biases and external social pressures that constitute complex human decision-making [120, 127, 133]. They manipulate users into making choices that are not in their best interest and lead to various negative consequences [12, 82, 83]. Literature has identified four issues associated with deceptive design, including loss of autonomy and decision-making capability [83], financial loss [6, 73, 77, 82], labor and cognitive burdens (e.g., emotional distress) [6, 47, 79, 95], and invasion of privacy [8, 54, 83]. Within the context of video games, research has found deceptive designs for psychological and social manipulation [57, 135], attention capture [91], and mechanisms that prolong gameplay or encourage impulsive spending [26, 39, 66, 135]. Building on early deceptive design research [11, 48, 82, 135], academic researchers and government agencies have further investigated and categorized deceptive design across various digital platforms, such as social media [87, 88], websites [12, 46, 96, 101], mobile apps [26, 53], games [57, 68, 128], and 3D immersive environments [52, 55, 69]. Research has also proposed user empowerment design patterns—"bright patterns"—to counteract deceptive design [51, 114, 130]. In recent work, Gray et al. [50] compiled an ontology of 64 deceptive designs based on regulatory and academic sources, and Hadan et al. [60] further expanded it into a VR-specific assessment guide.

Relevance. While deceptive design literature provided a foundation for our analysis, we primarily relied on Hadan et al. [60]'s *VR Deceptive Game Design Assessment Guide* as our deductive codebook

due to its integration of foundational works in deceptive design research (e.g., [11, 48, 50, 84]) and regulatory works that focus on how deceptive designs affect user privacy (e.g., [8, 21, 35, 96]). This *Assessment Guide* further includes frameworks specifically targeting VR and game-related deceptive designs [55, 68, 135]. In Section 3.2.3, we detail how this *Assessment Guide* shaped our exploration of privacy-impacting deceptive design in VR games and apps included descriptions of deceptive patterns from literature [50, 60] in Table 2.

2.1.1 Privacy Implications of Deceptive Design. As research on deceptive design evolves, it has expanded beyond issues of autonomy, financial harm, and cognitive burden to address privacy implications (e.g., [8, 54, 137]). In contrast to back-end privacy issues such as data breaches or compromised network traffic, users' immediate perception of privacy predominantly hinges on privacy interfaces. Regulatory efforts have sought to regulate the deceptive design issue [1, 62], and impose sanctions on companies that manipulate children and invade their privacy [19, 36]. Building upon established strategies for privacy preservation [61], Bösch et al. [8] formulated a taxonomy of eight privacy-related deceptive design strategies and documented their prevalence across popular online platforms. Zhang-Kennedy et al. [137] investigated the reasons behind implementing these strategies from the perspective of design practitioners. Gunawan et al. [54] summarized three privacy-related contexts where deceptive designs frequently appear on websites and mobile apps, such as user settings, exit requests, and "entry" requests and consent interactions. Deceptive practices in consent mechanisms have also been identified, such as missing terms of service, bundled consent, pre-checked opt-in boxes, and nagging [53, 95, 121]. These strategies create the illusion of informed and free choice [133]. Additionally, privacy policies can employ deceptive tactics, such as hiding hyperlinks [63], using positive framing, exploiting time gaps between notice and choice [4], and omitting privacy information [75, 138]. Legalistic language further discourages reading and hinders user understanding [32, 63, 101].

Relevance. Studies have shown that users are less aware of privacy harms caused by deceptive designs compared to other harms [6, 9]. However, existing academic and regulatory efforts have primarily focused on 2D websites and mobile applications (e.g., [26, 53, 54, 101]), and overlooked their impact in gaming and immersive environments. Given users' unawareness and lack of transparency in online games' data practices [9, 71, 118] and VR technology's data collection capabilities [59], our study explores how deceptive design practices manifest in gaming and VR environments and potentially compromise user privacy in these contexts.

2.1.2 Importance of Considering User Perspectives in Deceptive Design Research. The impact of deceptive design largely depends on users' ability to recognize such patterns, which varies depending on their literacy in this area [26, 77, 135]. For instance, Di Geronimo et al. [26] revealed that users often remain unaware of deceptive design in mobile apps, while Luguri and Strahilevitz [77] found that subtle deceptive practices are more likely to go unnoticed by less-educated users. M. Bhoot et al. [78] identified five key factors that influence users' susceptibility to deceptive design: frequency of exposure, perceived trustworthiness, level of frustration, misleading behavior, and the physical appearance of the user interface. Research also highlights the mixed reactions of players to game mechanisms that involve deceptive designs. For example, some players view daily tasks as rewarding and motivating, but others see them as pressure-inducing due to the "Fear of Missing Out" and the obligation to participate [41, 57]. Similarly, grinding may be perceived positively when it involves variations and achievements, but it can also be seen as tedious [57, 66, 135]. Given the complexity of identifying deceptive design, the literature advocates for user-centric approaches to discern practices that may not be overtly unethical [47, 49, 57] and derive ethical design solutions [57, 102]. However, non-expert participants are often unable to correctly identify malicious designs, let alone specific deceptive design patterns [26].

Relevance. To address the challenge while maintaining a user-centric focus, we adopted an autoethnographic approach [65, 109] to enable researchers to engage with VR applications as users, systematically document their frustrations, concerns, and observations over time [65, 109], and refine their interpretations through an introspective process [3, 109]. Autoethnography has been used to explore privacy risks [72], usability issues with privacy controls [33, 131], and deceptive design in both computer [66, 108] and VR and AR games [60, 72]. Given the subtle nature of deceptive designs in VR [55, 70], the autoethnography approach that paired our researchers' expertise with a first-hand user experience is ideal for studying deceptive design in VR [60].

2.2 Privacy Concerns of VR and Games and Their Interplay with Deceptive Design

2.2.1 Privacy Implications of VR Technology and Its Deceptive Design. The rise of VR technology has introduced new avenues for user profiling [13, 59], as VR sensors track user movements, generate feedback, and enable inferences about users' physical and mental conditions [89], habitual movements [89, 104], cognition, emotions, and personality [13, 86]. Enhanced user experiences in VR often encourages the sharing of private information, with companies often promising improved services in exchange [7]. These data can be exploited to manipulate user behavior [13, 86, 128] and drive profits for companies [28, 86, 128]. However, studies show that even experienced users are often unaware of the types, uses, and management of the data collected by immersive technology [2, 43, 59], which can lead to unclear expectations and increased privacy risks. Research suggests that deceptive designs that invade user privacy from non-VR environments are likely to migrate into VR [55, 69]. For example, XR[6] variations of "toying with emotion" such as hyper-personalized digital characters mimicking friends or family, can manipulate users into revealing private information [48, 55]. Similarly, perception hacking in VR might trick users into interacting with undesired virtual objects, leading to accidental information disclosure or unintended consent [48, 124]. Moreover, VR's immersive nature may introduce novel deceptive designs [55], such as immersion in realistic and multi-sensory environments [122], which can obscure users' sense of reality [22, 55, 69]. These XR features can lead to new deceptive practices, such as false memory implantation, blind-spot tracking, and reality distortion, all of which exploit human cognitive and perceptual limitations [7, 117, 124].

Relevance. While recent studies have examined the potential for deceptive design in immersive environments, they have primarily relied on hypothetical scenarios, expert predictions, and controlled experiments (e.g., [55, 69, 124]) that often focus broadly on XR technology but overlooked the contextual factors of VR. To address this gap, our research investigates how deceptive practices manifest in real-world VR games and apps, with special attention to their impact on user privacy.

2.2.2 Privacy Implications of Video Game and Its Deceptive Design. As a reason behind VR adoption [92], video games collect extensive data without sufficient disclosure [9, 71]. During account registration, users often provide personal information such as full name, date of birth, email address, postal address, and payment details [71]. Beyond these manual inputs, gaming devices can capture a wide array of data, including voice, gestures, heart rate, facial expressions, location, and hardware configurations [71, 111]. Games also track users' in-game actions and may request access to other applications or social media profiles [16, 111]. The granularity of data collection varies, with more advanced games gathering a broader range of information [27]. Such detailed data collection enables companies to profile users and infer their demographic traits, interests, personality, emotional states, skills, and financial habits [71, 81, 111]. Users may adopt fictional identities but their virtual behavior often reflects their real-world personalities [29, 123]. The entertainment value of games and the complexity of data practices make it difficult and demotivating for users to stay informed [71, 111].

[6]Extended Reality (XR) describes immersive technologies such as Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR).

In fact, many users remain unaware of or misunderstand how their data is handled in games [9]. In addition, privacy policies for video games are often vague and omit critical details [111], which leaves opportunities for deceptive designs. Furthermore, proposals to use player-NPC (non-player character) communication, such as emotional states communicated through NPC dialogues, can lead to privacy intrusions [42] and facilitate emotional manipulation [60]. Therefore, games' entertainment value, NPC intimacy, and vague privacy policies [42, 71, 111] all increase the risk of users being subtly deceived into sharing private information.

Relevance. While prior studies have examined privacy in gaming through information flow analysis [92] and data-driven prediction [81], research on user attitudes and awareness of data-sharing practices in online gaming remains limited (e.g., [9]). Regulatory guidelines primarily target privacy in computer and mobile games [100, 101], with minimal attention to those in VR. Although some studies have touched on deceptive designs that invade user privacy in VR, they often rely on practitioners' and literature's hypotheses (e.g., [55, 69]), a narrow selection of commercial VR games (e.g., [60]), and a limited focus on consent interactions and concerns in computer and mobile games (e.g., [9, 27, 54]). Deceptive design in broader privacy contexts and a wider range of VR applications remains a gap in the literature. In this study, we aim to understand privacy-invasive data practices in VR games and the role of deceptive design in these processes.

3 Methodology

Building upon methodology in previous deceptive design and privacy literature [9, 48, 60, 67], in this research, we adopted a two-phased methodology (see Figure 1): (1) an autoethnographic evaluation of VR games' and apps' privacy communication and interaction design mechanisms with our researchers with expertise in deceptive design, user privacy, and games research, and (2) a thematic analysis of privacy policies of the evaluated VR games and apps.

3.1 Research Context

We evaluated 12 popular VR games ($n = 6$) and apps ($n = 6$) that were top-rated on the Meta Quest Store[7] and highly recommended by VR users on Reddit[8] to cover diverse game genres and application categories to represent various gameplay styles and user experiences. Table 1 summarizes the selected VR games' and apps' publisher, initial release year, main gameplay mechanics, availability of a privacy policy, and available platforms. Although our analysis was performed on the Meta Quest 3 headset, the selected apps are available on multiple VR platforms and are widely accessed by millions of users worldwide. This wide user base enables us to identify privacy-related deceptive design patterns that are likely to manifest in the mainstream VR user experience.

3.2 Design Mechanism Evaluation

We employed an autoethnography method, which situates researchers as both the "protagonist" and observer, and enables a first-person engagement and understanding of the VR environment [65, 109]. Our decision to adopt this methodology is informed by literature on HCI, games, and security and privacy research (e.g., [33, 72, 107, 108, 131]), as discussed in Section 2.1.2.

3.2.1 Ethical Considerations and Limitations. Following the research ethics guidelines [15], we carefully designed our methodology to prioritize ethical considerations. Before initiating the autoethnographic diary data collection, we consulted our institution's Research Ethics Board (REB) to confirm that our approach did not require formal ethical review. To protect the privacy of other users, we focused our investigation on single-player modes in the selected VR games and apps to

[7]See footnote 4.
[8]See footnote 3.

Table 1. Summary of Virtual Reality (VR) Games and Apps in Our Research.

Title (acronym[a])	Genre[b]	Publisher	Year	Description	Privacy Policy[c]	Platforms[d]	Hours	Diaries
Beat Saber (BS)	Rhythm	Beat Games	2019	Players slash incoming beat cubes to the rhythm of the music.	In-game, On-website	PCVR, CVR, SAVR	18	9
Moss: Book II (MOSS2)	Action	Polyarc	2022	Players guide the mouse Quill through fantasy environments, solve puzzles and battle enemies on her journey.	On-website	PCVR, CVR, SAVR	8	9
The Room VR (ROOM)	Puzzle	Fireproof Games	2020	Players investigate mysterious environments, solve intricate puzzles, and uncover a secret within an ancient Egyptian artifact.	On-website	PCVR, CVR, SAVR	8	3
A Fisherman's Tale (FISHER)	Interactive Story	Vertigo Games	2019	Players guide a tiny fisherman through a series of dollhouse-like worlds to uncover a strange story.	On-website	PCVR, CVR, SAVR	3	2
Down the Rabbit Hole (RABBIT)	Adventure	Beyond Frames Entertainment	2020	Players guide a lost girl through a whimsical prequel world to Alice in Wonderland.	On-website	PCVR, CVR, SAVR	3	2
LEGO®Bricktales [e] (LEGO)	Adventure	Thunderful Publishing AB	2023	Players build solutions to help LEGO characters navigate various themed environments and overcome challenges.	On-website	PCVR, CVR, SAVR	31	8
The Climb 2 (CLIMB)	Sports	Crytek	2021	Users climb mountains, skyscrapers, and caves, and find their way to the top and enjoying the views.	In-app, On-website	PCVR, SAVR	9	4
VRChat (CHAT)	Social	VRChat Inc.	2019	Users create avatars, explore diverse virtual worlds, and interact with others.	In-app, On-website	PCVR, SAVR	4	3
Meta Horizon Worlds[f] (HRZ)	Social	Facebook	2020	Users explore, build, and interact in immersive, user-created worlds.	In-app, On-website	SAVR	4	3
TRIPP (TRIPP)	Meditation	TRIPP, Inc.	2019	Users go on guided mindfulness journeys with calming visuals and sounds to help them relax and focus.	In-app, On-website	PCVR, CVR, SAVR	5	7
Supernatural (SN)	Fitness	Within Unlimited, Inc.	2020	Users go on guided fitness sessions in beautiful natural virtual locations with motivating music.	In-app, On-website	SAVR	8	4
Immersed (IMRSD)	Productivity	Immersed Inc.	2020	Users join virtual workspaces, set up virtual monitors, and stay focused in a distraction-free environment.	On-website	SAVR	40	5

Note. Information in this table was retrieved from the Meta Quest Store website. https://www.meta.com/experiences/

a. VR game acronyms are colored Blue and VR app acronyms are colored Pink.

b. For apps listed under multiple genres, the first listed genre was chosen.

c. A link to each game's and application's developer privacy policy is available on their Meta Quest Store page.

d. "PCVR", "CVR", and "SAVR" refer to computer-based VR (e.g., Valve Index, Meta Oculus Rift, HTC Vive), console-based VR (e.g., PlayStation VR), and standalone VR(e.g., Meta Quest VR, PICO VR) systems, respectively.

e. We included a second adventure game—LEGO®Bricktales—due to its appeal to children and child data privacy concerns raised by the Office of the Privacy Commissioner (OPC) [101] in its analysis of the game's website.

f. We included a second VR social platform—VRChat—given its popularity among children around 15 years old [24].

avoid other users' involvement without consent. For apps (e.g., VRChat, Meta Horizon Worlds, and Immersed) that inherently include social interactions, we centered our analysis on the researcher's journey and avoided video recordings that involved other users. We also consulted our university library on the appropriate use of screenshots for research purposes in this manuscript, under Fair Dealing guidelines in the Copyright Act of our country.

Our autoethnographic study, while providing valuable insights, has limitations. We have provided a detailed reflexivity statement (see Section 3.2.3) to address potential biases from the lead researcher's background. However, we recognize that our findings may not fully represent the experiences of a broader user base with varying levels of deceptive design literacy and perceptions [26, 41, 77, 135]. Nonetheless, we are confident that our autoethnographic study on the 12

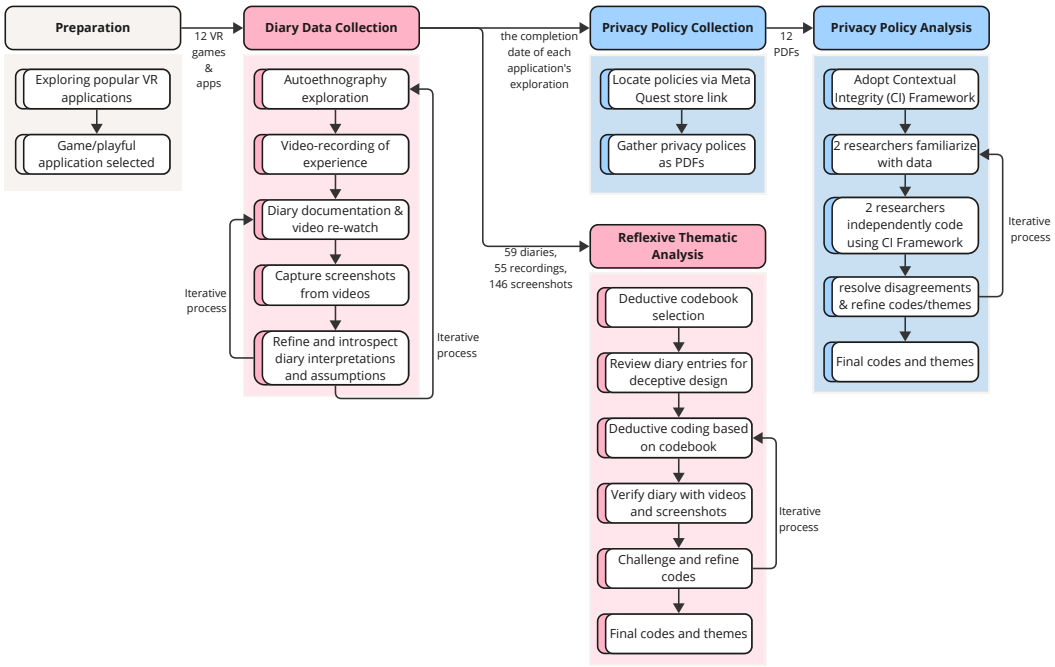


Fig. 1. Flowchart of our two-phased methodology, with **pink** denotes the process of our autoethnographic evaluation of VR games' and apps' privacy communication and interaction design mechanisms, and **blue** denotes the process of our privacy policy analysis. The reflexive thematic analysis and privacy policy data collection were conducted in parallel. We completed each application's autoethnographic exploration before collecting its privacy policy to ensure the policy was up-to-date during our analysis.

cross-platform VR games and apps allowed us to experience a wide variety of deceptive tactics and privacy issues in the privacy communication and interaction mechanisms in VR environments.

3.2.2 Data Collection. The lead researcher with expertise in VR, deceptive design, gaming, and usable privacy engaged and fully immersed in all 12 VR games and apps during a six-month timeframe. For games and apps with a clear endpoint (e.g., storyline completion), exploration continued until the endpoint was reached to ensure a comprehensive understanding of the privacy mechanisms. For genres without a defined endpoint (e.g., Beat Saber), the exploration followed the principle of saturation, ending when no new privacy issues and deceptive designs were observed and no new insights emerged from the privacy communication and interaction mechanisms. This autoethnography process resulted in 59 diary entries, 55 video recordings, and 146 screenshots.

Diary Entries. Dairy entries focused on the design mechanisms that allow users to (1) obtain privacy information, and (2) make privacy choices and express privacy preferences. Following an established method in literature [60], the lead researcher systematically documented the experience in two segments in each diary entry: (1) detailed observations of privacy communication and interaction design mechanics that incorporated deceptive designs, and (2) reflections on experiences, reactions, thoughts, and emotional responses when the design mechanics were encountered. Using this strategy, the lead researcher personally experienced and immersed in the VR games and apps. This process resulted in 55 immediate reflections after each session and 4 cross-session entries, identifying common trends across the games and apps. These diary entries ranged from 67 to 340

words in length, averaging approximately 146 words each. Table 1 details hours spent and diary entries for each VR game and app, with an example diary entry in Appendix B.

Video Recordings and Screenshots. Video recordings were captured throughout gameplay and application sessions to document instances of deceptive designs and user interactions in VR. Each session was experienced and screen-recorded using a Meta Quest 3 headset, with the recording paused after key privacy interactions, such as setting adjustments or consent agreements, to allow the lead researcher to immediately document reflections in a diary entry. The researcher repeatedly reviewed the video recordings during the diary entries to pinpoint moments of interaction with VR design mechanisms involving deceptive designs. This re-watching process enabled deeper reflection on how these designs might subtly influence user behavior and decision-making, which may not be immediately apparent during real-time interactions. Screenshots were also taken to visually support the text-based observational diary entries, with multiple screenshots taken for each design mechanism to provide clear insight into its design elements and functionality. The most illustrative screenshots and explanations of these design mechanisms are included in Appendix C. The diary entries, along with the corresponding video recordings and screenshots, were organized on Miro[9] for easier visual interpretation. Upon completing the autoethnography evaluation of all 12 VR games and apps, these data were then transferred to Dovetail[10] for thematic analysis.

3.2.3 Data Analysis. The lead researcher analyzed data using the *deductive reflective thematic analysis* method [18] to preserve the personal and reflexive nature of the autoethnography study [33, 60, 109] while enabling a "theoretically-informed exploration of qualitative data" [18, p. 263]. Prior studies have extensively used this method to analyze autoethnographic data (e.g., [33, 60, 72]). To offer transparency in our findings and interpretations [109], we provide a *Reflexivity Statement* that follows the recommendations for qualitative research [18, 85, 113].

Reflexivity Statement. To enhance the rigor of our qualitative research, we provide a *Reflexivity Statement* for our autoethnographic evaluation of VR games and apps to acknowledge potential biases in data coding and theme development, following guidance from the literature [18, 85, 113].

Our reflexive thematic analysis was led by our lead researcher who has a background in deceptive design and user privacy research, and has previously published on these topics in the context of VR and traditional computer environments (e.g., [55, 57, 59, 60]). Our research team's collective expertise in interaction design, usable privacy, and games user research also ensures the comprehensiveness and quality of our study.

The lead researcher self-identifies as empathetic and sensitive, with a strong emphasis on protecting personal boundaries. This personality sharpened the researcher's attention to subtle privacy intrusions and design patterns that exploit users' engagement with lifelike, responsive VR elements, but may have also influenced the focus and interpretation of the data compared to a typical VR user. We also acknowledge that the lead researcher's positive and negative personal experience with video games, VR technology, and deceptive design may have influenced the research.

Thematic Analysis. Our analysis primarily relied on an evolving *VR Deceptive Game Design Assessment Guide* [60] as our deductive codebook, given its integration of insights from foundational deceptive design works [11, 48, 50, 84] and VR and game-related [55, 68, 135] and privacy deceptive design frameworks [8, 21, 96]. We also draw insights from broader literature (as discussed in Section 2.1) to capture any deceptive design patterns beyond those in the codebook. We conducted the analysis in three stages. First, the lead researcher reviewed the data based on the deductive

[9]Miro—the Virtual Workspace for Innovation. https://miro.com/
[10]Dovetail—Thematic Analysis Software.https://dovetail.com/

codebook, with a focus on identifying potential deceptive designs in the privacy communication and interaction design mechanisms. In the second stage, the diary entries from the recordings were deductively coded. The video recordings and screenshots were used to verify the observations and reflections documented in the diaries. This involved an iterative coding process, where the analysis was continuously challenged and refined based on the researcher's critical insights and expertise in deceptive design within VR experiences. In the third stage, our research team collectively discussed the findings to ensure no key aspects were overlooked in the data. In the end, we identified and synthesized seven deceptive design patterns from privacy communication and interaction mechanisms of six VR games, and 14 patterns from six VR apps (see Table 2).

3.3 Privacy Policy Analysis

We analyzed the privacy policies of the selected VR games and apps, and compared them with findings from our design mechanics evaluation. This approach reveals the data collection and sharing practices of games [9, 110] and apps [14], and those in VR [10, 129]. Our goal was to uncover privacy issues and hidden data practices distorted by deceptive designs, which leave users vulnerable to unwanted data practices and unrecognized privacy risks.

3.3.1 Data Collection. We collected privacy policies for the selected VR games and apps from their official websites, accessed through the Meta Quest Store. Since these apps operate on the Meta Quest platform and rely on its device storage and functionality, we gathered this platform's privacy policy and found it shares the same privacy policy as the VR app *Meta Horizon Worlds*. Meta provides two privacy policies: the "Supplemental Meta Platforms Technologies Privacy Policy"[11] specifically for Meta's VR products and the broader "Meta Privacy Policy"[12] covering all Meta services, including Facebook and Messenger. For this research, we focused on the VR-specific policy and its related explanations about data practices, as the broader policy covers information about unrelated products. In total, the 12 privacy policies we collected cover both the data practices of the selected VR games and apps as well as their operating platform.

Since privacy policies often change with software updates, we collected them on the completion day of each autoethnography exploration. The Meta Quest Store privacy policy was collected in August 2024, after the final VR app evaluation. This approach ensured that our privacy policy analysis corresponded to the exact versions of the VR games and apps at the time of exploration. We manually downloaded the policies as PDF files. For multi-page policies, we compiled all content into a single PDF. This data collection process resulted in 12 PDF files, which were then uploaded to Dovetail[13] for analysis. Appendix E presents the retrieval dates of each privacy policy.

3.3.2 Data Analysis. Our analysis used a hybrid deductive-inductive approach [105, 125], which allows us to deductively analyze privacy policies using a theoretical framework from the literature [94, 119], while inductively developing codes directly from our observations and identifying themes specific to our data. Specifically, to capture a comprehensive picture of different elements such as personal information collected, sharing practices, purposes of use, and potential risks described in privacy policies [99], we adopted Nissenbaum's privacy as *contextual integrity (CI) framework* [94] as the starting point in our analysis. We were further inspired by Shvartzshnaider et al. [119]'s work on applying CI to privacy policies [34]. This deductive approach enabled us to systematically annotate, assess, and compare the *information flows* (i.e., a self-contained description

[11] Supplemental Meta Platforms Technologies Privacy policy (June, 20, 2024). https://www.meta.com/ca/legal/privacy-policy/. Last accessed on August 2, 2024.
[12] Meta Privacy Policy (June 26, 2024). https://www.facebook.com/privacy/policy/. Last accessed on July 28, 2024.
[13] See footnote 10.

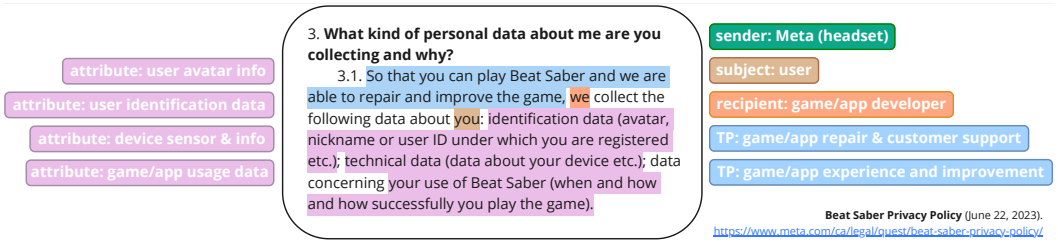


Fig. 2. TP=Transmission Principle. Example of our coding process using the contextual integrity framework (CI framework) [119] on a snippet of the privacy policy of VR game *Beat Saber*. Middle: The snippet; left and right: The respective thematic coding. The color of the codes correspond to the respective CI framework themes in our methodology description in Section 3.3.2.

of an information transfer) disclosed in the privacy policies [119]. In particular, we focused on codes relevant to the following five themes (colors correspond to the examples in Figure 2):

- **Sender.** Entities that transfer or share information, such as a person, company, website, or device. Examples include the "user" themselves and the "Meta" headset.
- **Recipient.** Entities that ultimately receive information, such as a person, company, website, or device. Examples include "app/game publisher" and "third-parties".
- **Transmission principle.** Conditions under which information transfers occur, such as in the "registration & subscription" process.
- **Attribute.** Type of information in the transfer, such as "game/app activity data" or "body, fitness, and health data".
- **Subject.** The individual whose information is transferred, either explicitly or implicitly, through pronouns or possessives. Examples include users (i.e., "you") and their friends (i.e., "your friends").

The lead researcher and a research assistant independently analyzed the 12 privacy policies uploaded to Dovetail[14]. The researchers began by familiarizing themselves with the data and taking rough notes of trends they observed. Then, three policies (25% of data) were randomly selected from the data and were read in detail and coded using inductive line-by-line coding based on the five themes from the CI framework [119] and any potential privacy issues and protection measures that appeared in the privacy policies. The researchers then met to address disagreements, refine codes, and collaboratively revisited the three policies to ensure insights were fully captured. In the second iteration, the two researchers independently analyzed five more policies (42% of data), held a discussion to compare coding results, refine and add to the codes, and collaboratively revisit the same five policies to ensure no neglected insights. In the final iteration, the remaining four privacy policies (33% of data) were independently analyzed, a discussion meeting was held, the codes were further refined and added to, and four policies were collaboratively revisited. Upon completing the coding process, the two researchers collaboratively discussed the larger patterns across the codes and grouped them into themes. Figure 2 presents an illustrative example of our line-by-line coding process. Figure 3 presents the user information flow revealed in privacy policies based on the CI framework themes [119]. Beyond the data practices, our researchers also noticed additional privacy issues and protective measures mentioned in the privacy policies, which we present in Table 4.

[14]See footnote 10.

4 Findings

We first present the findings from our autoethnography evaluation of the design mechanics, then ground these findings in our thematic analysis of their privacy policies and the operation platform—Meta Oculus Quest 3 headset. We go beyond VR games and apps' privacy-impacting design mechanics and provide insights into the types of user information collected and the purposes for which it is used. We discuss our findings in Section 5 within recent privacy deceptive design research (e.g., [9, 53, 54, 69]) and regulatory works (e.g., [46, 96, 101]), and draw implications for game and application designers, researchers, and policymakers in the VR field.

4.1 Deceptive Design Patterns in VR Privacy Communication Design Mechanisms

To address RQ1, our analysis of 59 diary entries identified five categories (themes) of 14 VR-adapted and VR-amplified deceptive design patterns that influence user privacy decisions. Although these patterns are previously observed from the mobile and web deceptive design literature [50, 60, 96], we focus our observations on the specific issues in the privacy communication and interaction design mechanisms in VR and how the effects of deceptive design are amplified by the technology.

This section describes the 14 deceptive design patterns in the sequence we experienced them within VR design mechanisms to illustrate how these patterns influence users' privacy decisions. For clarity, we denote VR games' and apps' titles in italics text (e.g., *Beat Saber*), use `monospace` font for deceptive design patterns (e.g., `Privacy Mazes`), and use quoted italics text for the descriptions directly extracted from the VR design mechanisms. To ensure a clear context for the findings presented in Table 2, we include each VR game and app's special icon (e.g., BS for *Beat Saber*) upon its first mention. Screenshots and short video clips of our researcher's interactions are available at OSF public repository: https://osf.io/axzve/.

4.1.1 Registration and Subscription Design Mechanisms. To access the core features, the VR apps *TRIPP* (TRIPP) and *Supernatural* (SN) require users to create independent accounts separate from their VR platform accounts, exemplifying the characteristics of `Forced Registration`. Furthermore, forcing users to disclose personal information through the registration process (i.e., `Privacy Zuckering`) is often not essential for the apps' functionality. For example, *TRIPP* asks users to provide their email address to start demo sessions, and unlocking all functionalities, including detailed privacy settings, requires users to register an account and pay a subscription fee with personal information like name and credit card details. In contrast, other VR games and apps operate without forcing registration, such as *Supernatural* which allows users to use their VR platform account during the first entry but requires account registration with their name and email address upon re-entry. While such design mechanisms may support cross-device experiences, they are unnecessary for users who only intend to use the applications in VR platforms.

Both *Supernatural* and *TRIPP* require users to pay a subscription fee. Our evaluation revealed that *Supernatural* employs `Endorsements and Testimonials` to entice potential subscribers to provide credit card information by promising positive experiences during the subscription process. However, the authenticity of these endorsements is questionable and likely comes from paid influencers rather than genuine users, as the highly polished, professional-looking photos far exceed the quality of typical user uploads (see Appendix C). At the same time, users are immersed in a realistic, vibrant, and lifelike environment that mirrors the beauty of natural surroundings. This combination creates a persuasive atmosphere, where users might feel compelled to provide payment information, believing the endorsements reflect authentic experiences.

Both VR apps' registration and subscription mechanisms also use `Visual Prominence` and `False Hierarchy`. *Supernatural*'s *"sign up"* and *"pairing additional user account"* options, which request users' personal information and details about others, are brightly colored and prominently

Table 2. Based on the VR Deceptive Game Design Assessment Guide from literature [50, 60], this table presents deceptive design we synthesized from our diary evaluation on the 12 VR games' and apps' privacy communication and interaction mechanisms.

Theme/Subtheme	Pattern	Description [50, 60]	Synthesized diary entries[a]	Mechanisms
Sneaking				
Hiding Information	Submissive Acceptance[b]	Trick users into accepting an agreement without prior access to the agreement content.	I feel tricked because agreement was assumed and I did not get to view the actual privacy policy. MOSS2 ROOM FISHER RABBIT LEGO IMRSD CHAT	Consent interactions
Obstruction				
Adding Steps	Privacy Mazes	Bury privacy controls under layers of confusing menus.	I feel irritated having to dig through various settings tabs to find data practices that affect my privacy. FISHER CLIMB	Settings & resources
Social Engineering				
Social Proof	Endorsements and Testimonials	Portray biased or fabricated testimonials as genuine to influence users' purchase decisions.	Seeing testimonials tempts me to enter my credit card for the free trial, even though I don't know if they are from genuine users or paid influencers. SN	Registration & subscription
Interface Interference				
Manipulating Choice Architecture	False Hierarchy	Prioritize certain options, make it difficult to compare choices.	I feel inclined to click on the "sign up" or "start the free trial", which grants access to my personal data, because they are higher positioned than other options. SN	Registration & subscription
	Visual Prominence	Highlight distracting elements, causing users to forget or lose focus on their initial intent.	I feel more likely to click the "sign up", "allow", and "start demo" options with bigger size and eye-catching colors, which grants access to my personal data, than other available options. ROOM CHAT TRIPP SN IMRSD	Registration & subscription, Consent interactions
Hidden Information	Hidden Information	Obscure crucial details or disguising them as unimportant.	I feel confused about why certain data are collected due to the missing privacy policy and privacy settings. MOSS2 ROOM FISHER RABBIT LEGO IMRSD	Consent interactions, Settings & resources
			I feel confused about why my media and photo library access is required since the permission was requested prior to viewing the privacy policy or using related function. CHAT	Consent interactions
Bad Defaults	Bad Defaults	Set default options that benefit the company, forcing users to manually change settings to avoid privacy risks.	I feel concerned about accidental data-sharing because the option is checked by default. ROOM CHAT HRZ	Settings & resources, Consent interactions
Emotional or Sensory Manipulation	Positive or Negative Framing	Hide or downplay critical information through visual cues.	I feel inclined to click on "accept", "agree", and "start demo" because the bright green buttons make me feel safe to do so. TRIPP SN	Registration & subscription, Consent interactions
Trick Questions	Trick Questions	Use confusing wording or double negatives to manipulate users' choices.	I feel tricked into revealing personal information because the game asked for my gender and skin color instead of asking "create your avatar." CLIMB	QoL features*
Language Inaccessibility	Complex & Lengthy Language[c]	Use hard-to-understand words and sentence structures, hindering users' informed decisions.	While the game/application has a privacy policy, it is too lengthy and hard to read. BS CLIMB CHAT HRZ TRIPP SN	Consent interactions

Note. Themes and codes in this table follow the sequence in our deductive codebook [60]. *QoL features = Quality-of-Life features.

a. VR games and apps acronyms match those in Table 1. VR game acronyms are colored Blue and VR application acronyms are colored Pink.

b. New deceptive design patterns synthesized from our diary entries, and are distinct from our initial codebook from literature [60].

c. We renamed the theme to highlight the "lengthy" issue in privacy policy language, in addition to the complexity noted in the original codebook [60].

positioned at the top. Similarly, *TRIPP*'s *"start demo"* option is visually emphasized when asking for users' email. These mechanisms use a bright green color for acceptance buttons for options that require financial commitment and careful consideration exemplifying `Positive or Negative Framing` by evoking emotional safety and subtly encouraging users to accept privacy-invasive options without fully understanding the implications of their choices.

Table 2 Continued. Based on the VR Deceptive Game Design Assessment Guide from literature [50, 60], this table presents deceptive design we synthesized from our diary evaluation on the 12 VR games' and apps' privacy communication and interaction mechanisms.

Theme/Subtheme	Pattern	Description [50, 60]	Synthesized diary entries[a]	Mechanisms
Forced Action				
Nagging	Nagging	Disrupt user focus with repeatedly unwanted interruptions to push actions they would rather avoid.	I feel annoyed by constant "permission error" messages because I didn't grant access to my photos and media. CHAT	Notification
Forced Registration	Forced Registration	Require account creation for tasks that shouldn't need it, potentially extracting unnecessary personal data.	I feel annoyed that nothing is accessible without registration, even after I paid for subscription. I have to sacrifice my privacy without knowing potential risks or if it's worth it. TRIPP SN	Registration & subscription
Forced Communication or Disclosure	Privacy Zuckering	Trick users into thinking it's essential for the service, leading to overshare personal data.	I feel pressured to give my credit card information to be able to see the item prices or demo session, and even after doing so I was asked for more personal details upon re-entry. BS SN	Registration & subscription, QoL features*
			I feel confused about granting media and photo library access as I do not see related functions. ROOM CHAT	Consent interactions
	Mandatory Acceptance[b]	Trick users into accepting all terms in the agreement without customization.	I feel coerced into agreeing to all data sharing practices because I cannot opt-out of those that are irrelevant to the functions. FISHER TRIPP SN	Settings & resources

Note. Themes and codes in this table follow the sequence in our deductive codebook [60]. *QoL features = Quality-of-Life features.

a. VR games and apps acronyms match those in Table 1. VR game acronyms are colored Blue and VR application acronyms are colored Pink.

b. New deceptive design patterns synthesized from our diary entries, and are distinct from our initial codebook from literature [60].

c. We renamed the theme to highlight the "lengthy" issue in privacy policy language, in addition to the complexity noted in the original codebook [60].

4.1.2 Consent Interaction Design Mechanisms. Upon launching, VR game *The Room VR* (ROOM) and the VR application *VRChat* (CHAT) prompt users to grant access to their *"photo, media, and files"* on the VR device, and the VR application *Immersed* (IMRSD) prompts users to grant access to their microphone. These permission request interfaces exhibit `Bad Defaults` by having *"Save my preference"* option checked by default and they use `Visual Prominence` by making the *"Allow"* option more visually bright and noticeable than other options. This combination of visual emphasis and default selection may cause users to grant access without fully considering or remembering their decision, potentially forgetting to revoke it later. Additionally, requesting such permissions in *The Room VR* which lacks related functions and in *VRChat* before users use relevant functions, can also be considered as `Privacy Zuckering`, as it may expose user data to unwanted usage.

Users are often prompted to review privacy policies before accessing core functions [9] in web and mobile games, but this is less common in VR. VR games like *Moss: Book II* (MOSS2), *The Room VR*, *A Fisherman's Tale* (FISHER), *Down the Rabbit Hole* (RABBIT), and *LEGO®Bricktales* (LEGO), and VR application *Immersed* lack a formal in-app privacy policy explaining what data is collected, by whom, and for what purpose. This lack of crucial privacy information demonstrates `Hidden Information` and leads to `Submissive Acceptance` of data practices without awareness. For instance, in *The Room VR*, users grant access to photos, media, and files without a clear reason. In *VRChat*, the privacy policy is presented only after permission requests. While the Meta Quest Store offers a link to the publisher's privacy policy at the bottom of the page, it is overshadowed by large video previews on top (see Figure 13 in Appendix), which can cause the link to go unnoticed.

While the VR game *Beat Saber* (BS) and apps *The Climb 2* (CLIMB), *VRChat*, *Meta Horizon Words* (HRZ), *TRIPP*, and *Supernatural* provide in-app privacy policies to inform users about data practices upon first entry, these documents are often lengthy and difficult to read. This complexity discourages users from fully reading the terms and hinders their comprehension of potential privacy

risks. Since content written above an 8th-grade reading level can be difficult for many people to understand [101, 132], they exhibit characteristics of `Complex & Lengthy Language`. Our findings from privacy policy analysis further support this observation (see Section 4.3.3 and Appendix E).

We further identified `Positive or Negative Framing` in the consent mechanisms in the VR application *TRIPP*, where the *"accept"* button is bright green. Despite being grayed-out until the *"I agree"* box is checked, the vibrant green color suggests emotional safety and may prompt users to accept the policy without fully reading the lengthy statements (see Appendix C).

4.1.3 Privacy Settings and Resource Design Mechanisms. During users' interaction with VR games and apps, having accessible privacy settings and resources is essential to their privacy. Our evaluation revealed the presence of `Privacy Mazes` in the VR game *A Fisherman's Tale* and the VR application *The Climb 2*. In *The Climb 2*, the privacy policy is buried three layers deep within the settings menu, requiring users to first navigate to *"Options"* among six menu items in the first layer, then find the *"Privacy Policy"* option in the second layer to open up the detailed privacy information on the third layer. Similarly, in *A Fisherman's Tale*, the game defaults to a *"standing"* gameplay posture without clear information about height calibration, which is only available under the settings menu. This convoluted design makes privacy information hard to find, and potentially discourages users from understanding data practices and privacy risks.

We also identified the use of `Bad Defaults` in the settings menu of VR apps *Meta Horizon Words*, including automatically turning on the microphone (*"people nearby can hear you talk"*), auto-joining the *"everyone"* voice channel, and automatic leaderboard participation (*"allow leaderboard to show your name and score in any world"*). While these features encourage social interaction, they may leave users who prefer to keep certain information private feeling exposed, such as automatically having their name displayed on a leaderboard without consenting. Although *VRChat* also auto-joins users to the world voice channel by default, we do not consider this privacy-invasive since the microphone is in "toggle" mode and remains off until manually activated.

Additionally, in *A Fisherman's Tale*, *TRIPP*, and *Supernatural*, users are subjected to `Mandatory Acceptance`, as they do not provide available settings for users to customize their privacy preferences without registration. Therefore, users are forced to consent to all publisher-stated data practices, even if these practices are irrelevant to the game's and application's functions.

4.1.4 Quality-of-Life Feature Design Mechanisms. Several quality-of-life (QoL) features—which are designs that make interaction smoother, more customizable, and enjoyable in VR games and apps—also employ privacy deceptive design patterns. In *The Climb 2*, users are initially asked to select their gender and skin color, framed as *"select your race and gender"*. Although this question is meant for avatar customization, the wording demonstrates the characteristic of `Trick Questions`. As users see the realistic rendering of their "hands" in the avatar creation process from a first-person perspective (see Appendix C), they may feel compelled to create avatars that resemble their real-life appearance. As a result, data from users' avatars can be used to infer their personal characteristics. Moreover, *Beat Saber* uses `Privacy Zuckering` when users must enter their credit card information before they can view and compare the prices of individual music and bundles.

4.1.5 Notification Design Mechanisms. The use of excessive permission notifications is common. In *VRChat*, we identified the use of `Nagging`, where users who select *"Not allow"* during the entry permission request are repeatedly interrupted by a *"permission error"* message each time they transfer to a different virtual interaction space (i.e., *"world"*). Users must press *"okay"* each time, which can become irritating and may ultimately grant permission to stop the interruptions.

Table 3. This table presents privacy-enhancing bright designs we identified from the 12 VR games and applications, and the desired ethical design strategies synthesized from our diary entries.

Bright Pattern[a]	Synthesized diary entries[b]	Interface
Accessible privacy policy	I feel satisfied that the privacy policy is accessible both at the start and in the menu for future checks. BS CLIMB CHAT HRZ TRIPP SN	Consent interactions
Unbiased presentation of choices	I feel relieved that all options are presented fairly and without bias, as I was not repeatedly prompted for permission after my initial refusal, and there was no misleading visual prominence or false hierarchy in the user agreement form and settings menu. ROOM HRZ	Consent interactions, Notification
Privacy-friendly default	I feel relieved knowing that the default settings respect my privacy concerns by leaving privacy-related options unchecked. CHAT TRIPP	Settings & resources
Private privacy configuration space	I feel relieved knowing that I can fine-tune my privacy settings and avatar in a private environment before joining other users. HRZ CHAT IMRSD	QoL features*
Transparent communication of data practices	I feel satisfied that the message clearly communicates the purpose of data collection, despite lacking details on its external purpose of use. ROOM HRZ	Notification
	I feel relieved that the microphone icon at my screen clearly communicates when my microphone is on or off. CHAT	QoL features*
	I feel relieved that the application specifies room privacy, which reduces my chance of accidentally entering a public space. IMRSD	QoL features*
Clear control mechanisms	I feel empowered knowing where in the menu I can control what gets shared with other players in the shared worlds. HRZ CHAT	Settings & resources
	I wish I could control my data sharing preferences beyond just other players to include the application and game publisher and external entities.	Settings & resources
Balanced privacy and functionality	I feel relieved that providing information like my pronouns, lifestyle, and VR preferences is not mandatory for my use of the functionality. CHAT SN	QoL features*
	I wish I could still participate in the leaderboard ranking without my name being publicly displayed.	Settings & resources

Note. *QoL features = Quality-of-Life features.

a. Patterns are organized by their frequency of appearance, with the most common among all VR games and apps at the top.

b. We included acronyms for VR games and apps, matching those in Table 1, from which the diary entries originated. VR game acronyms are colored **Blue** and VR app acronyms are colored **Pink**. Entries not linked to acronyms are desired ethical design strategies from our diary entries and do not exist in the selected VR games and apps.

4.2 Privacy-Enhancing "Bright Patterns" in VR

Through the lead researcher's autoethnographic documentation, we also noted several "bright patterns" [51, 130], as privacy-enhancing countermeasures of deceptive patterns. Similar to the previous section, game and application titles are italicized, "bright patterns" are set in `monospace` font, and verbatim descriptions from VR design mechanisms are set in quoted italics.

4.2.1 Consent Interaction Design Mechanisms. Our diary entries revealed that the VR game *Beat Saber* and VR apps *The Climb 2*, *VRChat*, *Meta Horizon Worlds*, *TRIPP*, and *Supernatural* all present an `accessible privacy policy` upon users' first entry and keep it accessible in the menu for later revisits. Of these, *Beat Saber*, *The Climb 2*, *VRChat*, *Meta Horizon Worlds* and *Supernatural* include the full privacy policy content within the menu alongside a hyperlink to an external page. In contrast, *TRIPP* only provides a hyperlink to an external privacy policy webpage. Although the language of these policies remains lengthy and complex (as noted in Section 4.1.2), making them available within core applications is an important first step toward improving the accessibility of privacy communication. Additionally, *Meta Horizon Worlds* avoided the use of visual prominence

in its permission request interfaces. Options in its user agreement form and the settings menu use balanced positions and consistent colors, exemplifying an `Unbiased presentation of choices`.

4.2.2 Privacy Settings and Resource Design Mechanisms. Both *VRChat* and *TRIPP* prioritize `privacy-friendly defaults` and allow users to opt-in based on their preferences. For instance, the acceptance box to user agreements is unchecked by default in both apps and the microphone is set to *"toggle"* mode to prevent unintended listening by others in *VRChat* (see Appendix D).

We found `clear control mechanisms` from *Meta Horizon Worlds* and *VRChat*, where illustrative images were used to guide users to navigate to the settings menu and manage specific controls (see Appendix D). The diary entries highlight a consistent desire for balanced privacy and functionality. For example, in *Meta Horizon Worlds*, privacy-conscious users are entirely excluded from leaderboard competition rather than being offered more inclusive options, such as hiding their nicknames on the leaderboard, allowing participation without compromising privacy.

4.2.3 Quality-of-Life Feature Design Mechanisms. *Meta Horizon Worlds* and *VRChat* offer private onboarding spaces and *Immersed* allows users to learn privacy controls in a single-user workspace before joining public areas (`private privacy configuration space`). Furthermore, *Immersed* clearly labels virtual workspaces as *"private"* or *"public"*, and *VRChat* implemented a microphone icon on the screen to keep users constantly aware of their microphone status (see Appendix D).

VRChat and *Supernatural* also maintained `balanced privacy and functionality` in their QoL features. While *VRChat* asks users to provide information such as lifestyle and social preferences to help find matching friends, it is optional. In *Supernatural*, users are asked to choose their fitness goal and preferred music genre for fitness sessions, with the options to skip these steps.

4.2.4 Notification Design Mechanisms. Unlike *VRChat*'s nagging tactics, *The Room VR* does not repetitively prompt users after denying permission for photos, media, and files (`Unbiased presentation of choices`). We further found `transparent communication of data practices` from *The Room VR*, *VRChat*, and *Meta Horizon Worlds*. These apps provide brief descriptions of data practices upon entry and during data collection that clearly state what is collected and its purpose. For example, *The Room VR* notifies users when their height is calibrated for gameplay.

Overall, the VR "bright patterns" demonstrate that fair and balanced design mechanisms can be implemented in privacy communication and interaction design mechanisms. Unlike deceptive designs, "bright patterns" promote transparent privacy communication, preserve user autonomy in privacy decisions, and allow users to manage their privacy while preserving user experience.

4.3 VR Information Flows from Privacy Policy Statements

To identify data practices and potential privacy risks users may unknowingly face, we addressed RQ2 by conducting a thematic analysis of the privacy policies of the 12 VR games and apps, and their operating VR platform, Meta Oculus Quest, using the Contextual Integrity framework (CI) [119].

We identified 1,222 information flows from 209 policy statements across 12 privacy policies (see Figure 3). The sender layers in the diagram are superimposed in the paper to provide a high-level overview showing the complexity of information flows across the five CI framework themes: (1) sender, (2) attribute, (3) subject, (4) transmission principle, and (5) recipient. Section 3.3.2 includes a detailed explanation of each CI framework theme in our analysis, and Appendix F provides a layer-by-layer breakdown of the information flows specific to each sender.

We acknowledge that despite our efforts to accurately classify and differentiate information flows, ambiguous language in privacy policies sometimes limited our precision. This occurred when multiple CI factors were grouped together in policy statements. In these cases where a single statement involves multiple instances of the same CI factor, we derived multiple information flows

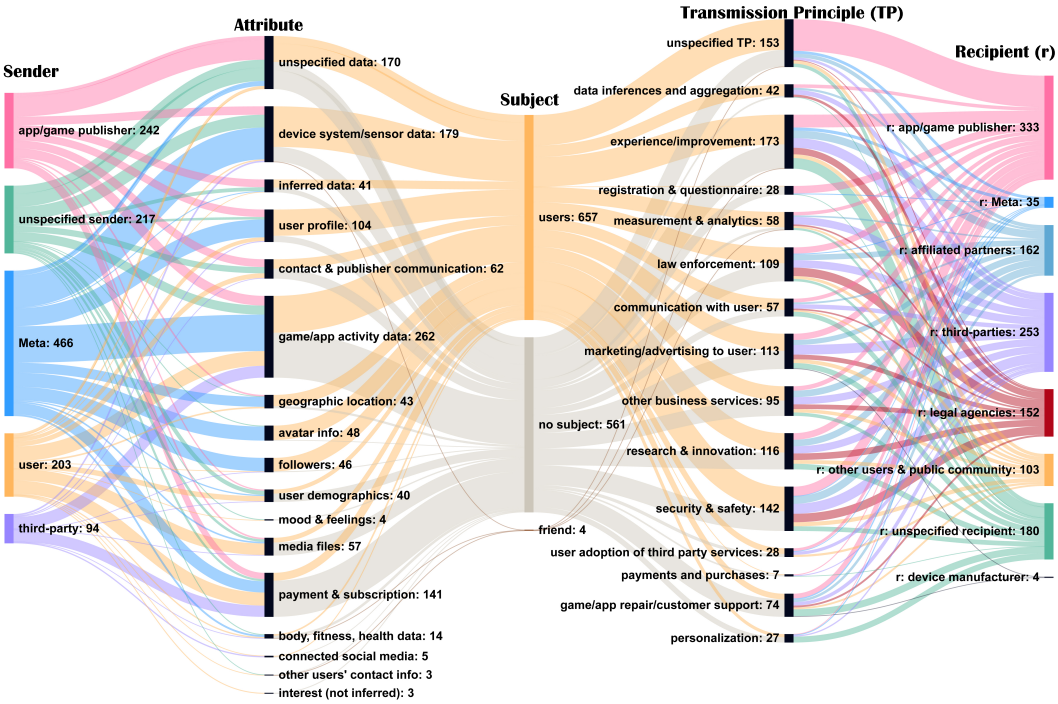


Fig. 3. This Sankey Diagram visualizes the 1222 information flows from 209 privacy policy statements through our thematic analysis of 12 privacy policies. The diagram moves from left to right, showing the codes in information flows across the five CI framework themes. For example, "app/game publisher" appears as the sender in 242 flows. Colors distinguish different information flows. For example, colors flowing from *sender* to *attribute* identify the sender of an *attribute*. A detailed breakdown of the layers is available in Appendix F.

from the statement. For example, if an *attribute* is transmitted to various *recipients*, the transmission to each *recipient* represents a separate information flow. Despite this limitation inherited from the ambiguity in privacy policies, we believe the CI classification still offers valuable insights into the broader patterns of data collection and sharing in VR apps.

In reporting our analysis, game and application titles are italicized (e.g., *Beat Saber*), codes from thematic analysis themes are placed in quotations ("game/app publisher"), and direct descriptions from VR design mechanisms are in quoted italics. "Information flows" is abbreviated as "i-flows".

4.3.1 Sender, Recipient, and Subject in the Information Flows. As summarized in Figure 3, our analysis identified five primary senders in the data transmissions: "Meta", "app/game publisher", "user", "third-party", and "unspecified sender". "Meta," the operational platform for VR games and apps and the publisher of *Meta Horizon Worlds*, acted as the sender in 466 (38%) i-flows. This reflects "Meta"'s role as the data handler and intermediary between users and other entities in the data flow. In less than a quarter of i-flows (n = 242, 20%), the "app/game publisher" acted as the sender by outsourcing data processing tasks, such as analytics, marketing, and user support, to third-party service providers. In these cases, they transmitted the collected information about users and their devices to external parties. In 203 (17%) i-flows, the "user" acted as the sender by actively providing or entering data, such as during the registration process or interacting with game or application features. In a few cases (n = 94, 8%), "third-party services" acted as the sender when VR games and apps allowed users to sync data from external devices and services, such as health information

from wearable devices. We also identified 217 (18%) i-flows where no clear sender ("unspecified sender") was identified due to the fragmented presentation of information within policy sections, which leaves the point of origin of the data ambiguous.

Our analysis identified eight primary recipients of user data. The "app/game publisher" was the recipient of 333 (27%) i-flows, and their "affiliated partner companies", such as parent companies, subsidiaries, and joint ventures, were involved in some (n = 162, 13%). Contractual "third-party" service providers, such as marketing, service, and analytics vendors, served as the recipient of 253 (21%) i-flows. "Legal agencies", including government authorities and professional advisors (e.g., lawyers, auditors, insurers), were recipients in 152 (12%) i-flows. "Other users & public community" were less involved as recipients (n = 103, 8%) in games and apps with public interaction spaces. The VR operational platform "Meta" was the recipient in 35 (3%) i-flows, often in collaboration with the publisher for legal requests, protection activities, customer support, and other user-related activities. The VR "device manufacturer" was a minor recipient (n = 4, <1%), primarily for device improvements and system-related needs. 180 (15%) i-flows had "unspecified recipient".

We identified two primary subjects indirectly involved in the data transmission. Around half are "users" (n = 657, 54%) and only a few are "friends" (n = 4, <1%). We applied "no subject" to 561 (46%) i-flows when they are directly involved in data transmission as the sender or recipient.

The wide range of senders and recipients involved in the i-flows shows that user data can be distributed across various entities beyond the user's knowledge. Many of these entities, such as "affiliated partners" and "third-parties", are not directly facilitating core functions or promised services. Additionally, many policy statements have vague unspecified senders and recipients. Given the deceptive design practices identified in Section 4.1, the lack of transparent communication and diminished user agency in user agreements becomes even more concerning.

4.3.2 Attribute and Transmission Principle. As demonstrated in Figure 3, we identified 17 data attributes transmitted across 15 transmission principles. Only a small portion supported core functionality "experience/improvements" (n = 173, 14%), promised services, or tailored "personalization" (n = 27, 2%). For example, fitness and meditation apps rely on "body, fitness, health data" (n = 14, 1%), "mood & feelings" (n = 4, <1%), and users' "interest" (n = 3, <1%). Social VR platforms collect "user profile" (n = 104, 8%), "avatar information" (n = 48, 4%), and "media files" (n = 57, 5%). VR games monitor users' "game/app activity data" (n = 262, 21%) and "device system/sensor data" (n = 179, 15%). Apps require a registration and subscription process users' "payment & subscription" details (n = 141, 12%) and for "payments and purchases" (n = 7, <1%). Upon "user adoption of third party services", only 2% (n = 28) of the apps transmit their data to external services.

Some data transmissions, while not essential to core functionality, are apparent in user interactions. These include "user demographics" (n = 40, 3%) and "connected social media" (n = 5, <1%) collected during "registration & questionnaire" (n = 28, 2%) for account creation and social media synchronization. Additionally, when users request "game/app repair/customer support" (n = 74, 6%), their "contact & publisher communication" (n = 62, 5%) are necessarily transmitted.

Beyond these apparent uses, many data attributes are transmitted under less apparent principles but still contribute to enhancing UX and protection. These transmission principles include "measurement & analytics" (n = 58, 5%), "research & innovation" (n = 116, 9%), "security & safety" (n = 142, 12%), "law enforcement" (n = 109, 9%), and "communication with user" (n = 57, 5%).

In contrast, many data attributes are transmitted covertly under principles that do not align with user interests or core VR functionality, primarily benefiting publishers while potentially compromising user privacy. For instance, we found i-flows involving "inferred data" (n = 41, 3%) from "data inferences and aggregation" (n = 42, 3%) that can reveal more information about users than they intend to disclose [89, 104]. Users' "geographic location" (n = 43, 4%) and "followers"

Table 4. Final themes from our thematic analysis of 12 VR privacy policies and the Meta Quest platform.

Theme/Code	**Description**[a]	**Example policy statements**
Privacy Inhibitors		
Plethora of policies	Multiple distinct privacy policies linked within a single main policy, requiring users to click on each link to fully understand their privacy rights and data practices. MOSS2 FISHER RABBIT CHAT HRZ TRIPP SN	"Learn more about the Hand and Body Tracking feature... [URL]." — Meta Quest Platform & Meta Horizon Worlds Privacy Policy (06/20/2024)
Blurred accountability	Unclear responsibility for user data management, obligations, and liability when data is transmitted with third-parties and entities in jurisdictions internationally. MOSS2 FISHER RABBIT LEGO CHAT HRZ TRIPP SN	"You will need to apply these opt-out settings... We cannot offer any assurance as to whether the companies we work with participate in the opt-out programs." — TRIPP Privacy Policy (11/30/2023)
No clear retention period	Ambiguous duration of user data retention without specifying timeframes or conditions for automatic data deletion. MOSS2 FISHER RABBIT CHAT HRZ TRIPP SN	"User data is stored indefinitely on Immersed servers." — Immersed Privacy Policy (08/01/2024)
Missing/unclear information	Vague statements that fail to distinguish between VR games and apps and other services, or lack details about VR games and apps entirely. MOSS2 ROOM RABBIT CHAT TRIPP SN	"This privacy and data policy applies and has effect in respects of all games, related online services..." — The Room VR Privacy Policy (02/14/2022)
Submissive consent	Assumed user consent to data practices based solely on their download or use of VR games and apps, or claims that user consent is unnecessary due to "legitimate reasons." MOSS2 ROOM	"We do not need your consent as for all forms of processing, we have other legitimate reasons..." — Beat Saber Privacy Policy (06/22/2023)
False rights	Statements create illusion of user rights without actual provision, such as claiming sharing user data based on their consent without having explicit consent design mechanisms, and offering limited, revocable rights that are contingent on the company's interpretation of "legitimate interests." FISHER RABBIT LEGO IMRSD	"... the processing is carried out with your consent..." — LEGO®Bricktales (11/30/2023) but we did not observe an explicit consent form in the game (see Table 2)
User-burdening policy	Statements that impose excessive restrictions or obligations on users, such as requiring users to forfeit security and privacy expectations for data, and irrevocably grant the publisher all rights to user data exchanged within the game. RABBIT SN	"We cannot and do not guarantee the security of your personal information and you transmit such information at your own risk." — Supernatural Privacy Policy (07/01/2024)

Note. a. We included acronyms for VR games and apps, matching those in Table 1, indicating the source of each privacy policy statement. VR game acronyms are colored **Blue** and VR application acronyms are colored **Pink**.

(n = 46, 4%) were often shared for unclear purposes, such as ("other business services" (n = 95, 8%) or entirely "unspecified TP" (n = 153, 13%). While not encountered in our diary evaluation, the privacy policies of *TRIPP* and *Supernatural* revealed their referral features that require "other users' contact info" (n = 3, <1%), which may result in unwanted contact. Additionally, we identified 170 (14%) i-flows with vague and "unspecified data". All these data attributes can be used for "marketing/advertising to users", as shown in 113 (9%) i-flows.

The diverse data attributes and transmission principles reveal the complexity of information flows. The deceptive design patterns in privacy communication and interaction mechanisms (as discussed in Section 4.1) further exacerbate the difficulty in user understanding and privacy decision-making. Even when users share personal data for enhanced gameplay purposes, they may unintentionally expose themselves to undisclosed and subtly disguised data practices.

Table 4 Continued. Final themes from our thematic analysis of 12 VR privacy policies and the Meta Quest platform.

Theme/Code	Description[a]	Example policy statements
Protective Measures		
Security & privacy protections	Protective measures like encryption, data minimization, disassociation from user accounts, restrictions on unauthorized activities, physical safeguards, privacy-friendly defaults, and ensuring third-party security practices. BS MOSS2 ROOM FISHER RABBIT LEGO CLIMB CHAT HRZ TRIPP SN IMRSD	"This [user data] is made available to us in aggregated form and we are not able to single out any one individual from this data..." — The Room VR Privacy Policy (02/14/2022)
Information on post-collection rights & notification	Clear notification about privacy policy updates and guidelines on users' rights to their data, including access, correction, and deletion, along with the publisher's contact information for related requests. BS MOSS2 ROOM FISHER RABBIT LEGO CLIMB CHAT HRZ TRIPP SN IMRSD	"Users can request the deletion of their data at any time by clicking on the 'Delete User Data' option or by emailing us at ... " — Immersed Privacy Policy (08/01/2024)
Proactive consent	Obtain explicit user consent before sharing personal data. Those that claimed to obtain user consent but do not have a consent interface in the VR games and apps are categorized as "false rights." HRZ TRIPP SN	"For sensitive personal information that we collect, we will use or disclose it with your specific consent..." — Supernatural Privacy Policy (07/01/2024)
Country-specific information	Privacy details tailored for users in specific regions, such as the European Economic Area (EEA), United States, United Kingdom, Switzerland, and Korea. BS MOSS2 ROOM FISHER RABBIT LEGO CLIMB CHAT TRIPP SN	"As a European resident, you also have the right to..." — The Climb 2 Privacy Policy (n.d.)
Children-specific instructions	Guidelines for children on data collection, non-collection, and how to request access, correction, or deletion of their data, with advice on involving parents. MOSS2 ROOM RABBIT CHAT HRZ TRIPP SN	"To provide social features your child's Meta Horizon profile will be set to private by default..." — Meta Quest Platform & Meta Horizon Worlds Privacy Policy (06/20/2024)
Direct guidance & communication	Explicit guidelines on adjusting settings to prevent unwanted data collection, along with transparent information on how user data is processed, shared with third parties, for what purpose. CHAT HRZ IMRSD	"If you pay for access to certain features... we may use your personal information to provide you access to them... If you request approval to... we may use your personal information to decide whether to grant your request..." — VRChat Privacy Policy (11/22/2023)

Note. a. We included acronyms for VR games and apps, matching those in Table 1, indicating the source of each privacy policy statement. VR game acronyms are colored **Blue** and VR application acronyms are colored **Pink**.

4.3.3 Complexity, Ambiguity, Omission, and Deception in the Policy Statements Introduce Further Privacy Barriers. Beyond complex information flows, our thematic analysis uncovered additional privacy issues within the 12 privacy policies. As demonstrated in Table 4, three VR games and four VR apps presented a "plethora of policies", where multiple distinct policies are linked within a single main policy. This forces users to navigate several documents to fully understand their privacy rights and data practices. We also identified "blurred accountability" in four VR games and four apps, where responsibility for data management, obligations, and liability is unclear.

The privacy policies of three VR games and four apps also exhibited "no clear retention period", as they do not specify time frames or conditions for data removal. Additionally, we found "missing/unclear information" in three VR games and four apps, where statements failed to differentiate between VR services and other platforms, or lacked information on VR data entirely, leaving users confused about how their data is handled in the VR context.

We also identified "submissive consent" in the privacy policies of two VR games, where user consent is implied through the act of downloading or using the games. Some policies even suggested that consent was unnecessary for *"legitimate reasons."* Additionally, we found "false rights" in the privacy policies of three VR games and two VR apps to create an illusion of user rights without actual provision. This included requiring users to agree to terms without explicit consent mechanisms in the game or application, and offering revocable rights subject to the company's interpretation of *"legitimate interests."* Finally, we identified "user-burdening policies" in the VR game *Down the Rabbit Hole* and the VR application *Supernatural*. These policies impose restrictions or obligations on users, such as requiring users to forfeit security and privacy expectations for their data and irrevocably granting the publisher all rights to user data exchanged within the game.

> *"We do not need your consent as for all forms of processing, we have other legitimate reasons because this is necessary for fulfillment of agreement or it is in our legitimate interest."*
>
> — *Beat Saber Privacy Policy (06/22/2023)*

To assess the challenge of interpreting convoluted privacy policy language, we evaluated the readability of the 12 selected policies using the Flesch Reading Ease Score in Microsoft 365, following the literature's approach [46]. Appendix E shows the results, with lower scores indicating more difficult content requiring higher education levels to understand. We found that all 12 privacy policies scored between 30 and 50, which indicates they are *"difficult to read"* and require at least a *"college-level"* understanding[15]. These findings align with our earlier identification of `Complex & Lengthy Language` in VR design mechanisms, as discussed in Section 4.3.

4.3.4 Clarity, Proactiveness, and Guidance in Privacy Policies Ease User Concern on Privacy. Our analysis also uncovered various approaches by publishers to ensure transparent privacy communication and protect user privacy, although these measures vary across different VR games and apps. As shown in Table 4, all 12 privacy policies reported implementing a range of "security & privacy protections", such as encryption, data minimization, disassociation from user accounts, restrictions on unauthorized activities, physical safeguards, privacy-friendly defaults, and adherence to third-party security practices. These measures reflect the publishers' commitment to safeguarding user data. Additionally, the privacy policies for all 12 VR games and apps clearly present "information on post-collection rights & notification", including users' rights to access, correct, and delete their data, as well as updates on privacy policies. They also provide contact information for users to exercise these rights, which ultimately enhances user control over their personal information after collection. Moreover, the publishers of three VR apps claimed to obtain "proactive consent" from users before processing certain data and implemented an explicit consent mechanism, which is a genuine effort compared to "false rights" that merely claim consent without effective mechanisms.

Moreover, we found that the privacy policies of six VR games and four VR apps included "country-specific information" with tailored privacy details for users in specific regions such as the European Economic Area (EEA), United States, United Kingdom, Switzerland, and Korea. This information clarifies publishers' compliance with local regulations and provides users with relevant legal context. Additionally, the privacy policies of three VR games and four VR apps offered "children-specific instructions" that outline data collection practices for minors, including non-collection policies and guidance on requesting access, correction, or deletion of their data. These policies often advise children to seek parental involvement in privacy-related decisions.

[15] Flesch-Kincaid readability tests. (n.d.). In Wikipedia. Retrieved April 14, 2023, from https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests

Finally, three VR apps offered "direct guidance & communication" by offering explicit guidelines on adjusting settings to prevent unwanted data collection. They are also transparent about how user data is processed, shared, and for what purposes. An exemplary privacy policy is from *Meta Horizon Worlds*, where representative icons were used to illustrate different types of data collection (e.g., motion tracking, eye tracking) to improve user understanding of data practices.

> *"The software fits a generic hand and body model over the estimated [approximate] points on your hands and body,... to ensure hand and body tracking works properly; this data will be deleted within 90 days..."*
>
> — *Meta Privacy Policy (06/20/2024).*

5 Discussion

In this section, we contextualize our findings within existing research (e.g., [9, 53, 54, 69]) and regulatory efforts (e.g., [46, 96, 101]) on VR privacy in Section 5.1. In Section 5.2, we provide design recommendations for VR researchers, designers, and policymakers to mitigate deceptive practices, prioritize user privacy, and improve user awareness and control.

5.1 Deceptive Design in Immersive VR Compared to Web and Mobile Platforms

Some deceptive design patterns from mobile and web are amplified by VR's unique features, while others were absent due to VR design mechanisms that are distinct from other platforms.

5.1.1 Migration of Deceptive Design Practices From Mobile and Web Platforms to VR. Our analysis reveals a disconcerting migration of deceptive design patterns from mobile and web platforms into VR environments [46, 53, 54]. We observed `submissive acceptance` in VR design mechanisms and `false rights` in privacy policies that align with issues of assumed consent and illusory mandatory permissions from prior mobile and web research [53, 54]. This coercion forces users to accept all data practices without opt-out options (`mandatory acceptance`), which further resembles the bundled consent problem [6, 53, 54, 77]. The convoluted privacy settings in VR apps (`privacy maze`) reflect similar challenges in web environments [46], while the issue of missing privacy information and settings (`hidden information`) parallels issues with lacking configure buttons and privacy policies on websites [53, 54]. Similarly, `bad defaults` and `forced registration` in VR privacy settings and consent forms resemble issues found on the web and mobile environments [8, 46, 48, 54].

Many VR games and apps lacked privacy policies, and those that had one often used `complex & lengthy language` that reflected similar *"information overload"* [54] challenges found in website and game privacy policies [46, 111]. We also identified `nagging` notifications in VR, similar to those seen in mobile and web contexts [53]. The presence of games and apps separate from the policy of their VR platforms further complicates users' comprehension, as they have to navigate and understand both without a clear connection between them [9]. Additionally, we found `false hierarchy` and `visual prominence` in VR, such as bright-colored buttons, echoing the grayed-out options that subtly steer user behavior in web and mobile environments [53, 54].

The migration of deceptive design patterns into VR represents a concerning threat, as the lack of sufficient disclosure of their data collection practices of VR applications can worsen with deceptive design practices [9, 71]. Our identified patterns still rely heavily on 2D interface elements in VR, such as menu screens and pop-up notifications, rather than fully capitalizing VR's 3D features (e.g., unbounded displays, whole-body interaction, and motion sensing) [69]. In other words, we found that immersive features, although enhance the effectiveness of deceptive patterns, do not directly enable them in the applications. Thus, these patterns may also appear in other immersive technologies, such as Augmented Reality and Mixed Reality, and in other interactive digital media

that use 2D interfaces for privacy communication and interaction. The combination of these designs and the ambiguous privacy policies can significantly disadvantage users. This challenge is exacerbated by immersive technologies' extensive, continuous, and granular data collection, which often is not recognized by users [13, 59, 89].

5.1.2 VR Amplifies the Impact of Deceptive Design on User Privacy. We found that several deceptive design patterns documented in mobile and web literature (e.g., [12, 50, 82, 96]) are amplified by features unique to VR [55, 69]. One example is that the artificial `endorsement and testimonials` discussed in Section 4.1.1 used as social proof to encourage payment information disclosure [50, 82] can become more problematic in VR. This is because, unlike mobile or web contexts where users can easily pause and seek external information on a secondary device, the occlusion of reality by wearing a VR headset [69] and the disruption of closing the application to switch to a browser in VR discourage users from doing so. This barrier, combined with the lack of demo or trial options, forces users to rely solely on in-app endorsements to assess the value of services (detailed in Section 4.1.1). Similarly, we observed that the VR application *TRIPP* provided hyperlinks to its privacy policy and terms of service during user registration, as discussed in the `accessible privacy policy` pattern in Section 4.2.1). While this is common in web and mobile environments (e.g., on Steam [9]), users can quickly open a new tab to skim the content. In VR, accessing these external links can be disruptive because users must exit the running application. This disruption makes accessing external resources in VR more difficult.

The realistic rendering of virtual elements in VR can also enhance the effectiveness of `trick questions` [12, 82, 96]. One example is the avatar creation mechanisms we observed in *The Climb 2*, where users are prompted to select their gender and race while viewing realistic virtual "hands" from a first-person perspective (see Appendix C). This avatar creation process is designed to resemble the user but blurs the line between voluntary choices and subtle manipulation [55, 69]. Section 4.3.2 shows that the fusion of virtual representation and physical identity may cause users to disclose personal characteristics without fully realizing how their data is shared with third parties.

We did not observe deceptive patterns that relied on VR's "device sensing" features, nor evidence of hyper-personalized manipulations as discussed in the literature [55, 69]. This may be due to most current VR apps needing to focus on functionality over advanced data-driven manipulation. Although our privacy policy analysis revealed that VR data are used for marketing (see Section 4.3.2), these can be legitimate business strategies when executed correctly [12]. Therefore, we argue that the current VR data collection primarily aims to ensure safety and facilitate VR interaction rather than deceive users.

5.1.3 Absence of Some Common 2D Deceptive Design Patterns in VR Due to Modality Differences. Our analysis in Section 4.1 reveals differences in privacy communication and interaction mechanisms between VR and traditional web or mobile platforms that have led to the absence of many common deceptive design patterns. For instance, we did not encounter problems with settings that cannot be saved [53], as privacy settings were often missing entirely in VR (`hidden information`). Similarly, deceptive patterns used in account deletion and logout, common on mobile and web platforms [46, 53, 101], were mostly absent because most VR apps do not require separate accounts beyond the one tied to the VR headset. However, the challenge of data deletion remains. Section 4.3.4 shows that while privacy policies outline users' post-collection data rights and provide contact information for data deletion requests, requesting data removal needs significant user effort such as filling out lengthy forms or sending personalized email requests. This can be viewed as a form of "obstruction" that discourages users from initiating the process [12, 50].

Cookie banners common in web platforms [46, 54] are noticeably absent in VR contexts. We found consent interactions are mostly submissive and paired with deceptive patterns, and privacy

policies are often missing in VR environments. While deceptive consent practices are ethically concerning, the complete absence of explicit consent mechanisms presents an even greater issue.

5.2 Implications for Privacy-Enhancing Designs in VR Games and Applications

Based on our findings on privacy-enhancing "bright patterns" in VR communication and interaction mechanisms (see Table 3), and good practices in publishers' privacy policies (see Table 4), we provide strategies on counteracting deceptive tactics, refining privacy communication and interaction designs, and tailoring privacy policies to users' needs.

5.2.1 Role of Privacy in VR Self-Expression and Social Interactions. Avatars in VR are perceived as digital extensions of users' personal identities [93], as directly experienced and documented by the lead researcher in Section 4.2.3 and Appendix B during the process of personalizing the avatar to create a strong connection between the virtual self and real-world image that is reinforced by the first-person perspective in VR. The literature suggests that the desire to present an ideal self in VR is driven by the need to align with societal norms [93]. Our lead researcher's decision to conceal sensitive details, such as default username, indicates that users may also project their privacy concerns onto their avatars. Research has proposed privacy-protecting methods like blurring effects and avatar reconstruction [30, 134], but these are not ideal for VR, as they unavoidably hinder social interaction and negatively impact user experience. The `private privacy configuration space` offers a more practical solution, as it allows users to configure their avatars based on privacy concerns in a private setting. This capability of managing their avatar gives users a sense of control over their self-representation and helps them maintain privacy in VR public spaces. However, avatars that closely resemble users can still be used for profiling, as avatar customization choices may reveal personal characteristics, demographic information, and health issues [30, 74, 81, 126]. Future research should further explore the phenomenon of projecting personal privacy concerns onto self-representation in virtual worlds as a crucial aspect of examining the privacy implications of VR technology and preserving user privacy.

5.2.2 VR "Bright Patterns" as Countermeasures to Deceptive Design. We identified several "bright patterns" (See Table 3) that offer exemplary privacy-enhancing alternatives to deceptive designs. Literature suggests that designers often rely on established industry conventions and some deceptive patterns were initially created to organize the UI and reduce visual complexity [137]. To guide designers toward more ethical practices, we suggest adopting VR-specific "bright patterns" as privacy-friendly standards. "Bright patterns" have been explored in 2D websites and mobile environments [51, 114, 130]. Our observed "bright patterns" in VR reflect and extend those documented in prior literature [51, 114, 130]. For example, our observed `privacy-friendly default` resembles the unchecked checkboxes from lab experiments [130] and website observations [114], while the `transparent communication of data practices` reflects the "dumb it down" bright pattern [114]. However, our analysis also identifies novel "bright patterns", such as `private privacy configuration space` and `balanced privacy and functionality` (see Table 3), which are not covered in existing research. This gap highlights the need for further research to expand the "bright patterns" beyond websites and develop privacy-friendly bright design standards tailored to immersive environments.

In addition, current mitigation strategies for deceptive designs, such as browser alerts and warning messages [115], may suffer from issues like software bugs, maintenance failures, and profit motives that undermine its long-term reliability and trust, as seen with digital certificates' failures to alter malicious websites [56, 64]. We encourage future research to expand on "bright patterns" literature [114, 130] and our findings by not only identifying deceptive designs but also drawing from ethical design practices to develop a standardized and accessible bright design toolkit for VR

designers. As designers often prioritize business goals over user convenience due to challenges in justifying privacy-enhancing choices [137], we believe that providing concrete, research-backed examples of "bright patterns" can empower them to make stronger cases for ethical design decisions.

5.2.3 Towards Effective VR Privacy Communication and Notifications. Literature suggests that personalized alerts during data collection improve user awareness and comprehension [9, 40]. Our analysis in Section 4.2.4 shows that although just-in-time privacy notifications are not widely adopted in VR, the few examples we observed are useful in informing users about data practices at the moment they occur. This communication approach is particularly useful in VR because users may not fully understand data collection implications from reading a standard privacy policy outside the VR context [59]. However, designing notifications in VR can be challenging. Existing approaches, such as head-up displays, haptic feedback, floating displays, and in-situ notifications on virtual objects [112], are often missed by the users due to other rich information and feedback in VR [45]. On the other hand, notifications that demand attention can disrupt users' VR experience [44]. Although some studies have explored optimal moments for delivering notifications (e.g., [17, 136]), this remains an unsolved issue that requires continuous research. Beyond notifications, Schaub et al. [116] developed a design space for privacy notices to help system practitioners conceptualize and implement effective privacy notices. Feng et al. [38] later extended this design space by incorporating necessary design dimensions for privacy controls. While some of these design dimensions, such as timing, delivery, and modality, can enhance privacy communication in VR [38, 116], further research is needed to adapt this space for VR-specific features such as unbounded displays, whole-body interaction, motion sensing, and personalized, context-aware privacy controls enabled by granular sensor data [55, 59, 69].

5.2.4 Independent Privacy Policy Dedicated to VR. Through our analysis in Section 4.3.3, we found that VR games and apps from publishers that offer services on multiple platforms, such as computers, mobile, and websites, often provided a general privacy policy that did not clearly distinguish VR-specific privacy concerns. Even when attempts were made to differentiate services using bolded indicator terms, the policy statements often used non-VR examples and failed to clarify privacy implications in VR. Since users generally have limited familiarity with these practices and often rely on their non-VR experiences in making privacy decisions [60], we argue that it is crucial to provide clear, accessible information to facilitate users' understanding. The data processing descriptions in *Meta Horizon World*'s privacy policy serve as a good example, despite suffering from the "plethora of policies" issue. We recommend that VR games and apps available across platforms adopt a VR-specific privacy policy to clearly address the unique privacy concerns of immersive technologies, including transparent explanations of how biometric data, such as movement patterns or physiological responses, are collected and used [89, 104].

5.2.5 Accessible Privacy Policies Optimized for VR Environments. Informing users about a system's data practices is crucial for facilitating their informed privacy decisions [116]. However, our selected VR games and apps' privacy policies remain complex, text-heavy, and reliant on 2D interfaces (see Appendix C). Some also include child-specific privacy instructions aimed at guiding both children and parents on protecting children's privacy (see Section 4.3.4). However, our analysis shows that these instructions appeared to be buried within the lengthy policies and were difficult to act upon. Although government agencies encourage user-friendly policy designs [46] and mandate special protections for children [1, 62], in practice, compliance with legal obligations tends to take priority over user experience due to pressures from compliance teams, senior managers, and security experts, despite designers recognizing the challenges users face [137]. However, overloading users with details can be counterproductive [37, 90, 106].

The selected VR games and apps often provide a hyperlink to privacy policies on their official websites, but this approach appeared to be insufficient without making the full policy accessible within the VR environment (see Section 4.1.2), as users are likely to ignore it [9]. Instead, we recommend presenting privacy policies upfront [17] before users engage with the VR experience, similar to the way they are shown on computers and mobile devices [9], while ensuring the information is accessible within the application for future reference. VR privacy policies may also harness the features of VR technology. For example, previous studies have used AR technology to visualize smart home device data flows (e.g., [5, 23]). VR privacy policies can also use the technology's features [55, 69] to present data flows through interactive 3D visualizations and sound cues, which have the potential to make privacy information more engaging, intuitive, and usable.

5.3 Limitations

As an early exploration of deceptive design in VR, our lead researcher's expertise was important in identifying these patterns, especially since non-expert users often struggle to recognize them [26]. However, further research is needed to assess the impact and harm of these patterns across diverse user groups. Our autoethnographic evaluation was guided by an evolving codebook [60] and supplemented by insights from broader literature (see Section 2.1). While this codebook incorporated established patterns from foundational deceptive design research [8, 11, 48, 50, 84] and privacy regulatory works [21, 35, 96], it does not capture previously unrecognized deceptive design patterns in VR. To address this, the lead researchers' expertise in user-centric privacy research guided the documentation of privacy-related expectations in diary entries and informed the exploration of patterns beyond those identified in the literature. However, blind spots may still persist [26, 53], and we welcome future research to confirm and expand on our findings.

Our analysis focused on data practices and privacy issues observable in VR design mechanics and privacy policies but left gaps for practices not disclosed in these contexts. While we aimed to identify elements in the information flows, many privacy policy statements were vague or overly broad, which resulted in some barriers in granular classifications (see Figure 3). Previous studies have also found discrepancies between actual VR device data transmissions and what privacy policies claim [28]. We encourage future research to extend our work by conducting network traffic analyses to determine if privacy policies align with actual data transmissions.

Due to ethical concerns about including other users without consent (see Section 3.2.1), our research focused on deceptive patterns that invade user privacy in single-user VR games and apps but left multi-user scenarios unexplored. This limitation constrains our understanding of how privacy risks emerge in user-to-user interactions, where social pressure and active data sharing may amplify deceptive practices. Future research could examine how deceptive design exploits privacy in multi-user environments, including (non)collocated interactions and bystander presence, as hypothesized in Krauss et al. [69]. We also noted non-privacy-related deceptive tactics, such as parasocial pressure and limited-time offers in *Beat Saber* that encourage impulsive purchases. Although outside our scope, these observations highlight the need for further research on deceptive design in VR that causes financial, temporal, or psychological harm.

To deepen our analysis of each VR game and app, we sacrificed the breadth of our study and analyzed fewer total VR games and apps than prior work (e.g., [26, 53]). Although we included at least one game or application from each genre, our limited scope prevents us from assessing the prevalence of deceptive design patterns in VR. We also acknowledge that our analysis was conducted exclusively on a Meta VR headset, which centers our findings around this platform and may not fully capture the deceptive design patterns and information flows present in other VR ecosystems. We encourage future research to explore and compare privacy mechanisms across

different VR platforms to obtain a broader perspective and a more comprehensive understanding of the manifestation of deceptive design and information flows.

Lastly, our data was collected from February to early August 2024. We acknowledge that these games and apps can evolve over time. For instance, by October 2024, we observed improvements in permission request notifications in *VRChat* and *The Room VR*, with added explanations of data usage. We also observed that VR privacy mechanisms were primarily implemented using 2D interfaces, which likely reflects a broader trend of limited integration of VR-specific features in current VR privacy mechanisms (as we discussed in Section 5.2.5). We encourage future research to explore how VR privacy mechanisms evolve with greater integration of VR-specific features over time and how deceptive designs emerge.

6 Conclusion

In conclusion, our research sheds light on the presence of deceptive design patterns in VR games and applications that hinder users' understanding of VR data practices and impair their ability to make informed privacy decisions. Through a two-phased methodology, we found that while some VR deceptive tactics are migrated from 2D web and mobile environments, and VR's unique features, such as realistic simulation, amplify their impacts on users. We also found that convoluted privacy policies and the absence of explicit consent interactions in VR further diminish users' awareness of the data transmission occurring in VR environments. On the other hand, we also clustered privacy-enhancing design strategies implemented in VR applications that can offer more ethical solutions for VR researchers, designers, and policymakers to create privacy-respecting immersive experiences and establish more transparent privacy policies. As VR continues to evolve, we argue that proactively implementing "bright patterns" that prioritize user privacy is essential for creating a safer and more privacy-friendly VR environment.

Acknowledgments

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC, the University of Waterloo, nor the UWaterloo Games Institute.

L. Zhang-Kennedy also acknowledge support from the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant (#RGPIN-2022-03353) and L. Nacke also acknowledge support from the Social Sciences and Humanities Research Council (SSHRC) INSIGHT Grant (#435-2022-0476), Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant (#RGPIN-2023-03705), and Canada Foundation for Innovation (CFI) John R. Evans Leaders Fund (#41844).

Thank you to the editors for their effort in organizing the peer-review process, and thank you to the reviewers for their insightful feedback that helped us to improve the quality of this manuscript. We also thank post-doctoral researcher Reza Hadi Mogavi and Eugene Kukshinov for their valuable feedback on the manuscript prior to our submission. Screenshots in this manuscript were from the selected games and applications and fall under fair use.

References

[1] Secretary of State of California. 2022. The California Age-Appropriate Design Code Act. https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false. Last accessed on Feb 22, 2025.

[2] Melvin Abraham, Pejman Saeghe, Mark Mcgill, and Mohamed Khamis. 2022. Implications of XR on Privacy, Security and Behaviour: Insights from Experts. In *Nordic Human-Computer Interaction Conference* (Aarhus, Denmark) *(NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 30, 12 pages. doi:10.1145/3546155.3546691

[3] Tony E Adams, Stacy Holman Jones, and Carolyn Ellis. 2016. *Handbook of autoethnography*. Routledge, London, UK.

[4] Idris Adjerid, Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2013. Sleights of privacy: framing, disclosures, and the limits of transparency. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, United Kingdom) *(SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 9, 11 pages. doi:10.1145/2501604.2501613

[5] Carlos Bermejo Fernandez, Lik Hang Lee, Petteri Nurmi, and Pan Hui. 2021. PARA: Privacy Management and Control in Emerging IoT Ecosystems using Augmented Reality. In *Proceedings of the 2021 International Conference on Multimodal Interaction* (Montréal, QC, Canada) *(ICMI '21)*. Association for Computing Machinery, New York, NY, USA, 478–486. doi:10.1145/3462244.3479885

[6] Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig, and Gabriele Lenzini. 2021. "I Am Definitely Manipulated, Even When I Am Aware of It. It's Ridiculous!" - Dark Patterns from the End-User Perspective. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference* (Virtual Event, USA) *(DIS '21)*. Association for Computing Machinery, New York, NY, USA, 763–776. doi:10.1145/3461778.3462086

[7] Elise Bonnail, Wen-Jie Tseng, Mark Mcgill, Eric Lecolinet, Samuel Huron, and Jan Gugenheimer. 2023. Memory Manipulations in Extended Reality. 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 875, 20 pages. doi:10.1145/3544548.3580988

[8] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proc. Priv. Enhancing Technol.* 2016, 4 (2016), 237–254.

[9] Amel Bourdoucen, Leysan Nurgalieva, and Janne Lindqvist. 2023. Privacy Is the Price: Player Views and Technical Evaluation of Data Practices in Online Games. *Proc. ACM Hum.-Comput. Interact.* 7, CHI PLAY, Article 418 (oct 2023), 43 pages. doi:10.1145/3611064

[10] Karoline Brehm and Yan Shvartzshnaider. 2024. Understanding Privacy in Virtual Reality Classrooms: A Contextual Integrity Perspective. *IEEE Security & Privacy* 22, 1 (2024), 53–62. doi:10.1109/MSEC.2023.3336802

[11] Harry Brignull. 2010. Deceptive patterns - user interfaces crafted to trick you. https://www.deceptive.design/. Last accessed on July 24, 2023.

[12] Harry Brignull. 2023. *Deceptive patterns – exposing the tricks that tech companies use to control you.* Testimonium Ltd, UK.

[13] Lauren Buck and Rachel McDonnell. 2022. Security and Privacy in the Metaverse: The Threat of the Digital Human. In *Proceedings of the 1st Workshop on Novel Challenges of Safety, Security andPrivacy in Extended Reality*. Association for Computing Machinery, New York, NY, USA, 4 pages.

[14] Duc Bui, Yuan Yao, Kang G. Shin, Jong-Min Choi, and Junbum Shin. 2021. Consistency Analysis of Data-Usage Purposes in Mobile Apps. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (Virtual Event, Republic of Korea) *(CCS '21)*. Association for Computing Machinery, New York, NY, USA, 2824–2843. doi:10.1145/3460120.3484536

[15] Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council. 2024. Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2 (2022). https://ethics.gc.ca/eng/policy-politique_tcps2-eptc2_2022.html. Last accessed on April 24, 2024.

[16] Alessandro Canossa and Anders Drachen. 2009. Patterns of play: Play-personas in user-centred game development. In *Proceedings of DiGRA 2009 Conference: Breaking New Ground: Innovation in Games, Play, Practice and Theory*. DiGRA, Finland, 1–10.

[17] Kuan-Wen Chen, Yung-Ju Chang, and Liwei Chan. 2022. Predicting Opportune Moments to Deliver Notifications in Virtual Reality. 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 186, 18 pages. doi:10.1145/3491102.3517529

[18] Victoria Clarke and Virginia Braun. 2021. *Thematic analysis: a practical guide.* SAGE Publications Ltd, California, United States.

[19] Federal Trade Commission. 2025. Genshin Impact Game Developer Will be Banned from Selling Loot-boxes to Teens Under 16 without Parental Consent, Pay a $20 Million Fine to Settle FTC Charges. https://www.ftc.gov/news-events/news/press-releases/2025/01/genshin-impact-game-developer-will-be-banned-selling-lootboxes-teens-under-16-without-parental. Last accessed on Feb 22, 2025.

[20] Commission nationale de l'informatique et des libertés. 2021. *Deliberation of the Restricted Committee No. SAN-2021-023 of 31 December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED.* Technical Report. Commission nationale de l'informatique et des libertés. 1–30 pages. https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-023_of_31_december_2021_concerning_google_llc_and_google_ireland_limited.pdf Last accessed on August 14, 2024.

[21] Competition and Markets Authority (CMA). 2022. Online choice architecture - how do we end up making decisions we don't want to make? https://competitionandmarkets.blog.gov.uk/2022/04/07/online-choice-architecture-how-do-we-end-up-making-decisions-we-dont-want/. Last accessed on August 14, 2024.

[22] James J Cummings and Alexis Shore. 2022. All too real: A typology of user vulnerabilities in extended reality. In *Proceedings of the 1st Workshop on Novel Challenges of Safety, Security and Privacy in Extended Reality*, Vol. 29. ACM, New York, USA, 3 pages.

[23] Archi Dasgupta, Mohamed Handosa, Mark Manuel, and Denis Gračanin. 2019. A User-Centric Design Framework for Smart Built Environments: A Mixed Reality Perspective. In *Distributed, Ambient and Pervasive Interactions: 7th International Conference, DAPI 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings* (Orlando, FL, USA). Springer-Verlag, Berlin, Heidelberg, 124–143. doi:10.1007/978-3-030-21935-2_11

[24] Jacob Davey. 2021. *Games Who Hate: An Introduction to ISD's Gaming and Extremism Series.* Technical Report. Institute for Strategic Dialogue, Paris.

[25] Sebastian Deterding, Dan Dixon, Rilla Khaled, and Lennart Nacke. 2011. From game design elements to gamefulness: defining "gamification". In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments* (Tampere, Finland) *(MindTrek '11)*. Association for Computing Machinery, New York, NY, USA, 9–15. doi:10.1145/2181037.2181040

[26] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 2020. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. 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. doi:10.1145/3313831.3376600

[27] Anders Drachen, Christian Thurau, Rafet Sifa, and Christian Bauckhage. 2014. A comparison of methods for player clustering via behavioral telemetry. *arXiv preprint arXiv:1407.3950* 0, 0 (2014), 1–8.

[28] Ben Egliston and Marcus Carter. 2023. Examining visions of surveillance in Oculus' data and privacy policies, 2014–2020. *Media International Australia* 188, 1 (2023), 52–66. doi:10.1177/1329878X211041670

[29] M.S. El-Nasr, A. Drachen, and A. Canossa. 2013. *Game Analytics: Maximizing the Value of Player Data.* Springer London, London. https://books.google.ca/books?id=-guHadEPrFcC

[30] Somaya Eltanbouly, Osama Halabi, and Junaid Qadir. 2024. Avatar Privacy Challenges in the Metaverse: A Comprehensive Review and Future Directions. *International Journal of Human–Computer Interaction* 0, 0 (2024), 1–18.

[31] European Parliament, Council of the European Union. 2022. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32022R2065. Last accessed on December 7, 2023..

[32] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. 2017. Large-scale readability analysis of privacy policies. In *Proceedings of the International Conference on Web Intelligence* (Leipzig, Germany) *(WI '17)*. Association for Computing Machinery, New York, NY, USA, 18–25. doi:10.1145/3106426.3106427

[33] Matthias Fassl and Katharina Krombholz. 2023. Why I Can't Authenticate — Understanding the Low Adoption of Authentication Ceremonies with Autoethnography. 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 72, 15 pages. doi:10.1145/3544548.3581508

[34] Federal Trade Commission (FTC). 2019. PrivacyCon 2019. https://www.ftc.gov/news-events/events/2019/06/privacycon-2019 Accessed: 2024-07-24.

[35] Federal Trade Commission (FTC). 2022. *Bringing Dark Patterns to Light.* Technical Report. Federal Trade Commission (FTC) Bureau of Consumer Protection.

[36] Federal Trade Commission (FTC). 2022. Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges. https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations. Last accessed on Jan 6, 2023..

[37] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: user attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 3, 14 pages. doi:10.1145/2335356.2335360

[38] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. 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 64, 16 pages. doi:10.1145/3411764.3445148

[39] Dan Fitton and Janet C. Read. 2019. Creating a Framework to Support the Critical Consideration of Dark Design Aspects in Free-to-Play Apps. In *Proceedings of the 18th ACM International Conference on Interaction Design and Children* (Boise, ID, USA) *(IDC '19)*. Association for Computing Machinery, New York, NY, USA, 407–418. doi:10.1145/3311927.3323136

[40] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' Expectations About and Use of Smartphone Privacy and Security Settings. 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 407, 24 pages. doi:10.1145/3491102.3517504

[41] Julian Frommel and Regan L Mandryk. 2022. Daily Quests or Daily Pests? The Benefits and Pitfalls of Engagement Rewards in Games. *Proceedings of the ACM on Human-Computer Interaction* 6, CHI PLAY (2022), 1–23.

[42] Julian Frommel, Cody Phillips, and Regan L. Mandryk. 2021. Gathering Self-Report Data in Games Through NPC Dialogues: Effects on Data Quality, Data Quantity, Player Experience, and Information Intimacy. 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 118, 12 pages. doi:10.1145/3411764.3445411

[43] Andrea Gallardo, Chris Choy, Jaideep Juneja, Efe Bozkir, Camille Cobb, Lujo Bauer, and Lorrie Cranor. 2023. Speculative Privacy Concerns About AR Glasses Data Collection. *Proceedings on Privacy Enhancing Technologies* 4 (2023), 416–435.

[44] Ceenu George, Manuel Demmler, and Heinrich Hussmann. 2018. Intelligent Interruptions for IVR: Investigating the Interplay between Presence, Workload and Attention. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI EA '18)*. Association for Computing Machinery, New York, NY, USA, 1–6. doi:10.1145/3170427.3188686

[45] Sarthak Ghosh, Lauren Winston, Nishant Panchal, Philippe Kimura-Thollander, Jeff Hotnog, Douglas Cheong, Gabriel Reyes, and Gregory D Abowd. 2018. Notifivr: Exploring interruptions and notifications in virtual reality. *IEEE transactions on visualization and computer graphics* 24, 4 (2018), 1447–1456.

[46] Global Privacy Enforcement Network (GPEN). 2024. *GPEN Sweep 2024:"Deceptive Design Patterns"*. Technical Report. Global Privacy Enforcement Network. Last accessed on Aug 25, 2024.

[47] Colin M. Gray, Jingle Chen, Shruthi Sai Chivukula, and Liyang Qu. 2021. End User Accounts of Dark Patterns as Felt Manipulation. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 372 (oct 2021), 25 pages. doi:10.1145/3479516

[48] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. 2018. The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. ACM, New York, USA, 1–14.

[49] Colin M Gray, Lorena Sanchez Chamorro, Ike Obi, and Ja-Nae Duane. 2023. Mapping the Landscape of Dark Patterns Scholarship: A Systematic Literature Review. In *Companion Publication of the 2023 ACM Designing Interactive Systems Conference*. ACM, New York, USA, 188–193.

[50] Colin M. Gray, Cristiana Teixeira Santos, Nataliia Bielova, and Thomas Mildner. 2024. An Ontology of Dark Patterns Knowledge: Foundations, Definitions, and a Pathway for Shared Knowledge-Building. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 289, 22 pages. doi:10.1145/3613904.3642436

[51] Paul Graßl, Hanna Schraffenberger, Frederik Zuiderveen Borgesius, and Moniek Buijzen. 2021. Dark and Bright Patterns in Cookie Consent Requests. *Journal of Digital Social Research* 3, 1 (Feb. 2021), 1–38. doi:10.33621/jdsr.v3i1.54

[52] Saul Greenberg, Sebastian Boring, Jo Vermeulen, and Jakub Dostal. 2014. Dark Patterns in Proxemic Interactions: A Critical Perspective. In *Proceedings of the 2014 Conference on Designing Interactive Systems* (Vancouver, BC, Canada) *(DIS '14)*. Association for Computing Machinery, New York, NY, USA, 523–532. doi:10.1145/2598510.2598541

[53] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. 2021. A Comparative Study of Dark Patterns Across Web and Mobile Modalities. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 377 (oct 2021), 29 pages. doi:10.1145/3479521

[54] Johanna Gunawan, Cristiana Santos, and Irene Kamara. 2022. Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions. In *Proceedings of the 2022 Symposium on Computer Science and Law* (Washington DC, USA) *(CSLAW '22)*. Association for Computing Machinery, New York, NY, USA, 181–194. doi:10.1145/3511265.3550448

[55] Hilda Hadan, Lydia Choong, Leah Zhang-Kennedy, and Lennart E. Nacke. 2024. Deceived by Immersion: A Systematic Analysis of Deceptive Design in Extended Reality. *ACM Comput. Surv.* 56, 10, Article 250 (may 2024), 25 pages. doi:10.1145/3659945

[56] Hilda Hadan, Nicolas Serrano, and L Jean Camp. 2021. A holistic analysis of web-based public key infrastructure failures: comparing experts' perceptions and real-world incidents. *Journal of Cybersecurity* 7, 1 (12 2021), tyab025. arXiv:https://academic.oup.com/cybersecurity/article-pdf/7/1/tyab025/50476414/tyab025.pdf doi:10.1093/cybsec/tyab025

[57] Hilda Hadan, Sabrina A. Sgandurra, Leah Zhang-Kennedy, and Lennart E. Nacke. 2024. From Motivating to Manipulative: The Use of Deceptive Design in a Game's Free-to-Play Transition. *Proc. ACM Hum.-Comput. Interact.* 8, CHI PLAY, Article 309 (oct 2024), 31 pages. doi:10.1145/3677074

[58] Hilda Hadan, Derrick M. Wang, Reza Hadi Mogavi, Joseph Tu, Leah Zhang-Kennedy, and Lennart E. Nacke. 2024. The Great AI Witch Hunt: Reviewers' Perception and (Mis)Conception of Generative AI in ResearchWriting. *Computers in Human Behavior: Artificial Humans* 0, 0 (2024), 1–33. doi:10.1016/j.chbah.2024.100095

[59] Hilda Hadan, Derrick M. Wang, Lennart E. Nacke, and Leah Zhang-Kennedy. 2024. Privacy in Immersive Extended Reality: Exploring User Perceptions, Concerns, and Coping Strategies. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 784, 24 pages. doi:10.1145/3613904.3642104

[60] Hilda Hadan, Leah Zhang-Kennedy, and Lennart E. Nacke. 2024. Computer-based Deceptive Game Design in Commercial Virtual Reality Games: A Preliminary Investigation. In *Companion Proceedings of the 2024 Annual Symposium on Computer-Human Interaction in Play* (Tampere, Finland) *(CHI PLAY Companion '24)*. Association for Computing Machinery, New York, NY, USA, 109–123. doi:10.1145/3665463.3678820

[61] Jaap-Henk Hoepman. 2014. Privacy Design Strategies. In *ICT Systems Security and Privacy Protection*, Nora Cuppens-Boulahia, Frédéric Cuppens, Sushil Jajodia, Anas Abou El Kalam, and Thierry Sans (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 446–459.

[62] Information Commissioner's Office. 2020. Age appropriate design: a code of practice for online services. https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf. Last accessed on Feb 22, 2025.

[63] Carlos Jensen and Colin Potts. 2004. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vienna, Austria) *(CHI '04)*. Association for Computing Machinery, New York, NY, USA, 471–478. doi:10.1145/985692.985752

[64] Skyler Johnson, Katherine Ferro, L. Jean Camp, and Hilda Hadan. 2021. Human and Organizational Factors in Public Key Certificate Authority Failures. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (Virtual Event, Republic of Korea) *(CCS '21)*. Association for Computing Machinery, New York, NY, USA, 2414–2416. doi:10.1145/3460120.3485360

[65] Annika Kaltenhauser, Evropi Stefanidi, and Johannes Schöning. 2024. Playing with Perspectives and Unveiling the Autoethnographic Kaleidoscope in HCI – A Literature Review of Autoethnographies. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 819, 20 pages. doi:10.1145/3613904.3642355

[66] Faltin Karlsen. 2019. Exploited or Engaged? Dark Game Design Patterns in Clicker Heroes, FarmVille 2, and World of Warcraft. In *Transgression in Games and Play*. The MIT Press, MA, USA. arXiv:https://direct.mit.edu/book/chapter-pdf/2104393/9780262348706_ceb.pdf doi:10.7551/mitpress/11550.003.0019

[67] Daniel L King, Paul H Delfabbro, Sally M Gainsbury, Michael Dreier, Nancy Greer, and Joël Billieux. 2019. Unfair play? Video games as exploitative monetized services: An examination of game patents from a consumer protection perspective. *Computers in Human Behavior* 101 (2019), 131–143.

[68] John King, Dan Fitton, and Brendan Cassidy. 2023. Investigating Players' Perceptions of Deceptive Design Practices within a 3D Gameplay Context. *Proc. ACM Hum.-Comput. Interact.* 7, CHI PLAY, Article 407 (oct 2023), 17 pages. doi:10.1145/3611053

[69] Veronika Krauss, Pejman Saeghe, Alexander Boden, Mohamed Khamis, Mark McGill, Jan Gugenheimer, and Michael Nebeling. 2024. What Makes XR Dark? Examining Emerging Dark Patterns in Augmented and Virtual Reality through Expert Co-Design. *ACM Trans. Comput.-Hum. Interact.* 0, 0 (apr 2024), 37 pages. doi:10.1145/3660340 Just Accepted.

[70] Veronika Krauss, Pejman Saeghe, Alexander Boden, Mohamed Khamis, Mark McGill, Jan Gugenheimer, and Michael Nebeling. 2024. What Makes XR Dark? Examining Emerging Dark Patterns in Augmented and Virtual Reality through Expert Co-Design. *ACM Trans. Comput.-Hum. Interact.* 0, 0 (apr 2024), 37 pages. doi:10.1145/3660340 Just Accepted.

[71] Jacob Leon Kröger, Philip Raschke, Jessica Percy Campbell, and Stefan Ullrich. 2023. Surveilling the gamers: Privacy impacts of the video game industry. *Entertainment Computing* 44 (2023), 100537.

[72] Samuli Laato, Daniel Fernández Galeote, Ferran Altarriba Bertran, and Juho Hamari. 2022. Balancing the augmented experience: design tensions in the location-based game Pikmin Bloom. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*. Association for Computing Machinery, New York, NY, USA, 1–7.

[73] Chris Lewis. 2014. *Irresistible Apps: Motivational design patterns for apps, games, and web-based communities*. Springer, Berlin, Germany.

[74] Peter Likarish, Oliver Brdiczka, Nicholas Yee, Nicholas Ducheneaut, and Les Nelson. 2011. Demographic Profiling from MMOG Gameplay. In *11th Privacy Enhancing Technologies Symposium*. Citeseer, PETS, Waterloo, Canada, 1–19.

[75] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. 2018. The privacy policy landscape after the GDPR. *arXiv preprint arXiv:1809.08396* 0, 0 (2018), 1–18.

[76] Andrés Lucero, Jussi Holopainen, Elina Ollila, Riku Suomela, and Evangelos Karapanos. 2013. The playful experiences (PLEX) framework as a guide for expert evaluation. In *Proceedings of the 6th International Conference on Designing Pleasurable Products and Interfaces* (Newcastle upon Tyne, United Kingdom) *(DPPI '13)*. Association for Computing

Machinery, New York, NY, USA, 221–230. doi:10.1145/2513506.2513530
[77] Jamie Luguri and Lior Jacob Strahilevitz. 2021. Shining a light on dark patterns. *Journal of Legal Analysis* 13, 1 (2021), 43–109.
[78] Aditi M. Bhoot, Mayuri A. Shinde, and Wricha P. Mishra. 2021. Towards the Identification of Dark Patterns: An Analysis Based on End-User Reactions. In *Proceedings of the 11th Indian Conference on Human-Computer Interaction* (Online, India) *(IndiaHCI '20)*. Association for Computing Machinery, New York, NY, USA, 24–33. doi:10.1145/3429290.3429293
[79] Maximilian Maier. 2019. Dark patterns–An end user perspective.
[80] Divine Maloney, Samaneh Zamanifard, and Guo Freeman. 2020. Anonymity vs. Familiarity: Self-Disclosure and Privacy in Social Virtual Reality. In *Proceedings of the 26th ACM Symposium on Virtual Reality Software and Technology* (Virtual Event, Canada) *(VRST '20)*. Association for Computing Machinery, New York, NY, USA, Article 25, 9 pages. doi:10.1145/3385956.3418967
[81] Dragana Martinovic, Victor Ralevich, Joshua McDougall, and Michael Perklin. 2014. "You are what you play": Breaching privacy and identifying users in online gaming. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust*. IEEE, Toronto, ON, Canada, 31–39. doi:10.1109/PST.2014.6890921
[82] Arunesh Mathur, Gunes Acar, Michael J Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–32.
[83] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 2021. What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. 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 360, 18 pages. doi:10.1145/3411764.3445610
[84] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 2021. What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods. In *Proceedings of the 2021 CHI conference on human factors in computing systems*. ACM, New York, USA, 1–18.
[85] Tim May, Beth Perry, et al. 2014. Reflexivity and the practice of qualitative research. *The SAGE handbook of qualitative data analysis* 109 (2014), 109–122.
[86] Abraham Hani Mhaidli and Florian Schaub. 2021. Identifying manipulative advertising techniques in xr through scenario construction. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–18.
[87] Thomas Mildner, Merle Freye, Gian-Luca Savino, Philip R. Doyle, Benjamin R. Cowan, and Rainer Malaka. 2023. Defending Against the Dark Arts: Recognising Dark Patterns in Social Media. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference* (Pittsburgh, PA, USA) *(DIS '23)*. Association for Computing Machinery, New York, NY, USA, 2362–2374. doi:10.1145/3563657.3595964
[88] Thomas Mildner, Gian-Luca Savino, Philip R. Doyle, Benjamin R. Cowan, and Rainer Malaka. 2023. About Engaging and Governing Strategies: A Thematic Analysis of Dark Patterns in Social Networking Services. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (<conf-loc>, <city>Hamburg</city>, <country>Germany</country>, </conf-loc>) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 192, 15 pages. doi:10.1145/3544548.3580695
[89] Mark Roman Miller, Fernanda Herrera, Hanseul Jun, James A Landay, and Jeremy N Bailenson. 2020. Personal identifiability of user tracking data during observation of 360-degree VR video. *Scientific Reports* 10, 1 (2020), 1–10.
[90] Nurul Momen, Sven Bock, and Lothar Fritsch. 2020. Accept - Maybe - Decline: Introducing Partial Consent for the Permission-based Access Control Model of Android. In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies* (Barcelona, Spain) *(SACMAT '20)*. Association for Computing Machinery, New York, NY, USA, 71–80. doi:10.1145/3381991.3395603
[91] Alberto Monge Roffarello, Kai Lukoff, and Luigi De Russis. 2023. Defining and Identifying Attention Capture Deceptive Designs in Digital Interfaces. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (<conf-loc>, <city>Hamburg</city>, <country>Germany</country>, </conf-loc>) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 194, 19 pages. doi:10.1145/3544548.3580729
[92] Vivek Nair, Gonzalo Munilla Garrido, Dawn Song, and James O'Brien. 2023. Exploring the privacy risks of adversarial VR game design. *Proceedings on Privacy Enhancing Technologies* 2023, 4 (2023), 19.
[93] Carman Neustaedter and Elena Fedorovskaya. 2009. Presenting identity in a virtual world through avatar appearances. In *Proceedings of Graphics Interface 2009* (Kelowna, British Columbia, Canada) *(GI '09)*. Canadian Information Processing Society, CAN, 183–190.
[94] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.
[95] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY,

USA, 1–13. doi:10.1145/3313831.3376321

[96] OECD. 2022. *Dark commercial patterns.* Technical Report 336. OECD Publishing, Paris. doi:10.1787/44f5e846-en

[97] California Secretary of State 2020. 2020. California Privacy Rights Act of 2020 (CPRA). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. CPRA also known as Proposition 24, is a California ballot proposition that was approved by a majority of voters after appearing on the ballot for the general election on November 3, 2020. The CPRA amends the CCPA and includes additional privacy protections for consumers. The provisions that are not yet operative are listed after the CCPA provision in effect. Last accessed on November 28, 2022.

[98] Office of the Arizona Attorney General. 2022. Attorney General Mark Brnovich Achieves Historic $85 Million Settlement with Google. https://www.azag.gov/press-release/attorney-general-mark-brnovich-achieves-historic-85-million-settlement-google Accessed: [Insert access date here].

[99] Office of the Privacy Commissioner of Canada. 2018. Guidelines for Obtaining Meaningful Consent. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/. Last accessed on July 28, 2024.

[100] Office of the Privacy Commissioner of Canada. 2024. Gaming and personal information: playing with privacy. https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/digital-devices/gd_gc_201905/. Last accessed on July 28, 2024.

[101] Office of the Privacy Commissioner of Canada. 2024. *OPC Sweep Report 2024: Deceptive Design Patterns.* Technical Report. Office of the Privacy Commissioner of Canada, Ottawa, Canada. https://www.priv.gc.ca

[102] Elena Petrovskaya. 2024. Ask the players! Player-centric principles as guidelines for ethical microtransactions. *ACM Games* 2, 2, Article 18 (aug 2024), 3 pages. doi:10.1145/3675802

[103] Elena Petrovskaya and David Zendle. 2021. Predatory monetisation? A categorisation of unfair, misleading and aggressive monetisation techniques in digital games from the player perspective. *Journal of Business Ethics* 181 (2021), 1065—-1081.

[104] Ken Pfeuffer, Matthias J Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural biometrics in vr: Identifying people from body motion and relations in virtual reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–12.

[105] Kevin Proudfoot. 2023. Inductive/deductive hybrid thematic analysis in mixed methods research. *Journal of mixed methods research* 17, 3 (2023), 308–326.

[106] Marvin Ramokapane, Anthony C Mazeli, and Awais Rashid. 2019. Skip, Skip, Skip, Accept!!!: A Study on the Usability of Smartphone Manufacturer Provided Default Features and User Privacy. *Proceedings on Privacy Enhancing Technologies* 2019, 2 (2019), 209–227. doi:10.2478/popets-2019-0027

[107] Amon Rapp. 2017. Designing interactive systems through a game lens: An ethnographic approach. *Computers in human behavior* 71 (2017), 455–468.

[108] Amon Rapp. 2017. From games to gamification: A classification of rewards in World of Warcraft for the design of gamified systems. *Simulation & Gaming* 48, 3 (2017), 381–401.

[109] Amon Rapp. 2018. *Autoethnography in Human-Computer Interaction: Theory and Practice.* Springer International Publishing, Cham, 25–42. doi:10.1007/978-3-319-73374-6_3

[110] Sampsa Rauti and Samuli Laato. 2020. Location-Based Games as Interfaces for Collecting User Data. In *Trends and Innovations in Information Systems and Technologies*, Álvaro Rocha, Hojjat Adeli, Luís Paulo Reis, Sandra Costanzo, Irena Orovic, and Fernando Moreira (Eds.). Springer International Publishing, Cham, 631–642.

[111] N Cameron Russell, Joel R Reidenberg, and Sumyung Moon. 2018. Privacy in gaming. *Fordham Intell. Prop. Media & Ent. LJ* 29 (2018), 61.

[112] Rufat Rzayev, Sven Mayer, Christian Krauter, and Niels Henze. 2019. Notification in VR: The Effect of Notification Placement, Task and Environment. In *Proceedings of the Annual Symposium on Computer-Human Interaction in Play* (Barcelona, Spain) *(CHI PLAY '19)*. Association for Computing Machinery, New York, NY, USA, 199–211. doi:10.1145/3311350.3347190

[113] Johnny Saldaña. 2021. *The coding manual for qualitative researchers.* sage, Thousand Oaks, CA, USA.

[114] Hauke Sandhaus. 2023. Promoting Bright Patterns. CHI '23 Workshop: Designing Technology and Policy Simultaneously. arXiv:2304.01157 [cs.HC]

[115] René Schäfer, Paul Miles Preuschoff, René Röpke, Sarah Sahabi, and Jan Borchers. 2024. Fighting Malicious Designs: Towards Visual Countermeasures Against Dark Patterns. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 296, 13 pages. doi:10.1145/3613904.3642661

[116] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A Design Space for Effective Privacy Notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa,

1–17. https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub
[117] Raphael Schlembach and Nicola Clewer. 2021. 'Forced empathy': Manipulation, trauma and affect in virtual reality film. *International Journal of Cultural Studies* 24, 5 (2021), 827–843.
[118] Magy Seif El-Nasr and Erica Kleinman. 2020. Data-Driven Game Development: Ethical Considerations. In *Proceedings of the 15th International Conference on the Foundations of Digital Games* (Bugibba, Malta) *(FDG '20)*. Association for Computing Machinery, New York, NY, USA, Article 64, 10 pages. doi:10.1145/3402942.3402964
[119] Yan Shvartzshnaider, Noah Apthorpe, Nick Feamster, and Helen Nissenbaum. 2019. Going against the (Appropriate) Flow: A Contextual Integrity Approach to Privacy Policy Analysis, In AAAI. *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing* 7, 1, 162–170. doi:10.1609/hcomp.v7i1.5266
[120] Herbert Alexander Simon. 1997. *Models of bounded rationality: Empirically grounded economic reason*. Vol. 3. MIT press, MA, USA.
[121] Than Htut Soe, Oda Elise Nordberg, Frode Guribye, and Marija Slavkovik. 2020. Circumvention by design - dark patterns in cookie consent for online news outlets. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (Tallinn, Estonia) *(NordiCHI '20)*. Association for Computing Machinery, New York, NY, USA, Article 19, 12 pages. doi:10.1145/3419249.3420132
[122] Maximilian Speicher, Brian D Hall, and Michael Nebeling. 2019. What is mixed reality?. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. Association for Computing Machinery, New York, NY, USA, 1–15.
[123] Pieter Spronck, Iris Balemans, and Giel van Lankveld. 2012. Player profiling with Fallout 3. In *Proceedings of the Eighth AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment (AIIDE'12)*. AAAI Press, Stanford, California, USA, 179–184.
[124] Zihao Su, Faysal Hossain Shezan, Yuan Tian, David Evans, and Seongkook Heo. 2022. Perception Hacking for 2D Cursorjacking in Virtual Reality. In *Proceedings of the 1st Workshop on Novel Challenges of Safety, Security and Privacy in Extended Reality*. Association for Computing Machinery, New York, NY, USA, 5 pages.
[125] Jon Swain. 2018. A hybrid approach to thematic analysis in qualitative research: Using a practical example. *Sage research methods* 0, 0 (2018), 1–28.
[126] Carl Symborski, Gary M. Jackson, Meg Barton, Geoffrey Cranmer, Byron Raines, and Mary Magee Quinn. 2014. The Use of Social Science Methods to Predict Player Characteristics from Avatar Observations. In *Predicting Real World Behaviors from Virtual World Data*, Muhammad Aurangzeb Ahmad, Cuihua Shen, Jaideep Srivastava, and Noshir Contractor (Eds.). Springer International Publishing, Cham, 19–37.
[127] Richard H Thaler and Cass R Sunstein. 2009. *Nudge: Improving decisions about health, wealth, and happiness*. Penguin, London, United Kingdom.
[128] The European Consumer Organisation. 2024. Monetising Play: Regulating in-game and in-app premium currencies. https://www.beuc.eu/position-papers/monetising-play-regulating-game-and-app-premium-currencies. Last Accesed on September 12, 2024.
[129] Rahmadi Trimananda, Hieu Le, Hao Cui, Janice Tran Ho, Anastasia Shuba, and Athina Markopoulou. 2022. OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 3789–3806. https://www.usenix.org/conference/usenixsecurity22/presentation/trimananda
[130] Hellen Truong and Axel Dalbard. 2022. Bright Patterns as an Ethical Approach to Counteract Dark Patterns: A Closer Investigation of The Ethics of Persuasive Design.
[131] Sarah Turner, Jason RC Nurse, and Shujun Li. 2022. "It was hard to find the words": Using an Autoethnographic Diary Study to Understand the Difficulties of Smart Home Cyber Security Practices. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*. ACM, New York, NY, USA, 1–8.
[132] United for Literacy. 2022. *Adult Literacy Skills for Success: 2022 National Report*. Technical Report. United for Literacy, Canada. https://unitedforliteracy.ca
[133] Ari Ezra Waldman. 2020. Cognitive biases, dark patterns, and the 'privacy paradox'. *Current opinion in psychology* 31 (2020), 105–109.
[134] Cheng Yao Wang, Sandhya Sriram, and Andrea Stevenson Won. 2021. Shared Realities: Avatar Identification and Privacy Concerns in Reconstructed Experiences. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 337 (oct 2021), 25 pages. doi:10.1145/3476078
[135] José P Zagal, Staffan Björk, and Chris Lewis. 2013. Dark patterns in the design of games. In *Foundations of Digital Games 2013*. ACM, Crete, Greece, 8 pages.
[136] André Zenner, Marco Speicher, Sören Klingner, Donald Degraen, Florian Daiber, and Antonio Krüger. 2018. Immersive Notification Framework: Adaptive & Plausible Notifications in Virtual Reality. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI EA '18)*. Association for Computing Machinery, New York, NY, USA, 1–6. doi:10.1145/3170427.3188505

[137] Leah Zhang-Kennedy, Maxwell Keleher, and Michaela Valiquette. 2024. Navigating the Gray: Design Practitioners' Perceptions Toward the Implementation of Privacy Dark Patterns. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1 (2024), 1–26.

[138] Sebastian Zimmeck, Peter Story, Daniel Smullen, Abhilasha Ravichander, Ziqi Wang, Joel Reidenberg, N Cameron Russell, and Norman Sadeh. 2019. Maps: Scaling privacy compliance analysis to a million apps. *Proceedings on Privacy Enhancing Technologies* 2019, 3 (2019), 21.

A Appendix — Disclosure Statement for Our Use of AI in Writing and Grammar Enhancements

In accordance with ACM Publications Policy[16] and literature suggestion [58], we acknowledge our use of the Grammarly and Typingmind (GPT-4o model) AI writing assistants. These tools were used to correct grammatical errors and, in a few cases, condense and improve sentence structure using the prompt: "make the following sentence [our human-written sentence] more concise and fix any grammar errors." Our decision to use AI was based on our hope to achieve a concise and succinct writing while preserving the "human-touch" in our research writing [58]. We did not use AI for data collection, analysis, or image generation. Analysis was manually conducted by our lead researcher and a graduate research assistant using non-AI-supported version of Dovetail. Figures in this manuscript were captured with the Meta Quest 3 VR headset's screenshot function and formatted using Canva's default templates. Our research team manually reviewed, verified, and copy-edited the full manuscript.

[16] Association for Computing Machinery. (July 6, 2023). ACM publications policy guidance for SIGCHI venues. Retrieved October 22, 2024, from https://medium.com/sigchi/acm-publications-policy-guidance-for-sigchi-venues-87332173aad1

B Appendix — Example Diary Entry

Table 5. Structural outline of a sample diary entry from a *VRChat* autoethnography exploration session on July 22, 2024. The diary was documented in Miro given its feasibility in linking videos, screenshots, and diary texts. From left to right: (1) detailed observations of privacy communication and interaction design mechanics that incorporated deceptive designs, and (2) reflections on experiences, reactions, thoughts, and emotional responses when the design mechanics were encountered. We focused on the design mechanisms that allow users to obtain privacy information, make privacy choices, and express privacy preference.

Date: July 22, 2024	
Estimated Time: ~1.5 hours including diary writing	
[Imported Video Recording Available for Re-watch]	
[*Diary:*]	**[Reflection Note:]**
Today, I had my first experience with VR Chat. The initial on-boarding process was straightforward, and I was placed in a beginner world. While I'm unsure if this was intentional or simply a result of joining at a less populated time, I appreciated the opportunity of no immediate social interaction. I was able to explore the environment, customize my avatar, and familiarize myself with the platform's features and adjust my privacy settings without the pressure of being observed by other users.	I was very satisfied that I was placed in a private world upon joining. As a newcomer to social VR experiences, this private world gave me a safe and controlled space to get familiarized with the platform's features and configure my virtual identity without worrying about unwanted judgment or exposure. It gave me a safe adoption of social VR experiences and a smooth transfer from private to public spaces. Had I been immediately placed in a public world, I may have accidentally revealed sensitive information or made mistakes that could have compromised my privacy.
[Screenshots go here]	**[Screenshots go here]**
One interesting aspect of VR Chat was the way it made me feel more immersed in the virtual world compared to traditional PC games. The ability to view my avatar from a first-person perspective and interact with the environment using my full body made it feel like a more personal and realistic experience. While my avatar was entirely fictional and doesn't mirror my actual physical appearance, I still found myself carefully selecting clothing and accessories for my avatar and be mindful of what I wear or say in a public space, as if curating a public image of myself.	Overall, I experienced a heightened sense of self-awareness and concern for personal boundary in VRChat. I also wondered, can people infer my interests or preferences based on my avatar's clothing choices? Can they guess my personality and gender from my name tag? The possibility of being deanonymized through these cues made me feel vulnerable but having access to a private beginner world really eased my concerns.

C Appendix — Example Screenshots Deceptive Design Patterns from VR Games and Playful Applications



Fig. 4. The privacy settings mechanism in *The Climb 2* exemplifies the **`Privacy Maze`** deceptive design pattern. The main settings screen provides six distinct buttons that each leads to a sub-menu, with privacy-related information hiding within the "options" sub-menu without obvious indicator of its availability. To find the privacy-related information, users must navigate to the "options" sub-menu (see left screenshot). Inside the "options" menu, users encounter two buttons on the right and various application settings in the center (see center screenshot). To access privacy information, users must navigate to the right side and select "privacy," where the privacy policy is located (see right screenshot). *Note. Our researcher's username is concealed in the screenshots for anonymity.*

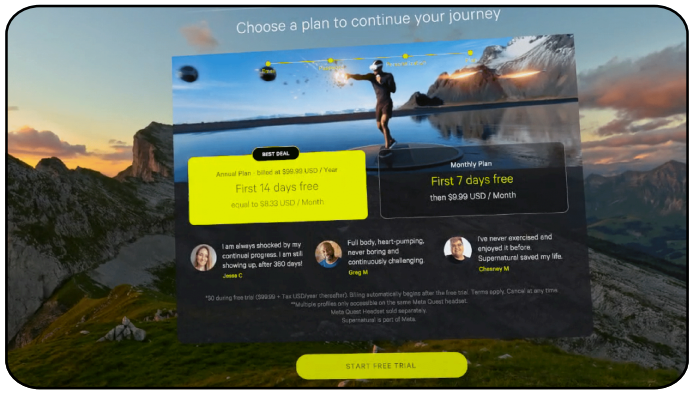


Fig. 5. The subscription mechanism in *Supernatural* exemplifies the **Endorsements and Testimonials** deceptive design pattern. The mechanism includes two different subscription plans alongside three testimonials that aim to persuade users to subscribe, which involves providing payment information, by highlighting highly positive experiences. However, the authenticity of these testimonials is questionable, as the professionally polished photos suggest they may have been provided by paid influencers rather than genuine users. This, combined with the realistic virtual environment that demonstrates vivid and lifelike landscapes, create a persuasive setting where users may be misled into believing the testimonials are genuine and be prompted to subscribe under the assumption that they will have similar positive experiences. In addition, the brightly colored and visually emphasized subscription plans and confirmation button also exemplifies **Visual Prominence** deceptive design. The use of bright green color scheme on an option that involves financial commitment exemplifies **Positive or Negative Framing** deceptive design, as it suggests emotional safety and subtly encourages users to accept privacy-invasive options without fully understanding their decisions.

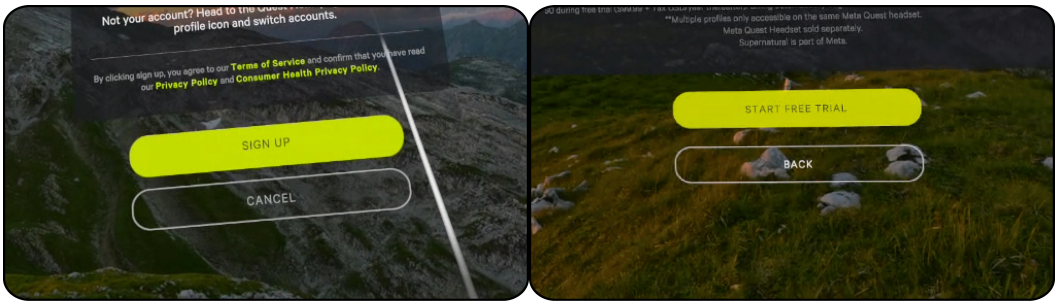


Fig. 6. The registration and subscription mechanisms in *Supernatural* (see left and right screenshots, respectively) exemplify the **False Hierarchy**, **Visual Prominence**, and **Positive or Negative Framing** deceptive design patterns. Options that involve acceptance are brightly colored, visually emphasized, and ranked above other available choices. The use of a bright green color scheme for options requiring financial commitment exemplifies Positive or Negative Framing, as it conveys a sense of emotional safety and subtly encourage users to opt for privacy-invasive choices.

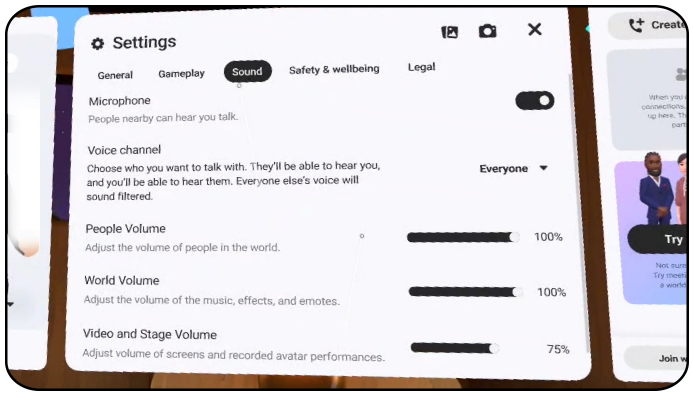


Fig. 7. The consent interaction mechanism in *Meta Horizon Worlds* exemplifies the **`Bad Defaults`** deceptive design pattern. Within the settings menu, several privacy-invasive options are pre-enabled by default. These include automatically activating the microphone ("people nearby can hear you talk"), auto-joining the "everyone" voice channel, and automatic leaderboard participation ("allow leaderboard to show your name and score in any world"). While these features are intended to foster social interaction, having them opted-in by default may leave users feeling exposed, especially for those who are more sensitive to personal privacy and boundaries. *Note: Our researcher's username is concealed in the screenshot for anonymity.*

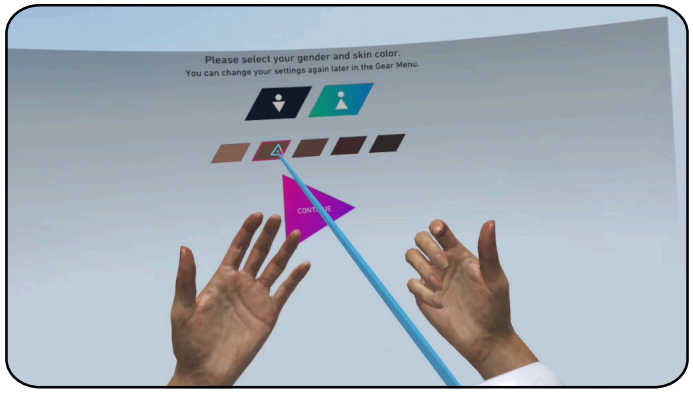


Fig. 8. The quality-of-life (QoL) feature that facilitates avatar customization in *The Climb 2* exemplifies the **`Trick Questions`** deceptive design pattern. In this interface, users are asked to choose their gender and skin color, phrased as "select your race and gender". Although this question was intended for avatar customization, the wording exemplifies the misleading nature of Trick Questions. As users see the realistic rendering of their "hands" in the avatar creation process from a first-person perspective, they may feel more compelled to create avatars that resemble their real-life appearance. As a result, the data about users' avatar becomes a valuable source for inferring their personal characteristics.

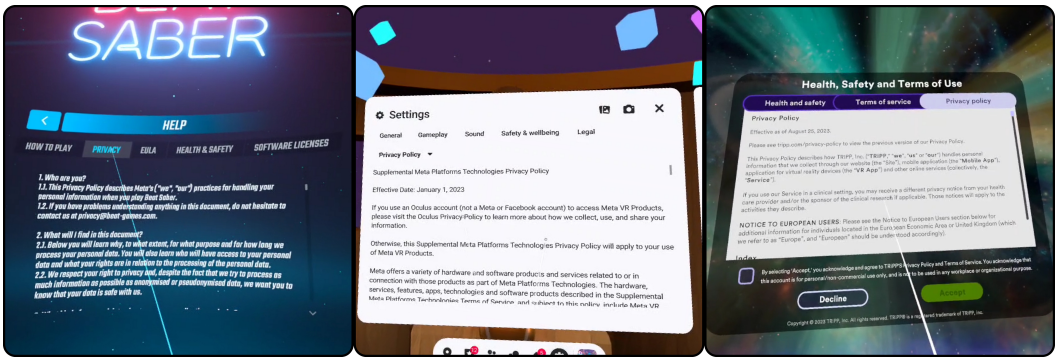


Fig. 9. The in-game and in-app privacy policies in *Beat Saber* (see left screenshot), *Meta Horizon Worlds* (see center screenshot), and *TRIPP* (see right screenshot) exemplify **`Complex & Lengthy Language`** deceptive design pattern. Although they are aimed to inform users about data practices upon first entry, these documents are often lengthy and difficult to read. This complexity may discourage users from fully reading the terms and hinders their comprehension of potential privacy risks. Our findings from privacy policy analysis further support this conclusion (see Section 4.3.3 and Appendix E).

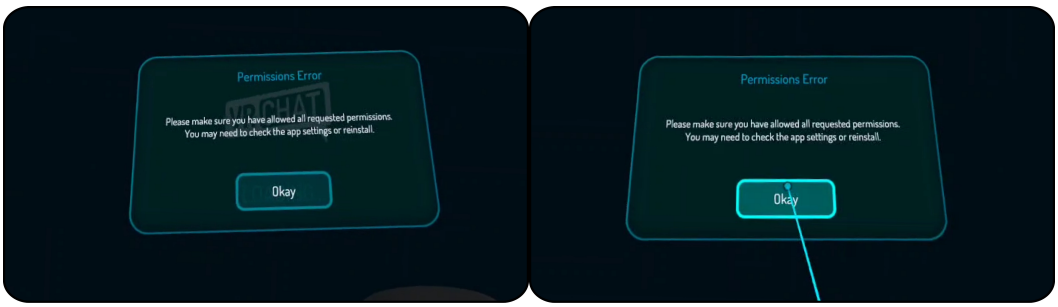


Fig. 10. The notification mechanism in *VRChat* exemplifies the **`Nagging`** deceptive design pattern. When users choose "Not allow" during the application's request for access to their photos, media, and files upon their entry, they are repeatedly interrupted by a "permissions error" message each time they transfer to a different virtual interaction space (i.e., "world"). Users must press "okay" each time, which can become irritating and may ultimately compel them to re-enter the application and grant the permission to stop the interruptions. Repeatedly prompting users for permissions related to photos, media, and files before those features are even used is excessive. The left screenshot captures the initial error message displayed after denying access, and the right screenshot shows the repeated message at a later time.

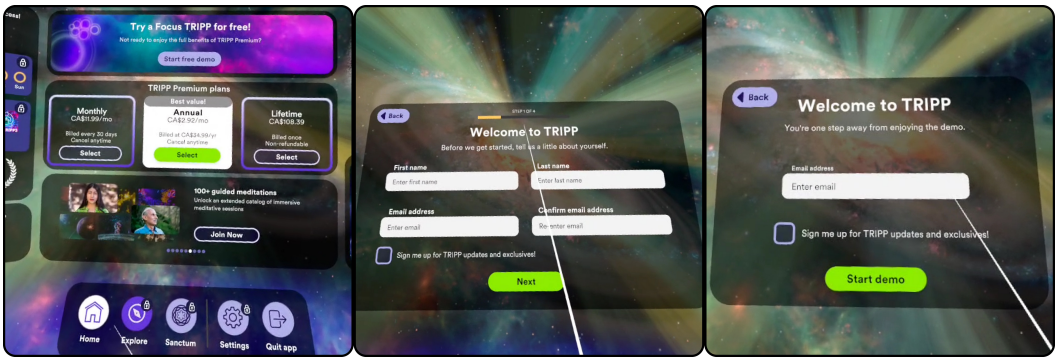


Fig. 11. The registration and subscription mechanism in *TRIPP* exemplifies the **Forced Registration** deceptive design pattern. No functions are usable or accessible without registration (see left screenshot). Users are required to provide their email address to even start a demo session (see center screenshot). Users also must register an account and pay a subscription fee with their name and credit card information to unlock all functions, including detailed privacy settings (see right screenshot). While these design mechanisms may support cross-device experiences, they are unnecessary for users intending to use the application solely on VR platforms. The forced disclosure of users' name and email address through the registration process also exemplifies **Privacy Zuckering**, as this information is not essential for the applications' functionality.



Fig. 12. The privacy settings mechanism in A Fisherman's Tale exemplifies the **Mandatory Acceptance** deceptive design pattern. The settings screen does not provide available settings for users to customize their privacy preferences at all. Therefore, users are forced to consent to all publisher-stated data practices without sufficient awareness, even if these practices are uncomfortable or irrelevant to the game's functions.

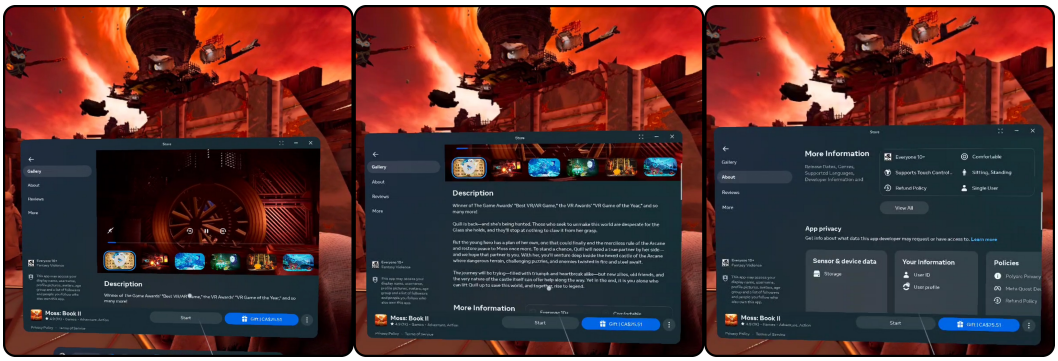


Fig. 13. The Meta Quest Store provides a link to the publisher's privacy policy, but it is placed at the very bottom of the page. The store page is primarily dominated by a large and attention-grabbing video preview (see left screenshot). Users are required to scroll down to locate the privacy policy hyperlink at the bottom of the page (see center and right screenshots). As a result, users may not scroll far enough to even notice its presence. This design of the Meta Quest store page can also be seen as an attention-capture tactic [91], as users' focus is naturally drawn to the visually striking VR game and application previews, and leave critical privacy information overlooked.

D Appendix — Example Screenshots Bright Design Patterns from VR Games and Playful Applications

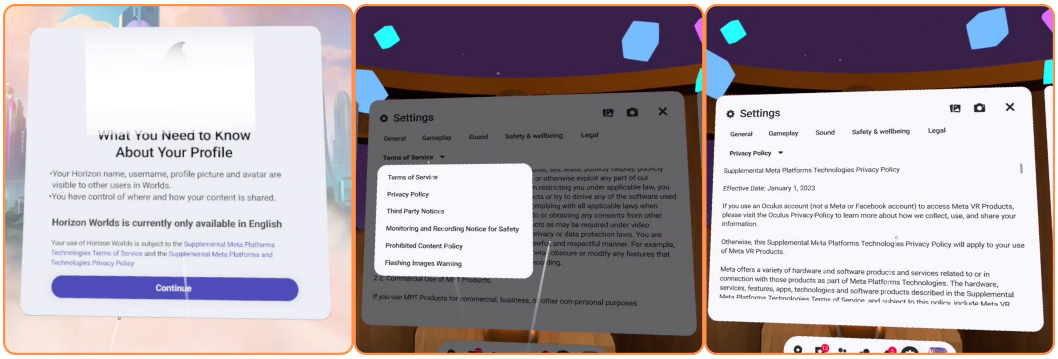


Fig. 14. The in-app privacy policy in *Meta Horizon Worlds* exemplifies the **`Accessible privacy policy`** bright design pattern. Upon entry, the application provides users with a brief description of its data practices, along with hyperlinks to more detailed information available on external webpages (see left screenshot). This privacy information can also be accessed at any time through the settings menu (see center and right screenshots). This design ensures users can easily revisit it as needed. *Note: Our researcher's username and avatar image are concealed in the screenshot for anonymity.*

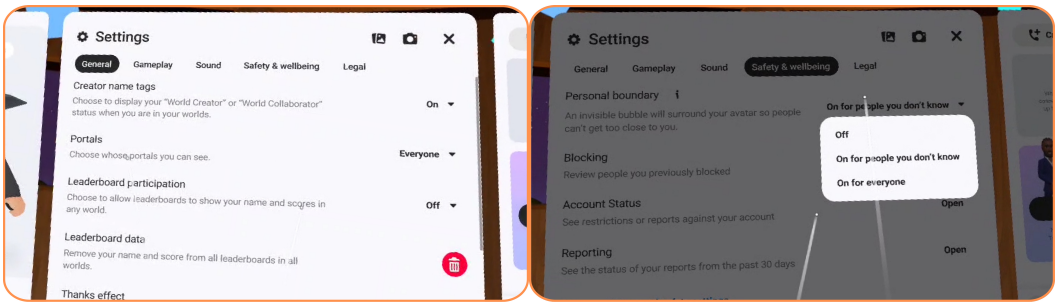


Fig. 15. The settings mechanism in *Meta Horizon Worlds* exemplifies the **`unbiased presentation of choices`** bright design pattern. All options in the menu are in black and white, with the data deletion option distinctively highlighted in red to make it stand out (see left screenshot). Even within the drop-down menus, the options maintain a consistent color scheme, with the most privacy-preserving choice ("off") placed at the top (see right screenshot).



Fig. 16. The consent interactions and settings mechanisms in *VRChat* (see the left and center screenshots) and the consent interactions mechanism in *TRIPP* (see right screenshot) exemplify the **`privacy-friendly default`** bright design pattern. These mechanisms ensure that privacy-related options are unchecked by default and require users to decide to opt-in. In *VRChat*, the microphone is set to "toggle" mode by default to prevent unintended listening by others. We note that although *VRChat* also enables auto-joining the world voice channel by default, we do not consider this a privacy-invasive bad default since the microphone remains in "toggle" mode and must be manually activated by the user. *Note: Our researcher's username is concealed in the right screenshot for anonymity.*



Fig. 17. The quality-of-life (QoL) features, such as the private beginner spaces in *VRChat* (see left screenshot) and *Meta Horizon Worlds* (see center screenshot) and private workspace in *Immersed* (see right screenshot), exemplify the **`private privacy configuration space`** bright design pattern. Upon entry, these applications place users in private spaces where they can explore functionalities, adjust settings, and customize avatars before interacting in public spaces. This design allows users to familiarize themselves with privacy settings, review policy information, configure privacy preferences, and customize their avatar and username tag to conceal personal information before joining public virtual worlds.



Fig. 18. The quality-of-life (QoL) feature, specifically the microphone icon in *VRChat* (see center screenshot), and the notification mechanisms in *The Room VR* (see left screenshot) and *Meta Horizon Worlds* (see right screenshot) exemplify the **`transparent communication of data practices`** bright design pattern. The *VR Chat* implemented a microphone icon on the bottom of the screen to keep users aware of their microphone status. *The Room VR* notifies users when their height is calibrated specifically for gameplay purposes, and *Meta Horizon Worlds* provides a brief description of data practices upon users' entry that clearly states what data is collected and for what purposes.



Fig. 19. The privacy resource mechanisms in *Meta Horizon Worlds* (see left screenshot) and *VR Chat* (see right screenshot) exemplify the **`clear control mechanisms`** bright design pattern. *Meta Horizon Worlds* uses an illustrative image to show users how to access the settings menu, and *VR Chat* provides sign boards to guide users to ensure that privacy controls can easily be located.

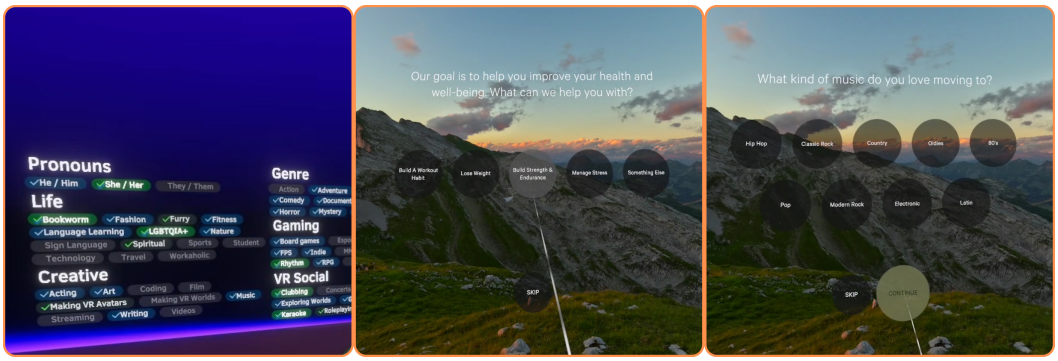


Fig. 20. The quality-of-life (QoL) features in *VRChat* (see left screenshot) and *Supernatural* (see center and right screenshots) exemplify the **balanced privacy and functionality** bright design pattern. In *VRChat*, users are invited to provide personal details like lifestyle and social preferences to help find matching friends, but this step is optional. The friend-matching can still be made without sharing this information. In *Supernatural*, users are asked to select their fitness goals and preferred music genre for sessions, with the option to skip these selections if preferred.

E Appendix — Privacy Policy Readability Assessment

Following GPEN's approach [46], we assessed the readability of the 13 selected privacy policies using the Flesch Reading Ease Score in Microsoft 365.[17] We copied the content of each privacy policy into a Word document and evaluated its readability using the *Flesch Reading Ease* option under the *Editor* menu. Table 6 presents the results, where lower scores indicate more difficult contents requiring a higher education level to understand.

Table 6. Readability of Privacy Policies based on Flesch Reading Ease (FRE) Assessment

Privacy Policy	Date Published	Date Retrieved	Language	FRE Score*
Beat Saber	June 2023	March 2024	English	42.4
Moss: Book II	September 2021	February 2024	English	36.5
The Room VR	February 2022	June 2024	English	46.4
A Fisherman's Tale	April 2023	June 2024	English	50.6
Down the Rabbit Hole	March 2020	June 2024	English	34.8
LEGO®Bricktales	November 2023	June 2024	English	39.2
The Climb 2	n.d.	July 2024	English	38.7
VRChat	November 2023	June 2024	English	35.9
TRIPP	November 2023	July 2024	English	36.1
Supernatural	July 2024	July 2024	English	35.6
Immersed	August 2024	August 2024	English	41.3
Meta Horizon Worlds Meta Platforms Technologies Privacy Policy	June 2024	August 2024	English	42.5

Note. *All privacy policies have a Flesch Reading Ease (FRE) score ranging from 30 to 50, indicating they are "difficult to read" and require at least "college" level knowledge. According to: https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests

[17] Microsoft Support. (n.d.). Get your document's readability and level statistics. Retrieved August 27, 2024, from https://support.microsoft.com/en-us/office/get-your-document-s-readability-and-level-statistics-85b4969e-e80a-4777-8dd3-f7fc3c8b3fd2

F Appendix — Information Flow by Senders

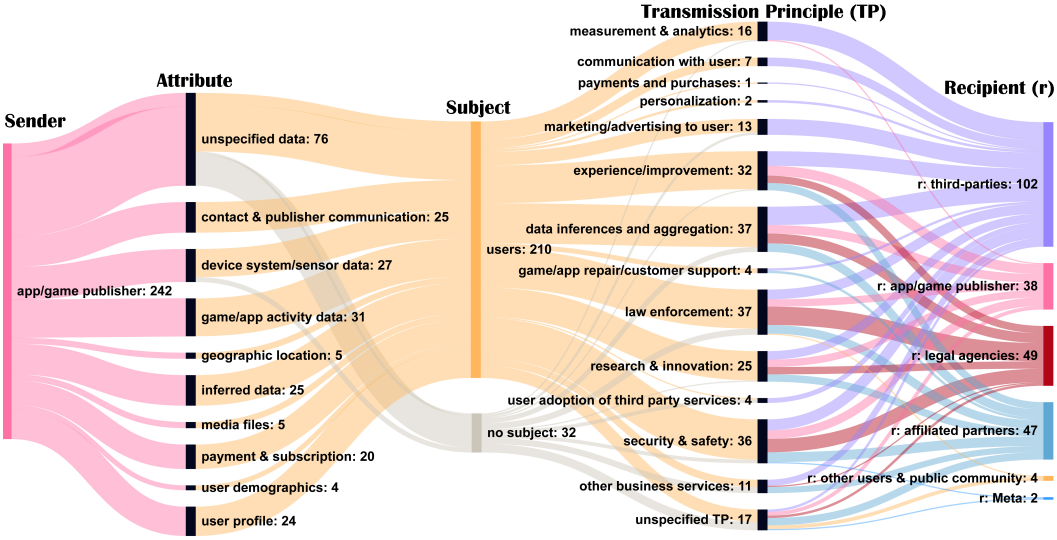


Fig. 21. This Sankey Diagram visualizes the 242 information flows sent from the "app/game publisher" that we identified from 21 privacy policy statements through our thematic analysis of 12 privacy policies. Multiple information flows may be derived from a single policy statement if it involves multiple instances of the same CI factor. For example, if an *attribute* is transmitted to various *recipients*, the transmission to each *recipient* represents a separate information flow. The diagram moves from left to right, showing the codes in the information flows across the five CI framework themes: (1) sender, (2) attribute, (3) subject, (4) transmission principle, and (5) recipient. For example, "device system/sensor data" appears as the data attribute in 27 flows. Color schemes distinguish different information flows. For example, colors flowing from *attribute* to *subject* identify the subject of which *attribute* relates to. *Note: despite our efforts to accurately classify and differentiate these information flows in the thematic analysis, ambiguous language in privacy policies may affect the accuracy of this figure, particularly when multiple CI factors are grouped together in a same policy statement without clear distinctions between their relationships. Nonetheless, the classification of these information flows still provides valuable insights into general patterns of data collection and sharing in VR applications.*

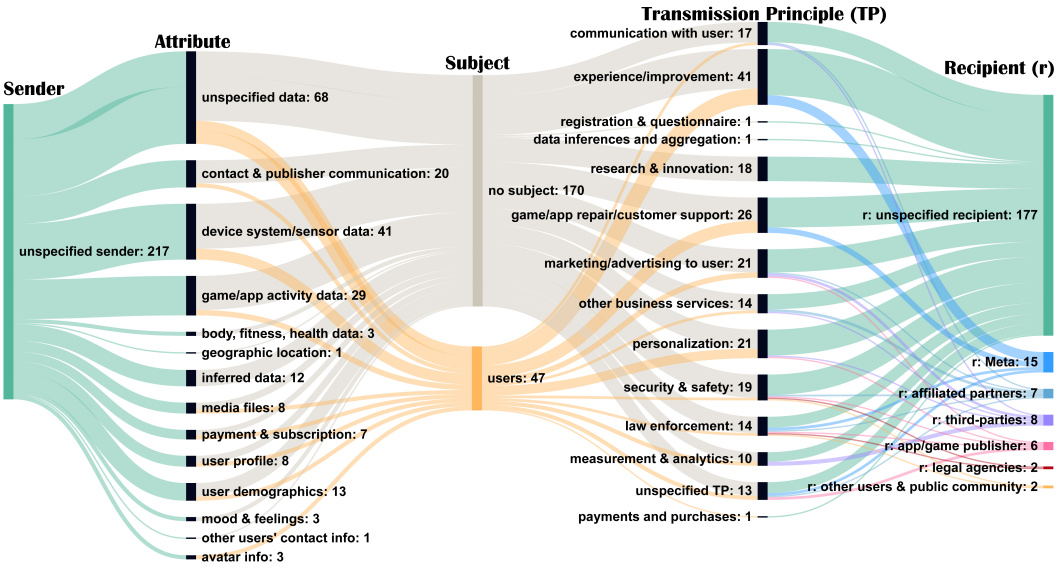


Fig. 22. This Sankey Diagram visualizes the 217 information flows sent from the "unspecified sender" that we identified from 87 privacy policy statements through our thematic analysis of 12 privacy policies. Multiple information flows may be derived from a single policy statement if it involves multiple instances of the same CI factor. For example, if an *attribute* is transmitted to various *recipients*, the transmission to each *recipient* represents a separate information flow. The diagram moves from left to right, showing the codes in the information flows across the five CI framework themes: (1) sender, (2) attribute, (3) subject, (4) transmission principle, and (5) recipient. For example, "device system/sensor data" appears as the data attribute in 41 flows. Color schemes distinguish different information flows. For example, colors flowing from *attribute* to *subject* identify the subject of which *attribute* relates to. *Note: despite our efforts to accurately classify and differentiate these information flows in the thematic analysis, ambiguous language in privacy policies may affect the accuracy of this figure, particularly when multiple CI factors are grouped together in a same policy statement without clear distinctions between their relationships. Nonetheless, the classification of these information flows still provides valuable insights into general patterns of data collection and sharing in VR applications.*

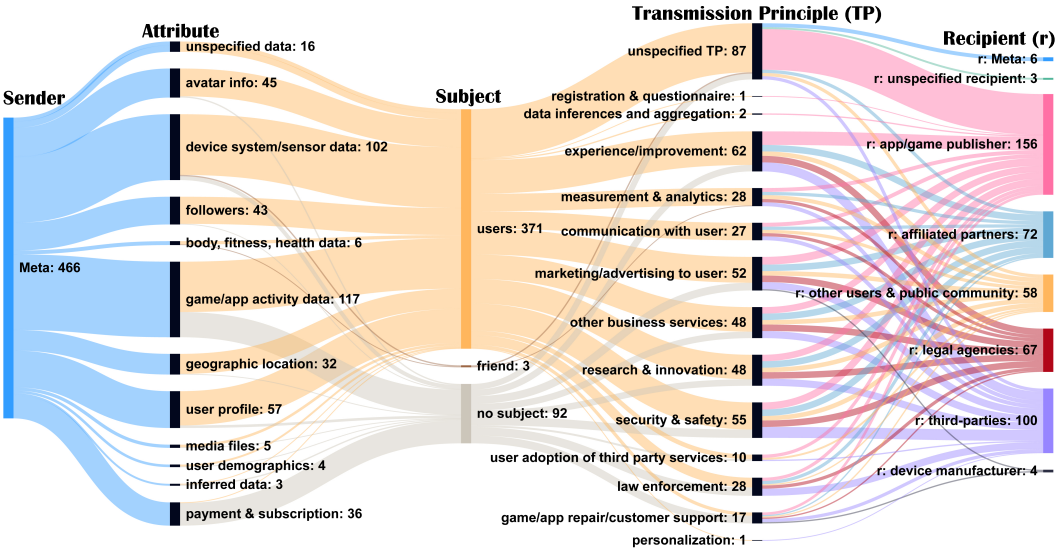


Fig. 23. This Sankey Diagram visualizes the 466 information flows sent from the "Meta" Quest VR platform that we identified from 53 privacy policy statements through our thematic analysis of 12 privacy policies. Multiple information flows may be derived from a single policy statement if it involves multiple instances of the same CI factor. For example, if an *attribute* is transmitted to various *recipients*, the transmission to each *recipient* represents a separate information flow. The diagram moves from left to right, showing the codes in the information flows across the five CI framework themes: (1) sender, (2) attribute, (3) subject, (4) transmission principle, and (5) recipient. For example, "device system/sensor data" appears as the data attribute in 41 flows. Color schemes distinguish different information flows. For example, colors flowing from *attribute* to *subject* identify the subject of which *attribute* relates to. *Note: despite our efforts to accurately classify and differentiate these information flows in the thematic analysis, ambiguous language in privacy policies may affect the accuracy of this figure, particularly when multiple CI factors are grouped together in a same policy statement without clear distinctions between their relationships. Nonetheless, the classification of these information flows still provides valuable insights into general patterns of data collection and sharing in VR applications.*

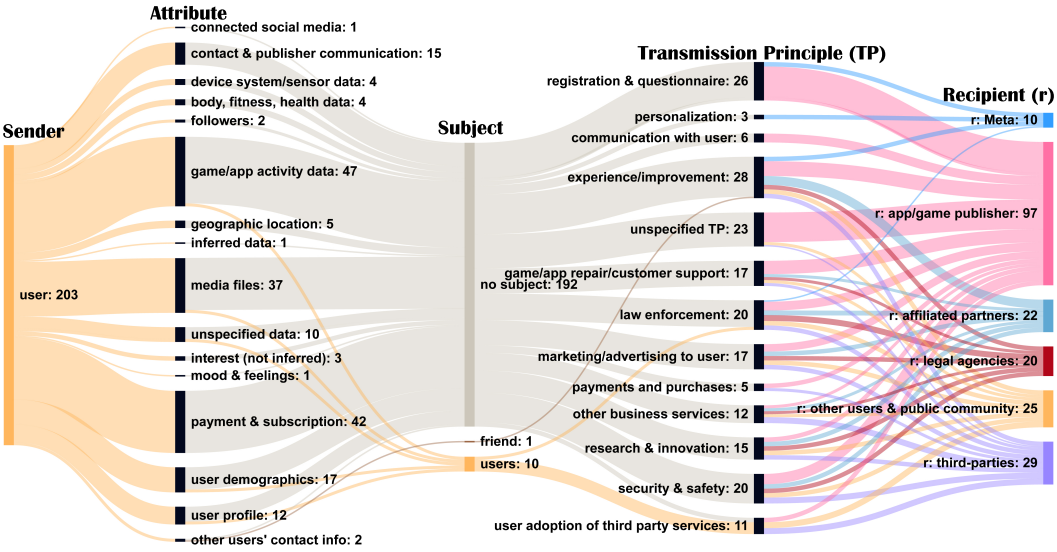


Fig. 24. This Sankey Diagram visualizes the 203 information flows sent from the "User" directly that we identified from 42 privacy policy statements through our thematic analysis of 12 privacy policies. Multiple information flows may be derived from a single policy statement if it involves multiple instances of the same CI factor. For example, if an *attribute* is transmitted to various *recipients*, the transmission to each *recipient* represents a separate information flow. The diagram moves from left to right, showing the codes in the information flows across the five CI framework themes: (1) sender, (2) attribute, (3) subject, (4) transmission principle, and (5) recipient. For example, "device system/sensor data" appears as the data attribute in 41 flows. Color schemes distinguish different information flows. For example, colors flowing from *attribute* to *subject* identify the subject of which *attribute* relates to. *Note: despite our efforts to accurately classify and differentiate these information flows in the thematic analysis, ambiguous language in privacy policies may affect the accuracy of this figure, particularly when multiple CI factors are grouped together in a same policy statement without clear distinctions between their relationships. Nonetheless, the classification of these information flows still provides valuable insights into general patterns of data collection and sharing in VR applications.*

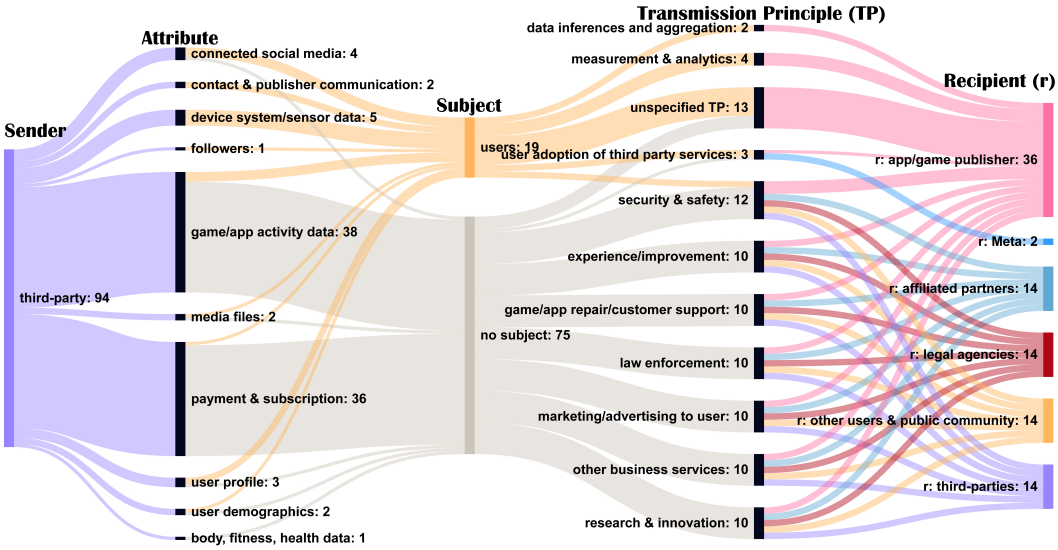


Fig. 25. This Sankey Diagram visualizes the 94 information flows sent from the "third parties" that we identified from 9 privacy policy statements through our thematic analysis of 12 privacy policies. Multiple information flows may be derived from a single policy statement if it involves multiple instances of the same CI factor. For example, if an *attribute* is transmitted to various *recipients*, the transmission to each *recipient* represents a separate information flow. The diagram moves from left to right, showing the codes in the information flows across the five CI framework themes: (1) sender, (2) attribute, (3) subject, (4) transmission principle, and (5) recipient. For example, "device system/sensor data" appears as the data attribute in 41 flows. Color schemes distinguish different information flows. For example, colors flowing from *attribute* to *subject* identify the subject of which *attribute* relates to. *Note: despite our efforts to accurately classify and differentiate these information flows in the thematic analysis, ambiguous language in privacy policies may affect the accuracy of this figure, particularly when multiple CI factors are grouped together in a same policy statement without clear distinctions between their relationships. Nonetheless, the classification of these information flows still provides valuable insights into general patterns of data collection and sharing in VR applications.*

Received October 2024; revised April 2025; accepted August 2025