Studying Immersive Deception: Manifestations and User Perceptions of Deceptive Design in Commercial Virtual Reality

by

Hilda Hadan

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Systems Design Engineering

Waterloo, Ontario, Canada, 2025

© Hilda Hadan 2025

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner:	Dr. Casper Harteveld Professor, Department of Art & Design Associate Dean of Graduate Programs and Strategic Initiatives Northeastern University
Supervisors:	Dr. Leah Zhang-Kennedy Assistant Professor, Stratford School of Interaction Design and Business Cross-appointed in Dept. of Systems Design Engineering University of Waterloo
	Dr. Oliver Schneider Associate Professor, Dept. of Management Science and Engineering University of Waterloo
Internal Member:	Dr. Cosmin Munteanu Associate Professor, Dept. of Systems Design Engineering University of Waterloo
	Dr. Ville Mäkelä Assistant Professor, Stratford School of Interaction Design and Business Cross-appointed in Dept. of Systems Design Engineering University of Waterloo
External Member:	Dr. Lennart Nacke Professor, Stratford School of Interaction Design and Business University of Waterloo

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

Chapters 1, 2, and 8 of this thesis were exclusively written by Hilda Hadan under the supervision of Dr. Leah Zhang-Kennedy and Dr. Lennart Nacke and were not written for publication. The remaining chapters of this thesis include portions from five manuscripts published in journals and conference proceedings. The exceptions to Hilda Hadan's sole authorship are detailed as follows:

Dr. Leah Zhang-Kennedy and Dr. Lennart Nacke served as the primary co-investigators on the grants that supported this work. These grants included the Office of the Privacy Commissioner of Canada (OPC) Contributions Program 2024-2025, the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grants, the Social Sciences and Humanities Research Council of Canada (SSHRC) Insight Grant, the Canada Foundation for Innovation (CFI) JELF Grant, and the University of Waterloo Games Institute (GI) 2024 Seed Research Grant.

Research in Chapter 3 is based on a systematization of knowledge of deceptive design in immersive technologies, published in collaboration with Lydia Choong [100]. This research was conducted at the University of Waterloo by Hilda Hadan under the mentorship of Dr. Lennart Nacke and Dr. Leah Zhang-Kennedy. Hilda Hadan, Lydia Choong, and Dr. Lennart Nacke contributed to the study design, literature search keyword formulation, and literature collection and analysis. Hilda Hadan and Lydia Choong were the primary coders in the analysis, with Dr. Lennart Nacke participated in the coding process as the tie breaker. Hilda Hadan drafted the initial manuscript, and Lydia Choong, Dr. Lennart Nacke, and Dr. Leah Zhang-Kennedy provided intellectual input.

Research in Chapter 4 is based on an empirical study, published in collaboration with Derrick M. Wang, Dr. Leah Zhang-Kennedy and Dr. Lennart Nacke [105]. This research was conducted at the University of Waterloo by Hilda Hadan under the supervision of Dr. Leah Zhang-Kennedy. Hilda Hadan and Dr. Leah Zhang-Kennedy contributed to the study design and data collection. Hilda Hadan conducted statistical analysis, and Hilda Hadan and Derrick M. Wang were the primary coders for the qualitative analysis. Hilda Hadan

drafted the initial manuscript, and Derrick M. Wang, Dr. Lennart Nacke, and Dr. Leah Zhang-Kennedy provided intellectual input.

Research in Chapter 5 is based on a literature analysis [106]. This research was conducted at the University of Waterloo by Hilda Hadan under the mentorship of Dr. Leah Zhang-Kennedy and Dr. Lennart Nacke. Hilda Hadan contributed to the study design and Hilda Hadan and Dr. Lennart Nacke contributed to the literature selection and synthesis of deceptive pattern definitions and examples from the literature through an affinity diagramming approach. Hilda Hadan drafted the original manuscript, and Dr. Lennart Nacke, and Dr. Leah Zhang-Kennedy provided intellectual input on the manuscript draft.

Research in Chapter 6 is based on a mixed-methods qualitative research, published in collaboration with PhD candidate Sabrina Alicia Sgandurra from the University of Waterloo, Department of English Language and Literature [103]. This research was conducted at the University of Waterloo by Hilda Hadan under the mentorship of Dr. Lennart Nacke. Hilda Hadan and Dr. Lennart Nacke contributed to study design and data collection. Hilda Hadan and Sabrina Alicia Sgandurra contributed to data analysis as the primary coders, with the assistance of Michaela Valiquette. Hilda Hadan drafted the initial manuscript, and Sabrina Alicia Sgandurra, Dr. Lennart Nacke, and Dr. Leah Zhang-Kennedy provided intellectual input.

Research in Chapter 7 is based on a mixed-methods qualitative research, conducted in collaboration with Dr. Lennart Nacke and graduate researcher Michaela Valiquette from Carleton University [11]. This research was conducted at the University of Waterloo by Hilda Hadan under the supervision of Dr. Leah Zhang-Kennedy. Hilda Hadan and Dr. Leah Zhang-Kennedy contributed to study design. Hilda Hadan contributed to the autoethnography data collection and analysis. Hilda Hadan and Dr. Leah Zhang-Kennedy contributed to the user survey data collection, which was analyzed through thematic analysis by Hilda Hadan and Michaela Valiquette as the coders. Hilda Hadan drafted the original manuscripts, and Michaela Valiquette, Dr. Lennart Nacke, and Dr. Leah Zhang-Kennedy provided intellectual input on the manuscript drafts.

Abstract

Deceptive Design (formerly "dark patterns") refers to design practices that distort or impair users' ability to make informed decisions, regardless of intent. As immersive technologies, such as Virtual Reality (VR) and Augmented Reality (AR), transform people's daily experiences, their immersive virtual environments unleash a highly engaging experience while enabling new opportunities for deceptive design strategies that users cannot easily recognize or resist. Consequently, ethical and privacy concerns are expanding into these environments. While previous research has examined deceptive design issues in websites, mobile apps, games, and gamification, the extent of these problems in immersive environments remains largely unexplored. This thesis investigates deceptive design in immersive environments with a specific attention to VR. It identifies deceptive design that presents in VR and emerges from VR technology's unique properties, and examines their impacts from users' perspective.

We first conducted a systematic literature review to synthesize the state-of-the-art research on deceptive design. This review revealed potential deceptive strategies that can be employed in immersive environments, and those that can be enabled by the large amount of user data collected by these technologies. However, most of the existing literature focused on hypothetical scenarios rather than examining deceptive design as it appears in commercially available applications. Informed by the findings from this review, we surveyed experienced users about their awareness of data practices in immersive technologies, examined deceptive design in commercially available VR applications, and compared these findings with those from traditional computer platforms. To ensure consistent and comparable deceptive design analyses across these platforms, we developed a *Deceptive Design Assessment Guide* grounded in foundational deceptive design literature. This *Assessment Guide* was applied and validated in two studies that examined how deceptive practices manifest and influence user experience in exemplary computer and VR applications. Our findings show that the deceptive design in VR applications relies heavily on 2D interfaces, such as dialogue windows and checkboxes, rather than fully integrating VR-specific properties. Hypothesized scenarios from the literature, such as perception-hacking and emotional-based manipulation,

were not observed in our selected VR applications. Certain VR properties (e.g., realistic simulation, virtual-physical barrier) amplified the impacts of deceptive design in users' decision-making process but did not directly enable it. While users cannot point out specific design elements that used deceptive practices, they still expressed a general discomfort and feeling of manipulation. Nevertheless, many users felt powerless in protecting themselves or asserting their autonomy, and perceived deceptive design as a standardized industry practice with no possible escapes.

Our research has implications for future research, and immersive technology design, development, and regulation for building better industry design standards and stronger user protections. For future researchers, the findings provide guidance on fostering user awareness through effective educational strategies, expanding theoretical approaches for understanding deceptive design in immersive environments, and refining user-centered empirical approaches for identifying and evaluating deceptive practices. For designers and developers, this thesis offers a structured *Assessment Guide* and actionable recommendations for supporting the creation of ethical and user-centered immersive applications that respect privacy and autonomy. For immersive technology regulation, this thesis identifies the limitations of current regulations and provides practical advice for expanding and strengthening regulatory frameworks, enforcing transparent privacy communication and ethical industry design standards tailored to immersive technologies. In conclusion, this thesis advances the understanding of deceptive design in commercially available VR applications, delivers actionable strategies for identifying and mitigating deceptive practices, and establishes a foundation for cross-disciplinary collaborations to protect user well-being in immersive environments.

Acknowledgements

As I conclude this challenging yet rewarding journey, I would like to express my sincere gratitude to the many people who have supported me throughout my doctoral research.

First and foremost, the completion of this thesis would not have been possible without the guidance from my beloved mentors, Dr. Leah Zhang-Kennedy, Dr. Oliver Schneider, and Dr. Lennart Nacke. I am deeply thankful to them for giving me the opportunity to pursue my PhD research. Their mentorship, insightful advice, and unwavering support have been instrumental in guiding me through every stage of my research journey.

I am also sincerely grateful to my committee members, Dr. Ville Mäkelä, Dr. Cosmin Munteanu, and Dr. Casper Harteveld, for their expertise and constructive feedback. Their diverse perspectives and thoughtful insights have greatly enriched my work and supported me in refining and strengthening this dissertation.

This thesis would not have been possible without the HCI Games Group. Special thanks to Ph.D. (Postdocs & Hilda's Driver) candidate Derrick M. Wang, who drove me to groceries so I did not live on instant noodles, edited my presentation videos so they became less cringe, and supported me in qualitative analyses to keep our papers credible. I am also deeply appreciative of Dr. Reza Hadi Mogavi, whose radiant positivity and encouraging spirit have been a source of motivation and a guiding light throughout my research journey. Huge thanks to Michaela Valiquette and Lydia (Lili) Choong, whose collaboration and data analysis skills turned my chaos datasets into clarity.

Thank you to my roommate, Amy J. Nahwegahbow, who kept me alive with home-cooked meals during my 'research hermit' phases, acted as my unofficial life coach and cooking instructor, and saved me from raw chickens and undercooked potatoes. I am also thankful for our countless horror movie nights and the endless bags of chips that restored my sanity after paper rejections.

I also thank the generous support of the Games Institute, which provided an environment and resources essential to conducting my studies, connecting with colleagues, practicing presentations, writing research manuscripts, and hosting both my PhD comprehensive

examination and defence. I especially want to thank Associate Director Agata Antkiewicz and Executive Director Dr. Neil Randall, whose dedication kept the Institute running and made it feel like home.

I also want to thank the designers, developers, and publishers of Overwatch, Genshin Impact, Marvel Rivals, Don't Starve Together, R.E.P.O., and other 112 games on Steam and Meta VR Store for providing the best mental breaks I needed to survive the tough time of my PhD. Thanks to all my friends in these games for the lively voice chats, the perfectly imperfect teamwork, and the unpredictable friendly fire that gave me something to look forward to after my long days of research. Without you, I would probably have graduated a year earlier. Thanks to Overwatch for igniting my passion for deceptive design research and providing such a rich case for my first video game study.

Lastly, I gratefully acknowledge the financial support that some of the research in this thesis were funded by the Office of the Privacy Commissioner of Canada (OPC) Contributions Program 2024-2025, the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grants, the Social Sciences and Humanities Research Council of Canada (SSHRC) Insight Grant, and the Canada Foundation for Innovation (CFI) JELF Grant, and the University of Waterloo Games Institute 2024 Seed Research Grant. The views expressed herein are those of the authors and do not necessarily reflect the views of the OPC, NSERC, SSHRC, the CFI, the Games Institute, nor the University of Waterloo.

Dedication

To Dr. L. Jean Camp, whose remarkable mentorship ignited my passion for research and taught me that it is never too late to pursue my true interest.

Also to my parents and grandparents whose support has shaped the person I am today.

Table of Contents

Examining Committee ii

Author's Declaration iii

Statement of Contributions iv

Abstract vi

Acknowledgements viii

Dedication x

List of Figures xix

List of Tables xxvii

1 Introduction 1

1.1 Motivation 1

1.2 Research Statement 2

1.3 Contributions 4

1.4 Related Publications 6
1.5 Thesis Outline 8

2 Background **9**

2.1 Deceptive Design and Its Theoretical Evolution 9
2.1.1 From Patterns, Antipatterns, to Deceptive Design 9
2.1.2 Decision-Making and Choice Architecture 10
2.1.3 Nudge, Sludge, Persuasion, and Coercion 12
2.1.4 Harms from Deceptive Design 13
2.2 Virtual Reality and Its Properties 14
2.3 Established Deceptive Design Research Methodologies 18
2.3.1 Design, Regulatory, and Literature Perspectives 18
2.3.2 User Experience Perspectives 19

3 Synthesizing State-of-the-Art in Deceptive Design Research in Immersive Environments **21**

3.1 Introduction 21
3.1.1 Motivation and Gaps in Existing Literature 22
3.1.2 Chapter Research Goal 22
3.1.3 Chapter Contributions 23
3.2 Methodology 24
3.2.1 Literature Search and Screening 24
3.2.2 Thematic Synthesis 26
3.3 Findings 27

3.3.1 Themes 1 & 2: Properties of immersive technologies are capable of enhancing user experience while amplifying user manipulation . . . 29
3.3.2 Themes 3-5: Psychological manipulation, Reality distortion, and User perception tricking . . . 30
3.3.3 Themes 6-7: Privacy and security risks, changes in users' views and beliefs, and buying decisions . . . 32
3.3.4 Theme 8: manipulation prevention techniques . . . 33
3.4 Discussion . . . 34
3.5 Limitations . . . 34
3.6 Literature Gaps and Research Direction . . . 35

4 Understanding User Awareness and Concerns About Data Practices in Immersive 37

4.1 Introduction . . . 37
4.1.1 Motivation and Gaps in Existing Literature . . . 38
4.1.2 Chapter Research Goal . . . 38
4.1.3 Chapter Contributions . . . 39
4.2 Methodology . . . 40
4.2.1 Scenario Development and Survey Design . . . 40
4.2.2 Recruitment and Participants . . . 44
4.2.3 Data Analysis . . . 44
4.3 Findings . . . 45
4.3.1 RQ4.1: How much are people aware of the data collected through Immersive Technologies? . . . 45
4.3.2 RQ4.2: To what extend are people concerned about their privacy regarding data collection in Immersive Technologies? . . . 46

4.3.3 RQ4.3: What factors contribute to user privacy concerns in Immersive Technologies? . . . 47
4.3.4 RQ4.4: What coping strategies (if any) do people use to mitigate their privacy concerns? . . . 51
4.4 Discussion . . . 54
4.4.1 Users' Resignation and Limited Mitigation Strategies . . . 54
4.4.2 Limited User Awareness of Data Practices . . . 55
4.4.3 Limitations . . . 56
4.5 Conclusion . . . 56

5 Developing an Assessment Guide for Investigating Deceptive Design in Immersive Environments 58
5.1 Introduction . . . 58
5.1.1 Motivation and Gaps in Existing Research . . . 59
5.1.2 Chapter Research Goal and Contribution . . . 59
5.2 Constructing Deceptive Design Assessment Guide Based on Literature . . . 60
5.3 Discussion and Conclusion . . . 64

6 A Preliminary Exploration on Deceptive Design in Immersive Environments 65
6.1 Introduction . . . 65
6.1.1 Motivation and Gaps in Existing Literature . . . 66
6.1.2 Chapter Research Goal and Context . . . 67
6.1.3 Chapter Contributions . . . 68
6.2 Methodology . . . 70

6.2.1 Analyzing Design Mechanics in the Computer Application 70
6.2.2 Analyzing User Perspectives on the Computer Application 72
6.2.3 Autoethnographic Analysis of Deceptive Design in VR Applications 73
6.2.4 Ethical Considerations 75
6.3 Findings 75
6.3.1 RQ6.1: Deceptive Design Patterns and User Impacts in the Computer Application 75
6.3.2 RQ6.2: What deceptive design patterns are currently implemented in commercial VR games? 82
6.4 Discussion 83
6.4.1 Limitations 85
6.5 Conclusion 85

7 A Structured Investigation of Deceptive Design in Immersive Environments 87

7.1 Introduction 87
7.1.1 Motivation and Gaps in Existing Literature 88
7.1.2 Chapter Research Goal 88
7.1.3 Chapter Contributions 89
7.2 Methodology 90
7.2.1 Research Context 90
7.2.2 Design Mechanics Evaluation 92
7.2.3 Scenario-Based User Survey 94
7.3 Findings 100

7.3.1 RQ7.1: Deceptive Design in VR Privacy Communication Design Mechanics . . . 100
7.3.2 RQ7.2: Awareness, Perceptions, and Concerns about deceptive design and online privacy . . . 105
7.4 Discussion and Future Work . . . 110
7.4.1 Limitations . . . 111
7.5 Conclusion . . . 112

8 Contributions, Implications, and Future Work 113
8.1 Contributions to Research Objectives . . . 114
8.1.1 Objective 1: Understand the existing state-of-the-art research of deceptive design in immersive environments . . . 114
8.1.2 Objective 2: Develop a structured guide for assessing deceptive design in VR based on foundational literature. . . . 115
8.1.3 Objective 3: Investigate and compare the manifestation of deceptive design in commercially available VR and computer applications. . . . 116
8.1.4 Objective 4: Contextualize VR deceptive design analysis in user experiences and perceptions. . . . 121
8.2 Implications for Future Research, Immersive Technology Design, Development, and Regulation . . . 122
8.2.1 Implications for Future Researchers . . . 123
8.2.2 Implications for Immersive Technology Designers, Developers, and Publishers . . . 127
8.2.3 Implications for Immersive Technology Regulation . . . 131
8.3 Future Work . . . 135
8.4 Conclusion . . . 136

References **138**

APPENDICES **162**

A Appendix A Reflexivity Statement **163**

B Appendix B AI Disclosure Statement **166**

C Appendix C Materials from Study "Understanding User Awareness and Concerns..." **168**

C.1 Survey Questions 168

C.1.1 User Awareness of XR Data Operation 168

C.1.2 Scenarios and Questions 169

C.2 Codebook 171

C.3 Participant Demographic Information 173

C.4 Wilcoxon Signed Rank Test 176

D Appendix D Materials from Study "A Preliminary Exploration on..." **180**

D.1 Example of Our Game Mechanics Analysis Process 180

D.2 Reddit Search Keywords 183

D.3 OW2 In-Game Items Glossary 184

D.4 Sample Diary Entry Structure 186

D.5 Deceptive Game Design Patterns Identified from Overwatch2 and VR Applications 187

D.6 Thematic Analysis Codebook of Reddit Posts 193

E Appendix E Materials from "A Structured Investigation of..." 195

E.1 Example Diary Entry 196

E.2 Example Screenshots Deceptive Design Patterns from VR Games and Playful Applications 197

E.3 Privacy Policy Readability Assessment 203

E.4 Detailed Demographics 204

E.5 Kendall correlation matrix of participants' awareness and concerns about VR deceptive design and privacy, and demographics 207

E.6 Scenarios 208

E.7 Survey Questionnaire 216

E.7.1 General Experience with VR Technology and Selected Applications 216

E.7.2 Perception and Experience with Privacy Deceptive Design Patterns 218

E.7.3 General Concerns of Influence of Online Design and Privacy 221

List of Figures

3.1 This PRISMA flow diagram [201] presents all the phases of our systematic analysis of the literature, from the identification of articles to the final articles we included. 24

4.1 Survey flow: Upon passing the screening questionnaire, 464 participants were asked about their understanding of immersive technologies and awareness of data collection. Next, they were presented with four randomly selected scenarios from a total of 18 scenarios from Table 4.2, resulting in approximately 103 responses per scenario. For each scenario, participants answered questions relating to comfort with data collection, perceived data sensitivity, and how realistic they perceived the scenario to be. Finally, the participants shared their experience with immersive technologies and demographic information. 40

4.2 Percentage of participants' ($N = 464$) perceived data collection of various data types through immersive technologies. 46

4.3 Participants' ($n = 464$) comfort level, perceived data sensitivity, and scenario realism across data types and device statuses. Darker cells indicate higher percentages. For example, 29% of participants selected "very uncomfortable" when their *cognitive, emotional, and personality estimates* were observed. . 47

4.4 n = number of participants who answered the conditional open-ended question: "What would you do (if any) to mitigate the discomfort raised?" (Q5). This question was shown only to those who selected as "1-very uncomfortable" or "2-uncomfortable" (Q3) in each scenario. Total percentages exceed 100% as a participant may mention multiple coping strategies. 52

6.1 Left: sample gameplay moment in *Moss2*, a VR puzzle adventure game where players guide a tiny mouse character through a fantastical world. Quill, the main character, gives the player a full-body hug, with her tiny arms wrapped tightly around the controller pointers. Center: sample gameplay moment in *Beat Saber*, a VR rhythm-based block-slashing game, when players are required to physically move left, right or squat down to avoid oncoming obstacles (semi-transparent walls). Right: sample gameplay moment in OW2, a first-person team-based shooter game, when players is using ability to heal (restore) the health of allies at the front by holding down the right-click on mouse. 68

6.2 Battle Pass from OW2 season 2. Each level requires 10,000 XPs (*Grinding*) and rewards players with an item (*Adorable Design*). A total of 80 "premium" items are only for players who paid premium fee (*Bundling*). The progress resets every season [61] (*Fear of Missing Out* and *Infinite Treadmill*). . . . 69

6.3 Weekly Challenges from OW2. The completion of each challenge offers 5,000 XPs (*Grinding*). Upon the completion of 4, 8, and 11 challenges, players can obtain 30, 20, and 10 OW coins (*Endowed Progress)*. The progress resets every week (*Fear of Missing Out*). 69

6.4 OW2 Game Shop from season 2 with bundles (*Bundling*) and "featured" items in a price that is different from amount of purchasable coins (*Waste Aversion*). Items refreshes periodically (*Countdown Timers*). 69

6.5 OW coins purchasable with real money (*Premium Currency*). 69

6.6 The new unlockable character from OW2 season 1. Players who have purchased the premium Battle Pass can unlock this character once they complete level 1. Other players can unlock this character once they complete level 55 (*Grinding*). Players who miss this opportunity will complete character-specific challenges in later seasons, a much lengthier and more difficult path of obtainment (*Fear of Missing Out*). 70

6.7 Percent of Reddit posts that mentioned each OW2 design mechanic. 76

7.1 Survey flow: After passing the screening questionnaire, participants answered about their experience with VR devices and the presented application. They were then shown a VR privacy mechanism scenario, followed by questions about their reactions, decision-making, the role of specific design elements in their decisions, and perceived privacy impacts. Lastly, participants answered their general concerns about online design influences, internet privacy, and demographic details. In total, we received $N = 424$ valid responses, with $n \approx 61$ per scenario. The full survey questionnaire is in Section E.7. 99

D.1 Example of our game mechanics labeling process on screenshots of OW2 Battle Pass. Only key screenshots are included in this example. From top to bottom: (1) core Battle Pass interface demonstrating rewards, XP requirements, and duration; (2) XP earning breakdown illustrating XP earning sources; (3) Battle Pass level purchase interface with prices in OW coins that are purchasable with real money. Green labels denotes specific deceptive game design patterns from our *Assessment Guide*. Green arrows and highlighted areas denote the presence of these deceptive game design in the game mechanics. In the deductive labeling process, we wrote down the "Notes" from our researchers during the collaborative review session to support labeling decisions. 181

D.2 Example of our game mechanics labeling process on screenshots of OW2 Battle Pass. Only key screenshots are included in this example. From top to bottom: (1) core Battle Pass interface demonstrating rewards, XP requirements, and duration; (2) Battle Pass information page detailing rewards and premium benefits; (3) mythic skin interface highlighting it's unique and customizable design. Green labels denotes specific deceptive game design patterns from our *Assessment Guide*. Green arrows and highlighted areas denote the presence of these deceptive game design in the game mechanics. In the deductive labelling process, we wrote down the "Notes" from our researchers during the collaborative review session to support labeling decisions. 182

E.1 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.* 197

E.2 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 photorealistic 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. 198

E.3 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. 199

E.4 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.* 199

E.5 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 photorealistic 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. 200

E.6 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 Chapter 7 and Section E.3). 200

E.7 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. 201

E.8 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. 201

E.9 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. 202

E.10 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 [177], as users' focus is naturally drawn to the visually striking VR game and application previews, and leave critical privacy information overlooked. . . 202

E.11 An example screenshot of the video clip. 218

E.12 Example UI elements we used to support participants' understanding. . . . 220

E.13 An example screenshot of the video clip. 221

List of Tables

2.1 The high-level and Meso-level deceptive patterns synthesized by Gray et al. [89], which served as the foundation of our *Assessment Guide* in Chapter 5. 11

2.2 Deceptive design attributes grouped by their influence on the user's choice architecture, by Mathur et al. [163]. 12

3.1 The final search queries in the syntax of each database. We kept the filters for all databases as consistent as possible. The search was conducted twice over each database in September 23 and 27, 2022 to ensure outcome consistency. 25

3.2 Overview of all publications included in the systematic literature review, and the identified themes and sub-themes (✔) by RQ. 28

4.1 Factors, their corresponding levels in the scenarios, and descriptions of each. 42

4.2 Summary of the 18 scenarios used in the study. ID= Scenario identifier, n = number of participants presented with each scenario. Each scenario was presented to approximately 103 participants on average. 43

4.3 Breakdown of our participants' ($N = 464$) gender, age, education level, income level, and three IUIPC dimensions [156]. A detailed overview of participants' demographic is located in Table C.2. 45

4.4 Univariate Cumulative Linked Mixed Model analyses of factors impacting participants' comfort level (5-point Likert data, from 1-very uncomfortable to 5-very comfortable), with a random intercept per participant. Ordinal data are used as is. Participants demographics and experience with immersive devices were considered in the analysis but are not presented as they did not show significance ($P > .05$). 49

4.5 Multivariate Cumulative Linked Mixed Model analyses of factors impacting participants' comfort level (1-very uncomfortable to 5-very comfortable), with a random intercept per participant. Ordinal data are used as is. Only variables showed significance are presented ($P \leq .05$). 50

5.1 This table presents our *Deceptive Design Assessment Guide* and the source literature of themes and codes [89, 287, 129, 100]. This *Assessment Guide* served as the foundation of our identification of deceptive designs in the selected VR-based and computer-based games. 61

6.1 This table presents the 24 deceptive design patterns we identified in *Overwatch2* (OW2), *Beat Saber* (BS), and *Moss Book: II* (*Moss2*) based on our *Assessment Guide* (see Chapter 5). Fourteen patterns from in OW2 and 14 patterns across the two VR games. See Section D.5 for specific game mechanics associated with each deceptive pattern and corresponding synthesized diary entries. 77

7.1 Summary of Selected Virtual Reality (VR) Applications. 91

7.2 Scenario 1-3 presented in our thesis. For the details of all seven scenarios, refer to Section E.6. 95

7.3 Participant demographics (n = 182), including gender, age, education level, professional VR work experience, IUIPC scores, and awareness and concerns about deceptive design. A detailed overview of participants' demographic is located in Section E.4. Participants received £8 for survey completion or GBP £0.80 if screened out. *DD=Deceptive Design.* 99

7.4 Using our *Assessment Guide* from Chapter 5, this table presents deceptive design we identified in the privacy communication and interaction mechanisms of 12 VR applications from our diary evaluation. 101

7.5 Scenarios 1-3 participants' awareness and concerns about the influence of VR application design on their choices and behaviors in personal information sharing decisions across six statements from the personal and the general perspectives. 106

8.1 Summary of observed deceptive design patterns in commercial VR applications in this thesis. See our *Assessment Guide* in Chapter 5 for the definition of each pattern. 117

C.1 This codebook presents the themes and codes we developed from participants' mitigation strategies responded to open-ended responses to Q5. 171

C.2 Overview of Participants' demographics ($N = 464$) 173

C.3 Wilcoxon Signed-Rank Tests with Bonferroni adjustment [34] on participants' comfort level and perceived data sensitivity across data types. A same pair of scenarios is presented to $n \approx 64$ participants. 176

C.4 Wilcoxon Signed-Rank Tests on participants' comfort level across device statues ($N = 464$). 179

D.1 Overwatch 2 In-Game Obtainable Items Glossary 184

D.2 Structural outline of a sample diary entry from a *Moss2* gameplay session on February 1, 2024. The diary was documented in Miro given its feasibility in linking videos, screenshots, and diary texts. From left to right: (1) description of the lead researcher's experience, reactions, thoughts, and feelings complemented by corresponding screenshots of game design elements, and (2) post-gameplay reflection on possible presence of deceptive game design and its context. 186

D.3 Deceptive designs identified in OW2 using our *Assessment Guide* (see Chapter 5), which formed the foundation for our qualitative analysis of user perceptions on Reddit. 187

D.4 Based on our *VR Deceptive Game Design Assessment Guide* in Table 5.1, this table presents deceptive design patterns we identified within *Moss2* and *Beat Saber*. 190

D.5 Codebook of players experiences and perceptions toward the candidate deceptive design and OW's business model transition, found in the Overwatch community discussions. 193

E.1 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. 196

E.2 Readability of Privacy Policies based on Flesch Reading Ease (FRE) Assessment 203

E.3 Overview of Participants' demographics (n=182) 204

E.4 Kendall's τ correlation matrix [68] of participants' awareness and concerns about VR deceptive design, online privacy, and demographics ($N = 182$). Only significant correlations ($P < .05$) are displayed. Low correlations ($\tau < 0.3$) have a white background; moderate correlations ($0.3 \leq \tau < 0.7$) have a light pink background. 207

E.5 Scenario description, corresponding VR application, design mechanism, and incorporated privacy deceptive design patterns. 208

E.6 This table presents the two screenshots used in each scenario, with 1 clean screenshot and 1 screenshot with all VR design elements labeled to facilitate participants' selection. 214

Chapter 1

Introduction

1.1 Motivation

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 [149, 22, 25]. The concept of deceptive design started to gain attention in 2010 when Harry Brignull [24] first introduced this concept. Since then, researchers have focused on its applications in various fields such as websites, mobile applications, games, and gamification [287, 54, 143]. Literature has identified four issues associated with deceptive design, including loss of autonomy and decision-making capability [163], financial loss [162, 149, 143, 19], labor and cognitive burdens [188, 154, 19, 83], and invasion of privacy [22, 163, 97].

The rise of immersive technologies [284], such as Virtual Reality (VR) and Augmented Reality (AR), and Mixed Reality (MR), has prompted discussions on deceptive design from experts in engineering [141, 245], security and privacy [27, 81], cognitive science [73], and humanities and social science [227]. Concerns about deceptive design in immersive technologies extend beyond the aesthetics of the design to include personal security [245, 141],

[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

safety [45], social implications [208, 227], ethical considerations [208, 227], and political influences [227] both during and after user engagement.

As a new medium for gaming and social interaction, VR opens a new frontier for manipulative tactics through its visual, audio, and haptic feedback that disconnects users from the real world [241, 259]. VR's spatial and realistic displays can enhance the subtlety of deceptive designs [100, 133], making it harder for users to critically assess content [45]. E-commerce companies could steer user decisions by rendering certain products brighter and more vivid than others, increasing the frequency with which users see the brand logo in the virtual environment, or even inducing artificial emotion and targeting users when vulnerable [169]. VR simulations using bodily sensor data enable hyper-personalized deceptive tactics [27, 169]. Additionally, privacy harms emerged from the uncertainty in VR data collection and inference [216], since new types of biometric data (e.g., people's gait or body movement patterns) are exposed [173, 206]. Users also 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 [196, 22, 97, 87]. Thus, deceptive design could be even more problematic in immersive environments because users are more deeply engaged and, therefore, more prone to manipulations [73].

Ethical and privacy concerns are growing as deceptive designs begin to expand to immersive environments [11]. However, most of the existing research relies on hypothetical scenarios, expert expectations, or controlled in-lab studies (e.g., [134, 169, 73, 100]), with limited attention to how deceptive design actually appears and functions in commercially available immersive platforms. As commercial games and social platforms continue migrating to immersive technologies, it becomes crucial to understand how deceptive practices evolve in these contexts and the implications for user autonomy and privacy.

1.2 Research Statement

The goal of this research is to examine how deceptive design manifests in commercially available immersive environments, including both patterns that migrate directly from

non-immersive environments and those that may emerge from the unique properties of immersive technologies. Given that deceptive design can distort users' understanding, influence their decisions, and lead to unintended data disclosures, we aim to assess the impact of deceptive design in VR on users' perceptions, behavioral responses, and digital privacy. The overarching research statement is:

How do deceptive design strategies manifest in Virtual Reality (VR) environments, and what are their impacts on user perceptions, behavioral responses, and digital privacy?

Scope: This thesis focuses on commercially available head-mounted display (HMD) VR technologies designed for general market users (e.g., Meta Quest[2] and Apple Vision Pro[3]). Specialized applications, such as those developed for healthcare or employment training, fall beyond the scope of this research. HMD-based VR is the most prevalent form of immersive technology available to consumers, with growing adoption in gaming, education, and social platforms [9, 10]. Thus, the outcomes from this thesis directly relate to various contexts in which people are currently using these technologies in their everyday lives, and provide practical insights for improving user autonomy, transparency, and ethical design in mainstream immersive applications.

For this research, we complete the following objectives:

Objective 1: Understand the existing state-of-the-art research of deceptive design in immersive environments (Chapter 3).

Objective 2: Develop a structured guide for assessing deceptive design in VR based on foundational literature (Chapter 5).

Objective 3: Investigate the manifestation of deceptive design in commercially available VR applications and compare them with those in traditional digital environments (Chapter 6 and Chapter 7).

Objective 4: Contextualize VR deceptive design analysis in user experiences and perceptions to explore how immersive properties amplify these issues and how users respond to the deceptive practices (Chapter 4, Chapter 6 and Chapter 7).

[2]Meta Quest Headset. https://www.meta.com/quest/
[3]Apple Vision Pro. https://www.apple.com/apple-vision-pro/

Given that early deceptive design literature often treats immersive technologies as a single category (e.g., [141, 20, 227]) and that many immersive technologies share similar data collection and processing capabilities [105, 284], Chapter 3, Chapter 4 and Chapter 5 take a broader perspective that examines the deceptive design and privacy problem across all immersive environments. In Chapter 6 and Chapter 7, we narrow our scope to focus specifically on commercially available VR applications.

1.3 Contributions

Through the examination of design mechanisms, critical researcher reflection, and user perspective analysis, this thesis contributes to the understanding of deceptive design in commercial VR applications by demonstrating that while current VR deceptive strategies primarily rely on traditional 2D interfaces, VR-specific properties can amplify their impact on user perception, experience, and decision-making.

The main contributions of each chapter of this thesis are:

- A systematic literature review (Chapter 3) that synthesizes current state of research on deceptive design in immersive environments. The findings illustrate gaps in understanding how these designs manifest in commercially available technologies, and emphasize the need to consider user perspectives and VR-specific data practices when developing mitigation and prevention strategies. These findings shaped the overall research direction of this thesis and informed the study designs of subsequent chapters.

- A synthesis of immersive technology data practices from academic literature and technical reports, and an online survey with experienced users (Chapter 4). The findings reveal users' limited awareness of data practices in immersive technologies, a sense of resignation about privacy risks, and reliance on inadequate protective strategies borrowed from non-immersive settings.

- A synthesis of foundational taxonomies in the research field of deceptive design, which results in a structured *Deceptive Design Assessment Guide* (Chapter 5) for identifying, analyzing, and evaluating deceptive design practices across immersive platforms. This *Assessment Guide* draws from foundational taxonomies of deceptive design in web, mobile, and immersive environments, supporting the analysis of both deceptive strategies that migrate directly from non-immersive platforms and those that may emerge from the unique properties of immersive technologies, as hypothesized in the literature (Chapter 3). This *Assessment Guide* offers a practical foundation for future research, ethical design evaluation, and intervention development.

- A comparative study of exemplary computer and VR applications (Chapter 6), combining a design mechanism analysis through autoethnography with a user perspective analysis based on an online survey and Reddit player reviews. The findings show how deceptive designs manifest in the same or different ways across platforms, with VR's multi-sensory stimuli and spatial display evoking users' immersion and emotional bond and amplifying the impacts of deceptive design. The user perspective investigations also reveal the diminished user experience due to the presence of deceptive design, which discourages users' long-term engagement and detriments the application and the creators' sustainability.

- A detailed examination of 12 popular VR applications (Chapter 7) that combines a design mechanism analysis through autoethnography with a user perspective analysis using an online survey. The findings identify the presence of 14 distinct deceptive design patterns embedded in VR applications' privacy communication and decision-making mechanisms, such as settings menus and permission prompts. The online survey further shows that users feel manipulated even though they lack knowledge of deceptive design or cannot pinpoint deceptive design elements. They perceive such designs as industry norms and therefore feel powerless to self-protection.

- In Chapter 8, we discuss the implications of this thesis for future researchers on extending theoretical and practical approaches to address deceptive design, advance ethical design strategies, and develop effective educational interventions; for designers

to proactively apply actionable guidelines to reduce deceptive practices in their design while creating ethical and user-centered immersive experiences that respect user privacy and autonomy; for future regulation to expand and strengthen regulatory frameworks to better govern user privacy and autonomy, and enforce ethical industry design standards to address the unique risks from immersive technologies.

This thesis provides the first research-driven investigation into the manifestation of deceptive design in commercially available immersive environments. We identified specific deceptive strategies employed in existing VR applications and their impacts on user perception, behavior, and privacy. Drawing from literature, real-world VR design analyses, and user perspectives insights, the findings from this thesis provide actionable implications for future researchers, immersive technology design, development, and regulation. Through these contributions, we advanced the understanding of deceptive design in immersive environments, delivered actionable guidelines for the development of practical tools for ethical design and user education, and established the foundation for stronger regulatory frameworks to protect users in immersive environments. This thesis contributes to the ongoing effort to create immersive experiences that prioritize user well-being, ethical standards, and transparency in the increasingly complex digital environments. It emphasizes that a collaborative and interdisciplinary approach is necessary for protecting user autonomy and privacy in the evolving immersive technologies.

1.4 Related Publications

Significant portions of the research in this thesis have appeared or have been submitted to peer-reviewed academic venues. Hilda Hadan is the primary author of these publications and is credited with generating research ideas, designing study methods and instruments, developing research ethics protocol, leading investigations, recruiting and remunerating participants, collecting and analyzing data, and disseminating findings. Co-authors include graduate student researchers (Lydia Choong, Derrick M. Wang, Reza Hadi Mogavi, Sabrina Alicia Sgandurra, Michaela Valiquette) and graduate and undergraduate student research

assistants, who helped with data analysis. A large portion of the text from published work in this thesis is taken directly from the publications.

The peer-reviewed full paper publications are:

- Chapter 3 (Objective 1): **Hadan, H.**, Choong, L., Zhang-Kennedy, L., & Nacke, L. E. (2024). Deceived by Immersion: A Systematic Analysis of Deceptive Design in Extended Reality. *ACM Computing Surveys,* 56(10), 1-25.

- Chapter 4 (Objective 4): **Hadan, H.**, Wang, D. M., Nacke, L. E., & Zhang-Kennedy, L. (2024, May). Privacy in immersive extended reality: Exploring user perceptions, concerns, and coping strategies. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (pp. 1-24).

- Chapter 6 (Objective 3): **Hadan, H.**, Sgandurra, S. A., Zhang-Kennedy, L., & Nacke, L. E. (2024). From Motivating to Manipulative: The Use of Deceptive Design in a Game's Free-to-Play Transition. *Proceedings of the ACM on Human-Computer Interaction, 8*(CHI PLAY), 1-31.

The peer-reviewed extended abstract publications is:

- Chapter 5 (Objective 2): **Hadan, H.**, Zhang-Kennedy, L., & Nacke, L. E. (2024, October). 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* (pp. 109-123).

The accepted manuscript awaiting for production is:

- Chapter 7 (Objective 3): **Hadan, H.**, Valiquette, M., Nacke, L. E., & Zhang-Kennedy, L. (2025, October). Immersive Invaders: Privacy Threats from Deceptive Design in Virtual Reality Games and Applications. Accepted and will be published at the *ACM SIGCHI Conference on Computer-Supported Cooperative Work & Social Computing (CSCW) 2025* (pp. 1-30).

1.5 Thesis Outline

This thesis is organized as follows:

- In Chapter 2, we give a background and previous studies on the deceptive deign patterns, the underlying factors that make deceptive design effective for users, the presence of deceptive patterns in non-VR environments and their impacts on VR users. The knowledge from these previous studies contributed to the foundation of my thesis.
- In Chapter 3, we present a completed systematic literature review that provides the current state-of-the-art deceptive design research in VR.
- Chapter 4 presents an empirical online survey research into users' perceptions and privacy concerns on immersive technology's data practices, as VR data is a main source of user inferences and targeted and personalized deceptive strategies.
- To gain a first-hand understanding of the manifestation of deceptive design patterns and their impacts on users, the research presented in Chapter 5 developed a *Deceptive Design Assessment Guide* based on the foundational literature in the field of deceptive design and insights from our Chapter 3. This *Assessment Guide* served as a standardized and consistent exploration and comparison tool in the subsequent studies.
- With this *Assessment Guide*, the research presented in Chapter 6 and Chapter 7 studied and compared the manifestation of deceptive design patterns in computer and VR applications and their impacts on users.
- In Chapter 8, we discuss our findings and conclude how deceptive design patterns manifest in VR, influenced and amplified by VR-specific properties, and how these manifestations influence user experience and manipulate user interactions in ways that differ from non-VR environments.

Chapter 2

Background

2.1 Deceptive Design and Its Theoretical Evolution

2.1.1 From Patterns, Antipatterns, to Deceptive Design

The concept of *patterns*, introduced in architecture and urban design, describes reusable solutions to recurring problems [7]. This idea was later applied to software design, where *design patterns* were defined as providing elegant and reusable solutions for common challenges in object-oriented software design [78]. The widespread use of software design patterns has led to the emergence of *antipatterns* as common but flawed solutions that can produce negative consequences [26]. While patterns represent best practices, antipatterns contribute to cautionary examples of pitfalls to avoid [26].

Unlike antipatterns, deceptive design consists of patterns that manipulate users, often impairing their ability to make informed decisions [163, 89, 62]. For example, websites use disguised ads to blur the line between genuine content and advertising, boosting revenue and click-through rates for website owners and advertisers. [24, 162]. Originally defined as tricks that websites and mobile apps use to push users into unintended actions, such as purchases or sign-ups [24], the concept has evolved to include any design practice that distorts user

choice, regardless of intent, as in recent deceptive design scholarship, researchers have concluded that user manipulation may not always be intentional [88, 25, 62].

Deceptive design is present in various digital platforms, such as social media [170, 171], websites [25, 192, 196, 82], mobile apps [52, 96], games [103, 129, 257], and 3D immersive environments [91, 100, 133]. Early work has described deceptive design using different terms such as "coercive," "manipulative", "misleading," "steering," "trickery," and "subvert user intent" [163, 24, 87, 22]. In 2021, Mathur et al. [163]'s literature review synthesized six attributes of deceptive design that manipulate users through interface design (e.g., visual and aesthetics) and user experience (e.g., user perceptions) [25, 87, 181, 287] (see Table 2.2).

The taxonomy of deceptive design is large and growing. Early classifications identified categories based on large-scale analyses of websites and real-world examples [162, 25]. These were later extended to include broader taxonomies, exploitative strategies, and patterns observed in social networking services and 3D environments [91, 170, 171]. Building upon these early taxonomies, Gray et al. [89] recently developed a domain-agnostic ontology categorizing deceptive design into high-, meso-, and low-level patterns for easier access and adaptation of existing knowledge (see Table 2.1). All these studies contributed to the foundation of our *Deceptive Design Assessment Guide* (see Chapter 5).

2.1.2 Decision-Making and Choice Architecture

Deceptive Designs exploit both internal cognitive biases and external influences that shape human decision-making [233, 276]. Due to *bounded rationality*, people have limited capacity to process information and make fully rational choices [233]. People's decision-making is further shaped by subjective perceptions of potential gains and losses, and often tends to be *loss-averse* [276]. Self-control challenges, such as susceptibility to *temptation* and *mindlessness*, also play a role, as does *social influence* from peers, communities, and broader societal norms [253]. Deceptive design exploits these weaknesses through modifying the choice architecture—the context and way in which choices are structured and presented—to influence people's decision-making [163, 149, 253] (see Table 2.2).

High-Level Pattern	Meso-Level Pattern	**Description**
Sneaking	Bait and Switch	Presents a seemingly desirable choice that leads to an unexpected, less desirable outcome.
	Hiding Information	Withholds or delays key details, preventing users from making fully informed decisions at the moment of choice.
	De(contextualizing Cues)	Presents information in a misleading context, making it hard for users to locate or interpret relevant details needed for informed decisions.
Obstruction	Roach Motel	Makes it easy for users to enter a situation but difficult or frustrating to exit or reverse the action.
	Creating Barriers	Complicates or obstructs key tasks, discouraging users from taking desired or intended actions.
	Adding Steps	Introduces unnecessary interactions that prolong a task, making it more tedious than technically required.
Interface Interference	Manipulating Choice Architecture	Structures options to steer users toward a specific outcome, rather than supporting their intended choice.
	Bad Defaults	Sets harmful or unfavorable options as the default, requiring users to actively opt out to protect their interests.
	Emotional or Sensory Manipulation	Alters design elements to evoke emotions or sensory reactions that steer users toward a specific action.
	Trick Questions	Uses confusing or misleading wording to influence user choices.
	Choice Overload	Presents excessive options, making comparison difficult and informed decision-making less likely.
	Hidden Information	Conceals or misframes relevant information, limiting informed choice.
	Language Inaccessibility	Uses overly complex or unfamiliar language to reduce user understanding.
	Feedforward Ambiguity	Obscures the link between user action and outcome, leading to unexpected results.
Forced Action	Nagging	Repeatedly interrupts or pressures users, pushing them toward unwanted actions.
	Forced Continuity	Makes subscriptions difficult to cancel or ends up charging users without clear consent.
	Forced Registration	Tricks users into thinking account creation is required to proceed.
	Forced Communication or Disclosure	Coaxes users into sharing unnecessary personal information.
	Gamification	Coerces repeated use of a service by tying features to reward-based interactions.
	Attention Capture	Misleads users about availability or demand to prompt rushed decisions.
Social Engineering	Scarcity and Popularity Claims	Exaggerates demand or limited availability to pressure quick purchases.
	Social Proof	Misrepresents others' behaviors to influence user decisions through perceived norms.
	Urgency	Creates false time pressure to accelerate decision-making.
	Personalization	Uses personal data to manipulate the experience while concealing alternative options.

Table 2.1: The high-level and Meso-level deceptive patterns synthesized by Gray et al. [89], which served as the foundation of our *Assessment Guide* in Chapter 5.

Choice Architecture	Attribute	Description
Modifying the decision space	Asymmetric	*Unequal burdens on choice available to the user*
	Restrictive	*Eliminate certain choices that should be available to users*
	Disparate Treatment	*Disadvantage and treat one group of users differently from another*
	Covert	*Hiding the influence mechanism from user*
Manipulation the information flow	Deceptive	*Induce false beliefs in users either through affirmative misstatements, misleading statements, or omissions*
	Information Hiding	*Obscure or delay the presentation of the necessary information to users*

Table 2.2: Deceptive design attributes grouped by their influence on the user's choice architecture, by Mathur et al. [163].

Literature highlights two challenges in counteracting deceptive design [175]. First, the subjective nature of choice architecture, originating from people's differences in preferences, values, and experiences, makes it challenging to define a universally "unacceptable" design [174, 249]. Second, efforts to counteract deceptive design also need to account for its potential benefits, as it can also guide users toward better decisions [247]. Addressing these challenges requires careful attention to the context-dependent and interpretive nature of choice architecture, where deceptive design occurs [175]. These complexities indicate the importance of engaging users directly in the understanding of how they interpret and respond to deceptive design in specific contexts, which inspired our methodologies in Chapter 6 and Chapter 7.

2.1.3 Nudge, Sludge, Persuasion, and Coercion

A positive use of choice architecture is *nudge*, which guides people toward certain decisions, to promote individual and societal well-being, while preserving their freedom to choose [253]. For example, smartphone GPS systems suggest optimal routes but allow users to ignore or modify the suggestions [252]. In contrast, *sludge* refers to harmful or manipulative nudges that serve the nudger's interests by creating friction (e.g., excessive paperwork, lengthy processes) that discourages beneficial behavior [252]. For instance, companies may offer rebates but require inconvenient steps like mailing in receipts to reduce claim rates [252].

Deceptive design can be seen as an extension of sludge but with more diverse tactics such as hidden defaults, forced continuity, fake urgency, and other strategies to influence user behavior [24]. In both sludge and deceptive design, users technically retain choice, but the way options are presented is skewed to serve others' goals.

These concepts are closely related to the concept of *persuasion* and *coercion*, all of which involve influencing people's attitudes or behaviors [71]. Early literature often defines *coercion* as associated with force, while *deception* relies on false or misleading information [25, 71]. In contrast, *persuasion* typically involves voluntary behavioral change based on accurate and balanced information [71]. Although these concepts originate from different research fields, they share a common focus on how design can influence user behavior through cognitive biases [2]. In recent literature, the distinctions between them have become increasingly blurred. For instance, some deceptive design taxonomies now include the forced actions category, which aligns more closely with the definition of coercion (e.g., [89, 29, 149] and Table 2.1). Literature has acknowledged that many deceptive design strategies resemble persuasive strategies [87] and view deceptive design as a type of unethical use of nudging [2]. In this thesis, we do not aim to draw strict distinctions between these concepts. Rather, we focus on the overarching impact of deceptive design that compromises user autonomy, manipulates their decision-making as if they were "puppets on a string", inflicts user harms, and are likely to lead to regret [248, 25, 2].

2.1.4 Harms from Deceptive Design

Research shows that deceptive patterns are often combined to amplify their effects. For instance, comparison prevention tactics may be combined with fake social proof and pre-selection to exploit authority biases and deceive users toward default choices [24]. As the application of deceptive design expands in various fields, research has documented its possible consequences on users and society. Deceptive design can erode user *autonomy* [163, 250], lead to unintended *financial loss* (e.g., accidental purchases [24, 287]), and interfere with informed decision-making, such as limiting access to price comparison [24]. Users can also experience *privacy invasion* from bad defaults, hard-to-access privacy settings, or fear-inducing prompts

that steer users away from privacy-preserving options [163, 24, 256]. In addition, deceptive designs can impose *cognitive burdens* by forcing users to invest unnecessary time and effort to complete or cancel actions, as seen in hard-to-cancel subscriptions or opaque cookie consent interfaces [239, 25, 97].

Beyond individual harm, deceptive design also poses broader societal risks. Companies often leverage users' cognitive biases for profit, using techniques like A/B testing to fine-tune manipulative strategies [109, 28, 181]. This can harm fair market competition, raise users' service switching costs, and guide them toward less optimal choices[47]. Over time, repeated exposure to such tactics will erode public trust, even for companies that maintain ethical practices [163, 149]. These harms become even more concerning in immersive environments, where deeper engagement, increased realism, and constant data collection have the potential to amplify the effectiveness and subtlety of deceptive strategies [100, 133].

2.2 Virtual Reality and Its Properties

Early research defined VR as an environment in which the user is fully immersed in a synthetic world that may or may not replicate the properties of the real world [172]. It distinguished VR from augmented reality (AR), which overlays simulated cues onto the natural environment, and mixed reality (MR), which allows users to experience physical and virtual elements simultaneously [172, 284]. Over time, definitions of these technologies have evolved significantly, with some researchers describing MR as a combination of AR and VR, or as a more advanced form, or even a synonym of AR [241]. Others argue that all technologically mediated experiences are forms of MR, since current systems can only influence people's exteroceptive senses (e.g., sight), not interoceptive senses (e.g., proprioception) that govern their internal bodily state [234]. Moreover, many commercially available VR headsets, such as Meta Quest[1] and Apple Vision Pro[2], also support AR and MR functionalities.

[1]Meta Quest Headset. https://www.meta.com/quest/
[2]Apple Vision Pro. https://www.apple.com/apple-vision-pro/

In this thesis, we do not seek to establish a definitive boundary between VR and other virtual technologies. Instead, we adopt a conventional understanding of "pure" VR applications as those that are fully immersive, do not incorporate real-world knowledge but replace it with a simulated experience, and exclude elements of the physical environment [234, 161].

In this section, we summarize the properties of head-mounted display (HMD) VR systems as discussed in the literature (e.g., [234, 259, 237, 112]), following Skarbez et al. [234]'s recently revised framework that built upon the widely adopted reality-virtuality continuum [237] with consideration of contemporary MR contexts. We extend this framework by introducing an additional dimension concerning device data from a privacy perspective, as this expanded set of dimensions closely aligns with the scope of our research. In Chapter 3, we further discuss how these properties may possibly interact with deceptive design in virtual environments through a systematic literature review.

The Extent of World Knowledge refers to the degree to which a VR system is aware of, models, and integrates the factual or semantic knowledge of the physical world, in terms of object location ("where") and identification ("what") within the virtual environment [172]. VR typically blocks out the physical environment ("reality") and replaces it with a fully virtual one [161, 160]. These systems often employ *unbounded displays*, where virtual content can appear anywhere within the user's field of view [133]. Since the rendered virtual environments possess little or no knowledge of the physical environment [234, 259], VR produces *physical-virtual barriers* that create asymmetries in users' awareness or perception of their real-world surroundings. These barriers can arise between the physical and virtual environments, between the user and bystanders, or even among multiple users sharing the same virtual environment [284, 133].

Immersion refers to the technological capability of a system to deliver a surrounding, convincing, and responsive sensory environment to the user [237, 235]. This property alone can support the *place illusion* of *presence* by creating a compelling sensation for users to feel physically present in a real place, even when the environment is entirely virtual [236, 234]. VR systems are generally considered to have high immersion [234], meaning they allow for a wide range of realistic and meaningful *sensorimotor* and *effectively* valid actions from users

and, in turn, produce perceptual and environmental feedback consistent with the users' expectations [234, 237]. Some virtual environments also include a *virtual self-representation* of the user, which functions both as part of the virtual environment, or virtual body, and as an embodiment of the perceiving subject [237]. In these cases, user perception is typically centered on the position of the virtual body, for example, viewing the virtual world from the egocentric (first-person) perspective of the virtual body's eyes and head, rather than from an exocentric (third-person) viewpoint, where the user observes their avatar from an external position [59].

Coherence refers to how consistently VR conveys its intended purpose or scenario to the user [234], which is essential for supporting the *plausibility illusion* of presence, the sense that the depicted experience is actually occurring, despite users knowing it is not real [112]. In VR, coherence manifests internally both between virtual objects and between virtual objects with the user [234]. For example, virtual objects may be dynamically or statically anchored to a user's physical body, and their spatial placement (e.g., position and distance) can support real-time user interactions [133]. The coherence in VR is further reinforced by high-fidelity multi-sensory stimuli, including visual, motion, audio, and haptic feedback, which align physical and virtual elements and can be nearly indistinguishable from real-world experiences [234, 32, 176]. For example, *motion* may be achieved through the manipulation of 3D models using motion capture technologies [32, 176]; *audio* can be supported by simulating room acoustics [224] and modeling sound propagation in multi-room environments [148]; and *haptic* feedback can take the form of tangible interfaces [269], output that allows users to feel virtual objects with their hands [222], or be passive that enhances the realism of immersive virtual environments [12]. These multimodal interactions and sensory stimuli can often carry symbolic or emotional meaning that further enhances immersion [117]. For example, turning the user's head produces corresponding updates in both the visual display and auditory cues so that sound direction remains consistent with the user's head orientation [237].

Device Sensing is at the core of all virtual technologies. The rendering of virtual content depends on a wide range of bodily and environmental sensors, including optical cameras, depth sensors, eye trackers, and motion trackers, which collect detailed data

about users and their surrounding environments [3, 58, 197]. While some of these sensor types are also present in non-immersive systems such as smartphones and smart home devices [105, 200], immersive technologies' sensors enable a more granular and multimodal understanding of *user behavior* by capturing 3D representations of the user, such as body dimensions, posture, movement, and gaze [3, 58, 284], as well as mapping their *physical surroundings* through interpretation of users' spatial layouts, object positioning, and user-environment interactions [58, 53]. This data can further facilitate inferences about users' behavioral patterns, preferences, habits, cognitive states, emotions, and personality traits [206, 173, 169], which can be exploited to deliver personalized content, such as targeted advertisements or manipulations adapted to user vulnerabilities [133, 100].

Given the complexities and inconsistencies in how virtual technologies are categorized and the varying functionalities of commercial devices, in our VR investigations in Chapter 6 and Chapter 7, following Speicher et al.'s recommendation, we distinguished our research based on application contexts rather than the underlying technologies [241]. We focused on VR applications that have (1) real-time rendering that responds to changes in users' head position, (2) immersive virtual spaces, either concrete or abstract 3D environments, and (3) real interactions that allow users to directly manipulate virtual objects [244]. Our decision to focus on HMD-based VR in this research is based on its status as the most prevalent form of immersive technology available to consumers, with increasing adoption in gaming, education, and social platforms [9, 10]. The fully immersive nature of VR allows us to concentrate on the interplay between deceptive design and the unique properties of virtual environments, without the added complexity of users' physical reality, like in other immersive technologies, which may further complicate the manifestation and user perception of deceptive design. We acknowledge that although current technologies cannot create a truly "perfect" VR, one that fully overrides people's both exteroceptive (e.g., sight, hearing) and interoceptive (e.g., proprioception, hunger) senses, virtual experiences enriched with sophisticated multimodal sensory stimuli can still feel convincing and even induce physical reactions [234, 119].

2.3 Established Deceptive Design Research Methodologies

2.3.1 Design, Regulatory, and Literature Perspectives

A common approach to studying deceptive design is content analysis, where researchers evaluate interface elements to determine the presence of deceptive patterns (e.g., [87, 22, 188, 97]). Another similar method is the cognitive walkthrough [144], which involves capturing detailed screenshots of user journeys and conducting expert evaluations at each step (e.g., [25, 170]). Many of these studies draw on existing taxonomies to identify deceptive designs across various contexts, including social media (e.g., [170, 171]), mobile apps (e.g., [52, 96]), games (e.g., [103, 102]), and consent banners (e.g., [97, 96]). In some studies, identifying deceptive elements is the central focus (e.g., [87, 162, 22]), while in others, it contributes to the groundwork for designing user-centric experiments (e.g., [52, 103, 129]). These studies often use illustrative examples to demonstrate the characteristics, impact, and effectiveness of deceptive design.

Beyond empirical interface analyses, several studies have explored deceptive design through literature reviews (e.g., [163, 287, 89, 88]) and analyses of legal texts and privacy policies (e.g., [128, 97, 6]). These studies often aim to synthesize existing taxonomies (e.g., [89, 163, 287]), trace the historical evolution of deceptive design practices (e.g., [189]), and examine how legal frameworks and policy language address or fail to address deceptive design practices (e.g., [97, 128]). Some studies also investigate expert perspectives through workshops and interviews with designers, expert researchers, and policymakers (e.g., [133, 289]). While these approaches understand the deceptive design problem from the regulatory and professional design perspectives, they provide limited insight into how such designs affect end-users' experience from the users' point of view [88].

2.3.2 User Experience Perspectives

Given the subjective nature of choice architecture (see Section 2.1.2), literature has advocated for user-centric approaches to studying deceptive design, especially in cases where practices may not be overtly unethical or manipulative [83, 88, 204]. The impact of deceptive design often hinges on individual factors such as digital literacy, frequency of exposure, perceived trustworthiness, and tolerance for frustration [287, 52, 149, 151]. Early research used online surveys and social media analyses to explore user behaviors, attitudes, and experiences (e.g., [37, 52, 76, 129, 19]). Experimental methods, including control and treatment group designs, have also been employed to assess how specific design elements influences user behavior (e.g., [188, 90, 271, 152, 99]). However, non-expert participants frequently struggle to identify deceptive patterns [52]. As a result, many studies have combined user experiments with experts' content analysis and cognitive walkthrough in identifying deceptive patterns (see Section 2.3.1). Although these methods are suitable for task-oriented evaluation with logical user steps and action execution [144], they are less effective for highly interactive or exploratory systems like VR [116, p. 211].

Autoethnography, a method involving researchers' first-person engagement and critical reflection, has gained traction for studying deceptive design in immersive environments (e.g., [106, 11]). This method situates researchers as both the "protagonist" and observer and enables a first-person engagement and understanding of how deceptive design manifests and operates in context [211, 185, 16]. Given the possibly persistent and subtle nature of deceptive design in immersive environments [133, 100], autoethnography encourages critical self-reflection by requiring researchers to question their interpretations and challenge their assumptions [211, 5]. This combination of subjective experience and introspective analytical reflection makes autoethnography well-suited for analyzing deceptive design in immersive contexts.

Drawing from established methodologies in deceptive design research, this thesis begins with a systematic review of the literature's perspective on deceptive practices in immersive technologies (Chapter 3). It then presents a user-centered study that explores people's understanding of unique data practices in immersive systems, particularly those that enable

preference inferences and targeted manipulation (Chapter 4). This is followed by a synthesis of existing deceptive pattern taxonomies (Chapter 5), which lays the groundwork for two mixed-method studies (Chapter 6 and Chapter 7) that combine design analysis, user opinion analysis on social media, and an introspective autoethnographic investigation. Together, this thesis identifies the presence of deceptive design and evaluates its impact from users' perspectives across traditional and immersive digital environments.

Chapter 3

Synthesizing State-of-the-Art in Deceptive Design Research in Immersive Environments

---

Suggested Citation:

Hadan, H., Choong, L., Zhang-Kennedy, L., & Nacke, L. E. (2024). Deceived by immersion: A systematic analysis of deceptive design in extended reality. *ACM Computing Surveys, 56*(10), 1-25. https://doi.org/10.1145/3659945

3.1 Introduction

In this chapter, we address Objective 1 by conducting a systematic literature review [100] to understand the current state of research on deceptive design in immersive environments.

3.1.1 Motivation and Gaps in Existing Literature

The literature has highlighted VR's potential to enhance gaming and socialization [106, 260], arts and design [227], e-commerce advertisements [169], and education [166]. Researchers have also recently begun examining deceptive design in VR and proposing corresponding solutions (e.g., [134, 169]). Deceptive design relies on interface design elements (e.g., a countdown timer) [25, 87]. Research indicates that the multi-sensory feedback [27, 169] of immersive technologies has the potential to modify users' choice architecture [228]. This raises the question of whether new deceptive designs, beyond those relying on traditional 2D interface elements, might emerge in immersive environments and pose new types of risks to users. Although extensive research on deceptive design has already elucidated the harms in non-immersive environments [163], its use in immersive technology is still not well understood. In addition, a high-level overview of deceptive design research in this area is also lacking. Specifically, there is no systematic examination of which immersive technology's properties contribute to deceptive design, how these properties (see Section 2.2) and deceptive design tactics interact, and what new harms deceptive strategies in immersive environments may introduce to users. Reviewing current knowledge on this area is an urgent necessity for providing a guideline for future research into this problem.

3.1.2 Chapter Research Goal

To provide analytical clarity, seed discussions, and derive important insights for researching and designing solutions for VR deceptive design, we conducted a *systematic literature review* using *thematic synthesis* to map and synthesize past research on deceptive design in VR. Since VR and other immersive technologies share similar properties, sensors, and data collection capabilities, and given the evolving definition of immersive technologies [284, 241], the distinction between VR and other immersive technologies has remained ambiguous in early deceptive design research (e.g., [141, 20, 227]). As a result, rather than isolating VR systems from other immersive technologies, we synthesized deceptive design patterns that rely on immersive properties, many of which may operate across all immersive technologies.

Specifically, our literature review explored three chapter research questions (RQ3.1-3.3):

RQ3.1) How can immersive technology amplify the effects of deceptive design?

RQ3.2) What deceptive design strategies can be present in immersive technology?

RQ3.3) what risks can deceptive design in immersive technology pose to users?

3.1.3 Chapter Contributions

In this chapter, we present our methodology, summarize core findings, and discuss their influence on this direction of this thesis research. Our systematic literature review makes the following **contributions**: *First*, we synthesize literature's discussions on how the unique properties of immersive technologies can be exploited for deceptive design, with literature's examples that illustrate how manipulative tactics may differ from those used on other platforms. *Second*, we present a categorization of deceptive design strategies that can be used in immersive technologies through our thematic analysis. *Third*, we analyze the interplay between deceptive design and existing risks from immersive technologies, and how they mutually exacerbate potential user harms. Finally and *fourth*, we synthesize prevention techniques from the research studies that can serve as actionable recommendations for the design, development, and regulation, and user education in mitigating deceptive design risks.

Through this work, we propose future research directions for studying deceptive design in immersive environments: 1) focusing on commercially available technologies and applications, 2) contrasting design mechanisms with user perspectives, and 3) gaining a better understanding of immersive technologies' data practices, as these data can be exploited for targeted deceptive design. These directions shaped the overall research trajectory of this thesis.

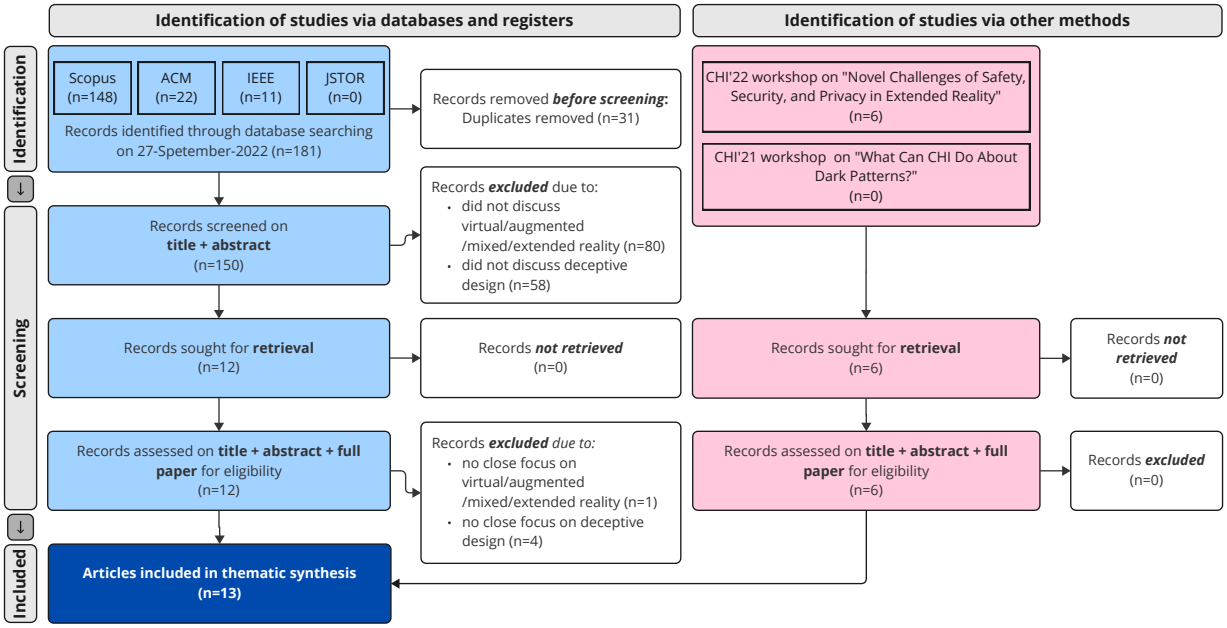


Figure 3.1: This PRISMA flow diagram [201] presents all the phases of our systematic analysis of the literature, from the identification of articles to the final articles we included.

3.2 Methodology

Our research methodology involves a systematic literature review [201] and a thematic synthesis [261]. To ensure a structured and rigorous approach to database searching, screening, and data extraction, we followed the PRISMA guidelines [201], which provides clear protocols for conducting literature reviews and meta-analyses.

3.2.1 Literature Search and Screening

We selected four bibliographic databases: Scopus[1], the ACM Guide to Computing Literature (ACM)[2], IEEE Xplore (IEEE)[3], and JSTOR[4] to ensure disciplinary diversity and balanced

[1] https://www.scopus.com/
[2] https://libraries.acm.org/digital-library/acm-guide-to-computing-literature
[3] https://ieeexplore.ieee.org/Xplore
[4] https://www.jstor.org/

scope of our research. The ACM Guide and IEEE Xplore focus on technology and engineering publications, Scopus covers multiple disciplines, and JSTOR provides access to humanities and social sciences publications.

After refining search terms with keywords related to deceptive design and immersive technology (as mentioned in Chapter 2), we finalized our query as: `(‘‘Virtual Reality’’ OR ‘‘Augmented Reality’’ OR ‘‘Mixed Reality’’ OR ‘‘Extended Reality’’) AND (‘‘dark patterns’’ OR ‘‘deceptive design’’ OR ‘‘deceive’’ OR ‘‘decept*’’ OR ‘‘manipulat*’’ OR ‘abus*’’)`. The use of `‘‘*’’` allowed us to include all derivations of the original words in our research. We also limited our results to English "Research Article", "Extended Abstract", "Short Paper", "Book Chapter", "Conference Paper", "Book Review", or "Journal Paper." Table 3.1 shows the customized syntax for each database. Beyond publications from these databases, we also included 6 records from the CHI workshops: *Novel Challenges of Safety, Security, and Privacy in Extended Reality* [93] in 2022 and *What Can CHI Do About Dark Patterns* [150] in 2021.

Database	**Search Query**
The ACM Guide to Computing Literature*	Abstract: [(“dark patterns” OR “dark pattern” OR “deceive” OR “deceptive” OR “manipulative” OR “abusive”) AND (“extended reality” OR “virtual reality” OR “augmented reality” OR “mixed reality”)]
Scopus	[ABS** (“dark pattern”) OR ABS (“dark patterns”) OR ABS (“deceive”) OR ABS (“deceptive”) OR ABS (“manipulative”) OR ABS (“abusive”)] AND [ABS (“extended reality”) OR ABS(“virtual reality”) OR ABS (“augmented reality”) OR ABS (“mixed reality”)] AND (LIMIT-TO (DOCTYPE , “cp”) OR LIMIT-TO (DOCTYPE , “ar”) OR LIMIT-TO (DOCTYPE , “re”) OR LIMIT-TO (DOCTYPE , “ch”)] AND (LIMIT-TO (LANGUAGE , “English”)]
IEEE Xplore*	([(“Abstract”:“dark pattern”) OR (“Abstract”:“dark patterns”) OR (“Abstract”:“deceive”) OR (“Abstract”:“deceptive”) OR (“Abstract”:“manipulative”) OR (“Abstract”:“abusive”)] AND [(“Abstract”:“extended reality”) OR (“Abstract”:“virtual reality”) OR (“Abstract”:“augmented reality”) OR (“Abstract”:“mixed reality”)]
JSTOR*	[(“dark pattern”) OR (“dark patterns”) OR (“deceive”) OR (“deceptive”) OR (“manipulative”) OR (“abusive”)] AND [(“extended reality”) OR (“virtual reality”) OR (“augmented reality”) OR (“mixed reality”)] AND la:(eng OR en)

Note. *To ensure the consistency of research queries across the four databases, the corresponding filters for research article, extended abstract, short paper, book chapter, conference paper, book review, or journal paper, and English language were applied through interface features.
**“ABS” is the search syntax for abstract search in Scopus library.

Table 3.1: The final search queries in the syntax of each database. We kept the filters for all databases as consistent as possible. The search was conducted twice over each database in September 23 and 27, 2022 to ensure outcome consistency.

Our research yielded 187 initial publications. After manually removing 31 duplicates

based on identical titles and DOIs, we imported the remaining 156 unique records into Covidence[5] for abstract and full-text screening following PRISMA guidelines [201]. We excluded papers that were: (1) not about immersive technologies, (2) not about deceptive or user-manipulating design, or (3) not examining deceptive design specifically within immersive technologies. This process resulted in a final sample of 13 papers, which we analyzed using thematic synthesis [261].

3.2.2 Thematic Synthesis

We used thematic synthesis [261], a rigorous and systematic literature analysis approach derived from thematic analysis [39]. Our analysis involved four stages:

(1) Data extraction: we downloaded the PDFs of the 13 selected publications and extracted their textual content into separate text files using Adobe Acrobat PDF reader. These files were then uploaded to the Dovetail[6] platform for thematic synthesis.

(2) Line-by-line coding: two coders conducted independent line-by-line coding of each publication using an inductive approach [39]. During the first round of coding, the two coders independently coded the first 2 publications. A third coder resolved disagreements and facilitated consensus building. The remaining 11 publications were then coded by repeating this procedure.

(3) Developing descriptive themes: initial codes were discussed in weekly meetings, leading to a collaboratively refined codebook. After four weeks, we finalized a codebook with 114 codes. We grouped codes into descriptive themes that closely summarize the publications' contents.

(4) Generating analytical themes: through affinity mapping and iterative discussions, we derived eight analytical themes that address our research questions. Table 3.2 maps these final themes to each publication.

[5]Covidence - Better systematic review management. https://www.covidence.org/
[6]Dovetailapp.com

We present our results in the following sections.

3.3 Findings

Our results show that prior studies on deceptive design in immersive technology largely refer to strategies from websites, computer and mobile applications, but extend them by proposing new implementations unique to immersive environments. As in other contexts, early research distinguishes among "deception" from "nudging" and "persuasion": persuasion transparently influences users and enables informed decisions; deception misleads users into actions they might otherwise avoid; and nudging subtly shapes users' decision-making without altering preferences [169, 208]. It lets people *"go their own way"* [208, p. 530].

Early literature often emphasizes designer intent (i.e., [132, 45, 169]), as they primarily relied on definitions of deceptive design from previous research on websites, apps, and general UX or practitioner-focused contexts [25, 87]. Some studies have further explored benevolent applications of deceptive strategies in immersive technology, such as educational games teaching online safety, virtual sports training using deceptive character movements, and social simulations mimicking real-world negotiation tactics [263]. Although recent scholarship recognizes that deceptive designs can be implemented unintentionally [89, 25, 62], only two papers in our analysis briefly acknowledge this possibility [132, 208]. Therefore, our systematic literature review focused on examining deceptive design characteristics rather than designer intentions.

Our analysis identifies eight main themes and 15 subthemes, summarized in Table Table 3.2. For clarity, in the following paragraphs, descriptions directly taken from the literature are set in *italics* text with quotation marks.

Reference	Nijholt et al. [186]	Lebeck et al. [139]	Torstensson et al. [263]	Schlembach & Clewer [227]	Lee et al. [141]	Mhaidli & Schaub[169]	Ramirez et al. [208]	Krauß [132]	Cummings & Shore[45]	Buck & McDonnell[27]	Bonnail et al. [20]	Su et al. [245]	Franklin [73]
Year	2012	2018	2020	2021	2021	2021	2021	2022	2022	2022	2022	2022	2022
Effects of Immersive Technology Properties on Deceptive Design													
Enhanced user experience	✔	✔	-	✔	✔	✔	✔	✔	-	✔	✔	-	✔
Exacerbated user manipulation:													
the illusion of objectivity in XR experience	-	-	-	-	-	-	✔	-	-	-	-	-	-
obscuring reality, disguising risks	-	✔	-	-	-	-	-	-	-	✔	-	✔	-
data fuels privacy risks and manipulation	-	✔	-	-	✔	✔	-	-	✔	✔	-	-	-
undesired access, undesired data use	-	✔	-	-	-	-	-	-	✔	✔	-	-	✔
insecurity worsen user manipulation	-	-	-	-	✔	-	-	-	-	✔	-	✔	-
constant exposure to manipulation	-	-	-	-	-	✔	-	✔	✔	-	-	-	✔
Strategies of Deceptive Design in XR													
Psychological manipulation:													
false memory implantation	-	-	-	✔	-	-	-	-	-	-	✔	-	-
empathy-based manipulation	-	-	-	✔	-	✔	✔	-	-	-	-	-	-
hyperpersonalization	-	-	-	-	-	✔	-	-	-	✔	-	-	-
Reality distortion	-	✔	-	-	-	✔	✔	-	✔	-	✔	-	✔
User perception tricking:													
blurry boundary between virtual and reality	-	-	-	-	-	✔	-	-	-	✔	-	-	-
perception hacking	-	-	-	-	✔	-	-	-	-	-	-	✔	-
Risks that Deceptive Design in Immersive Enviornments Pose to Users													
Privacy and Security risks	-	✔	-	-	-	✔	-	-	✔	✔	✔	✔	-
Changes in views, beliefs, and buying decisions	-	-	-	✔	-	✔	✔	-	-	✔	✔	-	✔
Manipulation prevention techniques:													
prevent false memories and empathy manipulation	-	-	-	-	-	-	✔	-	-	-	✔	-	-
security and privacy recommendations	-	-	-	-	✔	✔	-	-	✔	✔	-	✔	-
call for research efforts	-	-	-	-	-	✔	-	-	-	✔	-	-	✔
improve user literacy	-	-	-	-	-	✔	-	-	✔	✔	-	-	

Table 3.2: Overview of all publications included in the systematic literature review, and the identified themes and sub-themes (✔) by RQ.

3.3.1 Themes 1 & 2: Properties of immersive technologies are capable of enhancing user experience while amplifying user manipulation

As discussed in Section 2.2, immersive technologies enhance user experience by creating interactive and engaging virtual environments. Such technology enables users to virtually *"sample"* products or experiences before purchasing [169] and supports personal and historical memory reminiscence through immersive documentaries [227, 20]. With stereoscopic visuals, audio, and haptic feedback, these technologies can foster a strong sense of presence [44, 208, 278]. Well-designed simulations can also achieve high *"context-realism"* (i.e., where rules, settings, and interactions convincingly mirror real-world experiences) and *"perspective-fidelity"* (i.e., accurately generating a user's viewpoints), making virtual experiences feel real [208]. Nine publications in our analysis discussed how these features can amplify user manipulation.

The illusion of objectivity in immersive experiences. Although immersive simulations aim to provide authentic first-person experiences, achieving absolute objectivity is inherently impossible due to factors such as *"semantic variance"* [228], *"structural intersectionality"* [43], and the designers' explicit intentions or subconscious biases [208].

Obscuring reality, disguising risks. Immersive technologies can conceal real-life environments with virtual ones, even including actual physical threats. In multi-user settings, environmental deception, such as disguising hazardous physical objects as harmless virtual items, can expose people to risks [27, 245, 139].

Data fuels privacy risks and manipulation. Immersive technologies extensively collect sensitive user data, including body and eye movements [27, 139, 141], gestures [141, 169], physical appearance [169, 27], behavioural patterns (e.g., gait, mannerisms) [169, 139, 27], and physical surroundings [139, 27, 169]. These data can enable precise user identification [173, 206], undermine user anonymity [45, 27], and facilitate targeted manipulation based on individual preferences and vulnerabilities [169].

Undesired access, undesired data use. Within multi-user environments, users can

interfere with others' experiences by altering their virtual appearances, placing unwanted virtual objects on their avatars, or gaining unauthorized access to sensitive content, which can lead to unintended privacy violations [73, 139, 27]. Uninvolved bystanders might also become unwilling participants in others' virtual experiences [139].

Insecurity worsens user manipulation and privacy concerns. Existing immersive technologies lack robust, web-standardized security mechanisms, leaving user data susceptible to breaches and exploitation [141, 245]. The potential for attacks to exploit insecure hardware or migrate existing web-based scams into immersive environments raised concerns about exposing users to manipulation and privacy threats [245, 27].

Constant exposure to manipulation. Future users may be exposed to continuous immersion, persistent tracking, and an ongoing stream of personalized advertising and manipulation through daily-use devices (e.g., smart lens [7]).

3.3.2 Themes 3-5: Psychological manipulation, Reality distortion, and User perception tricking

Ten publications in our analysis discussed deceptive design strategies that can potentially be used in immersive technologies, but none proposed a formal taxonomy.

False memory implantation. The immersive nature of the technology creates potential risks regarding memory manipulation [20, 227]. Human memory is prone to confusion of memory sources (known as *"source confusion"* [230]). Immersive simulations can induce false memories by deliberately altering recorded experiences [20]. For example, one study proposed a scenario involving modifying details in a virtual wedding experience, which can cause users to falsely remember and subsequently repurchase particular branded items [20].

Empathy-based manipulation. Immersive technology can create *"prosthetic memory"* of historical events and enhance users' empathy toward others' experiences [227]. Such

[7] Mojo smart contact lens that overlays virtual information onto the physical world. https://www.roadtovr.com/mojo-vision-smart-contact-lens-ar-hands-on/

empathetic engagement can lead to increased social responsibility, political alignment, or unintended emotional impact [137]. For instance, people with no direct ties to victims of traumatic events can experience vicarious trauma from viewing immersive media reconstructions [126]. Another example is the *6x9* VR game that simulates the psychological effects of solitary confinement. The immersive experiences sparked emotional and social responses and contributed to reform efforts in the US [227, 258].

Hyper-personalized user manipulation. Hyper-personalization refers to creating tailored manipulations specifically optimized for each user [279, 27, 132]. Immersive technology can use its extensive data collection to precisely understand people's preferences and vulnerabilities (see Section 3.3.1). Examples include generating idealized interaction partners based on physiological data [27] or emotionally manipulating decisions by depicting trusted people, such as friends, relatives, or even deceased loved ones [132, 169]. The extreme realism and tailored content make it difficult for users to resist, leading them toward behaviors they otherwise would not perform [169, 27].

Reality distortion. Several studies highlight how immersive technologies can distort user perception by concealing real-world sensations through daily-use devices (see Section 3.3.1). Examples include visually erasing city poverty or economic downturns [169], subtly inserting branded content into personal memories [20, 130], or concealing pedestrians and altering traffic conditions [139]. Such manipulations might also lead to users' psychological distress or addiction to a manufactured, idealized version of reality [169].

Tricking user perception. As immersive technology becomes increasingly realistic, deceptive design practices grow subtler and harder to detect [73, 227, 45]. For example, highly realistic visuals might fool viewers that other people's shirts include digital brand logos[169]. Software-replicated human voices and digital personas raise concerns about impersonation [27]. While current equipment might not fully achieve this realism, literature anticipates its possibility in the near future [169, 27].

Perception hacking manipulates user input. Immersive technologies employ visual, auditory, and haptic feedback, which can exploit users' perceptual limitations through *"perception hacking"* tactics [245, 141]. Example tactics include cursor-jacking, blind-spot

tracking, and auxiliary display abuse [141]. *"Cursor-jacking"* manipulates VR visual cues to differ from users' proprioceptive cues, guiding their movements and interactions toward unintended virtual objects [245, 141]. *"Blind-spot tracking"* users' limited gaze in 360-degree environments by placing advertising content strategically out-of-view to inflate user engagement [141]. Lastly, *"auxiliary display abuse"* involves covertly displaying advertisements on secondary screens when users are immersed in the headset, removing them immediately upon users' exit from the immersive mode [141].

3.3.3 Themes 6-7: Privacy and security risks, changes in users' views and beliefs, and buying decisions

We synthesized three risks that deceptive design in VR can pose to users.

Privacy and security risks. Creating immersive experiences requires extensive user data, and often mandates information sharing for certain functionality [20], which can lead to increased privacy risks. Users may be manipulated into sharing personal information through digital humans or avatars that impersonate their trusted friends and family [27, 169]. Privacy concerns may also *"shield"* deceptive designs, as people may not report issues due to privacy concerns [45]. Perception hacking can also mislead users into granting security permissions unintentionally, and allow malicious actors to access sensitive data or introduce further deceptive elements [27, 245].

Changes to users' views, beliefs, and behaviors. Empathy-based manipulations in immersive technology can impact users' sociopolitical beliefs and attitudes. For instance, *6x9* [92] VR simulation game evoked empathy for prisoners and influenced legal and political decisions [227]. Similarly, scenarios such as the removal of poverty indicators from virtual cityscapes can falsely promote impressions of economic prosperity, serving political or social agendas [169]. Combined with the users' mistaken assumptions about the objectivity of immersive experiences, these manipulations have the potential to alter people's values, beliefs, and decision-making processes [208]. Customizing avatars' appearances and personalities can also prompt users toward undesirable behaviors, such as gambling [27, 73]. Attitude, belief, thought, and perception manipulations can influence users' behavior and lead to

physical behaviors they would not normally exhibit [208, 139, 141, 27, 73]. Behaviors learned or reinforced virtually may also persist in real-world contexts (i.e., *"virtual spillover"*) and potentially result in lasting behavioral changes, especially after frequent or continuous exposure to immersive technology [73].

Immersive technology can also manipulate users' buying decisions through altered previews (e.g., brighter and more colourful) [169], hyper-personalized ads with ad spokesman avatars tailored to user preferences [169, 27], and purposefully modifying memory reconstructions with brand logos [20].

3.3.4 Theme 8: manipulation prevention techniques

Eight publications proposed solutions to protect users from deceptive design in immersive technology. Suggested approaches include employing intelligent software to detect and remove deceptive tactics [73, 166], ensuring transparency and securing user consent when modifying objective simulations [20], and shifting empathy-focused simulations to more neutral bystander perspectives to minimize empathy-based manipulation [208]. For multi-user scenarios, recommended policies include prohibiting unauthorized overlays of virtual content and enabling user-defined virtual object editing permissions [139].

In addition, five publications offered privacy and security recommendations, such as enhancing system reliability to ensure safe and free information sharing [45], giving users the power of control [27], having adequate security measures [245, 141], and implementing targeted laws to protect children [45] and prevent malicious use of data from immersive technologies [27, 45, 169]. Three publications emphasized educating users to raise awareness and resilience towards deceptive design [169] and data flow and privacy implications [45, 27].

Lastly, three studies called for further research on psychological manipulation and the effects of avatars [27], implications of daily use of immersive technologies [27, 73], and the boundary between ethical nudge and manipulative preference changes [169]. Developing effective educational interventions will also require academic and industrial research [169].

3.4 Discussion

Our analysis revealed that deceptive design strategies from websites and mobile applications have the potential to be adapted to immersive environments [163, 87, 89, 91]. Immersive technologies can manipulate people's emotions through artificial prosthetic memory that exploits empathy [227] and hyper-personalized avatars designed to evoke positive feelings [169]. These tactics represent variations of *"toying with emotion"* [87], *"social engineering"* [89], and *"attention grabber"* [91]. Similarly, digital humans mimicking people's trusted ones resemble a form of *"friend spam"* [287, 87], and the precise user profiling capability of immersive technologies constitutes a form of *"disguised data collection"* [91]. Perception hacking in these settings mirrors deceptive strategies such as *"sneaking"* or *"forced action"*, which manipulate users into engaging with unwanted virtual elements [89, 87]. Furthermore, we identified potentially deceptive design patterns unique to immersive environments, including false memory implantation, blind-spot tracking, reality distortion, realistic simulations, 360-degree displays, and the blending of virtual and real-world elements. Overall, literature discussions suggest that deceptive designs in immersive environments share attributes with web-based deceptive practices, such as *"covert,"* *"deceptive,"* and *"information hiding"* [162, 163]. However, in immersive environments, they operate through subtler mechanisms, and can leverage extensive data to exploit user vulnerabilities in novel and less detectable ways.

3.5 Limitations

First, due to the novelty of immersive technologies, our literature review is based on limited resources. Nonetheless, we consider this preliminary review crucial for identifying literature gaps, anticipating potential deceptive design risks before they impact users, and laying the groundwork for protective strategies. Second, we acknowledge the potential instability in literature database search results, as prior research has shown that searches conducted on different days can yield varying record counts (e.g., [217, 153]). While we refined our

search syntax and conducted multiple iterations to mitigate this issue, it may still affect our outcome. Third, our thematic analysis involved three coders with backgrounds in HCI, games, and privacy and cybersecurity research. While this diversity strengthened our analysis, we recognize the potential for subjective influences in shaping the themes. Finally, our research focuses on the early stages of deceptive design in immersive technologies and provides a foundational understanding for future studies. As the field evolves and more research emerges, a re-examination of the literature will be essential for gaining a more comprehensive perspective.

3.6 Literature Gaps and Research Direction

Among the publications reviewed in our study, there was a notable consensus that data collected through immersive technologies enables deceptive design [27, 139, 173]. The extensive tracking capabilities of these technologies allow for precise user profiling, which can be exploited for hyperpersonalization and manipulation [169, 27, 245]. To better understand and address these issues, future research needs to begin by examining what types of data immersive technologies can collect. The investigation by the XR Safety Initiative (XRSI) research lab's *1st XR data classification roundtable* conference [284] and Dick [53] in 2021 laid the groundwork for analyzing how VR and AR technologies handle user data. However, several questions remain unanswered: What data do immersive technologies collect about users? How well do users understand these data collection practices and their implications? Literature emphasized the need for user education on deceptive design in immersive technologies [169, 27, 45], and understanding users' mental model on this issue is vital in supporting effective risk communication [79]. Motivated by these questions, our study in Chapter 4 explores users' awareness and concerns about specific data collection practices in immersive technologies.

Our analysis suggests that deceptive design strategies observed in websites and mobile applications can potentially extend to immersive environments. The unique properties of immersive technologies may also lead to novel forms of deceptive design. However,

since immersive technologies are still in their early stages, much of the existing literature relies on hypothetical scenarios, expert predictions, and controlled in-lab experiments. These studies often take a broad view of immersive technologies without fully considering the distinct properties of different immersive devices (e.g., [100, 133, 245]). Thus, future research is needed to examine how deceptive design patterns manifest in commercially available immersive technologies, how they differ from their counterparts in computer and mobile environments, and how novel deceptive design could be implemented using the available functionality of existing immersive technologies. Understanding these aspects will support the development of targeted countermeasures before immersive devices become widespread and before deceptive practices cause significant harm. This need motivated our investigations into how deceptive practices appear in real-world VR applications, how they differ from those in traditional computing environments, and their impact on user privacy. We discuss these investigations in Chapter 6 and Chapter 7.

Our literature analysis identified studies that attempted to distinguish between *"nudging"* and *"manipulation"* based on user interests and freedom of choice (e.g., [169, 208]). Research has also suggested that users' perceptions of manipulation can identify borderline practices that may not be explicitly problematic or illegal [83, 88]. Building on these insights, future research on deceptive design needs to incorporate a comprehensive, user-centered analysis of interaction and perception. This may include exploring questions such as: How do users perceive deceptive design in immersive technologies? Which design practices are considered manipulative and should be avoided, and which are deemed acceptable? Without a clear understanding of users' perspectives, it will be difficult to develop effective and user-friendly countermeasures against deceptive design. This need motivated our study on end-users' awareness of deceptive design and its impact, and their expectations for more ethical alternatives, which we discuss in Chapter 6 and Chapter 7.

Chapter 4

Understanding User Awareness and Concerns About Data Practices in Immersive

---

Suggested Citation:

Hadan, H., Wang, D. M., Nacke, L. E., & Zhang-Kennedy, L. (2024, May). Privacy in immersive extended reality: Exploring user perceptions, concerns, and coping strategies. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (pp. 1-24). https://doi.org/10.1145/3613904.3642104

4.1 Introduction

In this chapter, we address Objective 4 by classifying the types of data processed by immersive technologies and examining users' awareness of these data practices, their coping strategies for managing data privacy concerns, and their expectations for data protection [105]. As demonstrated in Chapter 3, data collected by immersive technologies can

enable precise user profiling and be exploited for hyperpersonalization and manipulation [169, 27, 245]. Therefore, understanding users' awareness and concerns is essential for designing effective risk communication strategies [79], as a lack of awareness can lead to users' unclear privacy expectations and increased risks [1].

4.1.1 Motivation and Gaps in Existing Literature

Immersive technologies create virtual environments where users interact with digital objects by tracking their positions, movements, and surroundings through body sensors [27]. As these technologies reshape how people access digital information and engage with the real world, advertisers can leverage sensor data for user profiling [169]. The immersive nature of these technologies introduces unique risks that users may not recognize or be able to mitigate. For instance, behavioral pattern data collected through sensors, often considered non-sensitive, can be used as a unique identifier [173, 206]. Inferences drawn from sensor data [216] and the ambiguity of multi-user access control [159, 139] are emerging issues that raise crucial privacy concerns. These data can reveal personal details such as location, interests, and behaviors, and facilitate targeted advertising, privacy infringements, and manipulation (as discussed in Chapter 3). Existing research had explored privacy issues around AR browsers [165], social VR [159, 158, 200], VR learning [95], and behavioural biometrics [206, 173] from the developers' perspective. These investigations have employed various methodologies to explore the potential privacy risks posed by immersive technologies, such as analyzing system functionality [165, 200, 53], modeling internal and external threats [95], and reviewing privacy policies [53, 3]. However, little attention has been given to users' perspectives on these risks.

4.1.2 Chapter Research Goal

The goal of this research is to understand *users' awareness of data practices in immersive technologies, factors influencing their concerns.* For users who express data privacy concerns, we also study *their coping strategies and expectations for data protection.* Specifically, using

a scenario-based survey with 424 users, we answer the following chapter research questions (RQ4.1-4.4):

RQ4.1) How much are people aware of data collection through immersive technologies?

RQ4.2) To what extent are people concerned about their privacy and data collection in immersive technologies?

RQ4.3) What factors contribute to user privacy concerns in immersive technologies?

RQ4.4) What coping strategies (if any) do people use to mitigate their privacy concerns?

4.1.3 Chapter Contributions

In this chapter, we present our methodology and core findings of our online survey. The findings make the following **contributions**: *First*, we compiled a detailed list of data types that immersive technologies can collect, along with possible device operational states in which data collection may occur, based on existing literature (e.g., [197, 58, 3]), law reviews (e.g., [53, 114]), and technical reports (e.g., [259, 284]). *Second*, we found that users are largely unaware that the sensors in immersive technologies can capture highly granular data, including involuntary bodily signals linked to emotional responses, which may pose greater privacy risks than those collected by non-immersive devices. *Third*, our survey revealed how factors such as data type and data sensitivity influence users' awareness and concerns about data privacy. *Fourth*, we found that most users lack sophisticated strategies to manage or mitigate data collection in immersive environments, with many participants expressing a sense of resignation, believing their data had already been compromised through other non-immersive devices. These insights into user awareness, concerns, and expectations shaped our focus on privacy issues in the deceptive design analysis in Chapter 6 and informed our dedicated investigation in Chapter 7 into how deceptive design manifests in VR privacy communication and decision-making mechanisms.

4.2 Methodology

We conducted a scenario-based online survey with 464 Prolific[1] participants who had prior experience with immersive technologies, though device ownership was not required. Before recruitment, our study received Research Ethics Board approval (REB#44772) from the University of Waterloo. Each participant was presented with four randomly selected data collection scenarios from a pool of 18 pre-designed scenarios.

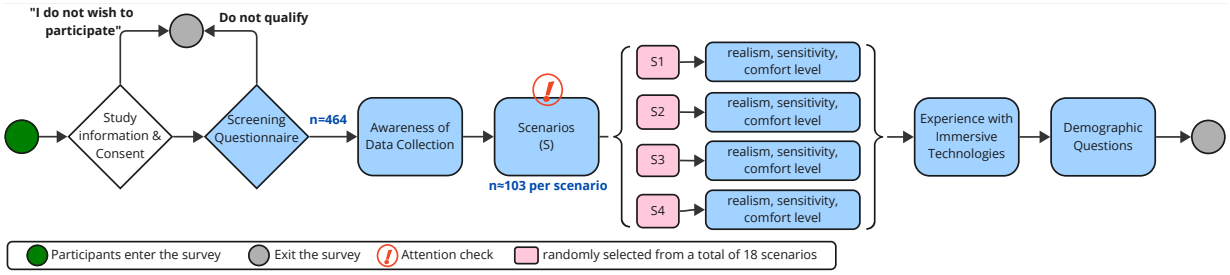


Figure 4.1: Survey flow: Upon passing the screening questionnaire, 464 participants were asked about their understanding of immersive technologies and awareness of data collection. Next, they were presented with four randomly selected scenarios from a total of 18 scenarios from Table 4.2, resulting in approximately 103 responses per scenario. For each scenario, participants answered questions relating to comfort with data collection, perceived data sensitivity, and how realistic they perceived the scenario to be. Finally, the participants shared their experience with immersive technologies and demographic information.

4.2.1 Scenario Development and Survey Design

Building on prior research in immersive technologies [3, 216, 190, 197, 77], IoT [180, 140], mobile [147, 267], and on the web [142], and discussions with privacy experts, we iteratively identified five high-level factors that likely influence users' privacy concerns in immersive environments. These factors include three static factors—`USER_TYPE`, `LOCATION`, and `DEVICE_TYPE`—which remain constant across all scenarios, and two dynamic factors—`DATA_TYPE` and `DEVICE_STATUS`—which vary between scenarios. We hypothesize that these factors influence users' privacy perceptions in immersive environments. Table 4.1 describes

[1]Prolific. https://www.prolific.co/

the factors and their corresponding levels. Following the literature [180], we structured the scenarios using the template below:

> *" You are at home/personal room, and your XR device (e.g., smart headset, touch controller, 3D projector) is keeping track of your [DATA_TYPE] when [DEVICE_STATUS]. "*

As the first exploration of users' awareness and concerns of data privacy in immersive technologies, we focused on personal systems in single-user scenarios, setting the data collection `LOCATION` as "Home/ personal room" and the `USER_TYPE` as "You" to keep the number of scenarios manageable for the participants. We referred to the `DEVICE_TYPE` as "extended reality (XR) devices" without distinguishing between VR, AR, MR, and other types of immersive technologies, as they often share similar data collection capabilities. Since data collection can occur through both direct user interactions and always-on sensors [3], our `DEVICE_STATUS` factor included: when users actively engage with the device (i.e., *in-use*) and when it operates in the background (i.e., *background-running*). For `DATA_TYPE`, we initially identified 26 data types that immersive technologies can capture, including account details (e.g., demographics, billing address, phone number), device information (e.g., crash reports, system logs), user geo-location, user movements, and visual attention based on existing literature (e.g., [197, 58, 3]), law reviews (e.g., [53, 114]), and technical reports (e.g., [259, 284]). To focus on data practices unique to immersive technologies, we excluded those extensively studied in mobile, web, and IoT research and narrowed our scenarios to nine data types (see Table 4.1). The combination of three static factors, two dynamic factors, nine data type categories, and two device statuses led to 18 unique scenarios, as shown in Table 4.2.

Participants were first asked to identify what data they believed immersive technology could observe based on their experience. Participants were then presented with four randomly selected scenarios and rated how likely each scenario was to happen today (`LIKELY_TODAY`), within two years (`LIKELY_IN_2YRS`), and within ten years (`LIKELY_IN_10YRS`), using a 5-point Likert scale from *1-extremely unlikely* to *5-extremely likely*, to assess

Factor	Levels
Static Factors	
`USER_TYPE`: the individual involved in data collection; Always set to the user	"you"
`LOCATION`: the location where the data collection occurs; Always set to a private place.	"home / personal room"
`DEVICE_TYPE`: the type of device that collects data. Always set to all immersive technologies.	"XR devices"
Dynamic Factors	
`DATA_TYPE`: the type of data collected by immersive technologies.	1.Physical appearance (e.g., body dimensions) [3, 58, 200, 197].
	2.Identifying in-app/in-world assets (e.g., personal virtual objects, personal avatars) [53, 197].
	3.Environment information and dimensions (e.g., users' surroundings, room layout, device/user position in relation to the environment, user position in relation to device) [58, 53, 165, 197].
	4.Physical movements and characteristics (e.g., head/hand/ body/eye motion, orientation, position, gestures, posture, fitness information) [53, 27, 94, 49, 173, 157, 139, 284, 197].
	5.Physiological data (e.g., pupil and cornea reflections, brainwaves, skin signals) [27, 94, 139, 284, 197].
	6.Visual attention (e.g., eye gaze, area of interest, fixation, heatmaps, time to first fixation, time spent on a certain point, fixation sequences) [27, 48, 206, 58, 284, 197].
	7.Mannerisms (e.g., gait, habitual movements) [53, 173, 206, 157].
	8.Cognitive, emotional, and personality estimates (e.g., cognitive load, stress, depression, excitement, identity traits, etc.) [27, 169, 200, 173, 197].
	9.Non-identifying virtual assets (e.g., in-app achievements) [53].
`DEVICE_STATUS`: if data collection happens actively or passively [3].	1. When "you" are interacting with the device.
	2. When the device is running in the background.

Table 4.1: Factors, their corresponding levels in the scenarios, and descriptions of each.

how *realistic* participants think the scenarios are. As an indicator of participants' concern [159, 180, 267, 147], we measured participants' comfort level with data collection (`COMFORT_LEVEL`), using a 5-point Likert-scale from *1-very uncomfortable* to *5-very comfortable*, to prevent biasing participants' perceptions with explicitly mentioned privacy-related terms. Participants were also asked to rate the perceived sensitivity of the data type

Table 4.2: Summary of the 18 scenarios used in the study. ID= Scenario identifier, n = number of participants presented with each scenario. Each scenario was presented to approximately 103 participants on average.

ID		**Scenarios**
	n	*All scenarios begin with*:
Scenario:Type-Status		"You are at home/personal room, and your XR device (e.g., smart headset, touch controller, 3D projectors) is keeping track of your..."
S:Appearance-Use	99	Physical appearance (e.g., body dimensions) when you use the device.
S:Appearance-Bg	107	Physical appearance (e.g., body dimensions) when the device is running in the background.
S:Identifying-Use	105	Identifying in-app/in-world assets (e.g., personal virtual objects, personal avatars) when you use the device.
S:Identifying-Bg	103	Identifying in-app/in-world assets (e.g., personal virtual objects, personal avatars) when the device is running in the background.
S:Environment-Use	102	Environment information and dimensions (e.g., users' surroundings, room layout, device/user position in relation to the environment, user position in relation to device) when you use the device.
S:Environment-Bg	107	Environment information and dimensions (e.g., users' surroundings, room layout, device/user position in relation to the environment, user position in relation to device) when the device is running in the background.
S:Movements-Use	106	Physical movements and characteristics (e.g., head/hand/body/eye motion, orientation, position, gestures, posture, fitness information) when you use the device.
S:Movements-Bg	103	Physical movements and characteristics (e.g., head/hand/body/eye motion, orientation, position, gestures, posture, fitness information) when the device is running in the background.
S:Physiological-Use	104	Physiological data (e.g., pupil and cornea reflections, brainwaves, skin signals) when you use the device.
S:Physiological-Bg	102	Physiological data (e.g., pupil and cornea reflections, brainwaves, skin signals) when the device is running in the background.
S:Visual-Use	99	Visual attention (e.g., eye gaze, area of interest, fixation, heatmaps, time to the first fixation, time spent on a certain point, fixation sequences) when you use the device.
S:Visual-Bg	101	Visual attention (e.g., eye gaze, area of interest, fixation, heatmaps, time to the first fixation, time spent on a certain point, fixation sequences) when the device is running in the background.
S:Mannerisms-Use	100	Mannerisms (e.g., gait, habitual movements) when you use the device.
S:Mannerisms-Bg	106	Mannerisms (e.g., gait, habitual movements) when the device is running in the background.
S:Cognitive-Use	104	Cognitive, emotional, and personality estimates (e.g., cognitive load, stress, depression, excitement, identity traits, etc.) when you use the device.
S:Cognitive-Bg	102	Cognitive, emotional, and personality estimates (e.g., cognitive load, stress, depression, excitement, identity traits, etc.) when the device is running in the background.
S:Non-identifying-Use	102	Non-identifying virtual assets (e.g., in-app achievements) when you use the device.
S:Non-identifying-Bg	107	Non-identifying virtual assets (e.g., in-app achievements) when the device is running in the background.

(DATA_SENSITIVITY) on a 5-point Likert-scale from *1-not sensitive* to *5-very sensitive*. For participants who expressed discomfort with the situation described in the scenario, we asked them to share their mitigation strategy in an open-ended question. Finally, we inquired about participants' personal experience with immersive technologies, including how many years they have been using these devices (EXP_YEARS), the type of devices used (EXP_DEVICE), the frequency of use (EXP_FREQUENCY), and the purpose for using these devices (EXP_PURPOSE). We measured participants' general level of privacy concern on the Internet using the Internet Users' Information Privacy Concerns Scale (IUIPC) [156], which consists of three dimensions of user privacy concerns: collection (IUIPC_COLLECTION), control (IUIPC_CONTROL), and awareness (IUIPC_AWARENESS). We closed the survey with demographic questions. Figure 4.1 summarizes the survey flow. A complete set of questions is included in Section C.1.

4.2.2 Recruitment and Participants

A power analysis [65] determined that at least 57 participants per scenario pair were needed to achieve $\geq 95\%$ power with a $\leq 5\%$ margin of error (effect size = 0.50) for a Wilcoxon signed-rank test. A total of 549 participants completed our REB-approved survey and received $5.80 USD each[2]. After excluding 49 incomplete responses, 23 that failed attention checks, and 13 flagged as bots by Qualtrics, we retained 464 valid responses ($n \approx 64$ per scenario pair). Table 4.3 presents participant demographics and IUIPC scores [156].

4.2.3 Data Analysis

We present details of our quantitative analysis while introducing our results in Section 4.3. For the open-ended question, two researchers conducted an inductive thematic analysis [39]. After familiarizing ourselves by scanning the data, we excluded blank or incoherent responses and retained answers like "none" or "nothing" as they reflect a lack of mitigation strategies

[2]The $5.80 USD payment ($\approx$ $8 CAD) was based on Ontario's minimum hourly wage. See: *Salary standards and minimum wage.* (n.d.). Retrieved March 20, 2025, from https://www.immigrationwaterlooregion.ca/en/study-and-work/salary-standards-and-minimum-wage.aspx.

Table 4.3: Breakdown of our participants' ($N = 464$) gender, age, education level, income level, and three IUIPC dimensions [156]. A detailed overview of participants' demographic is located in Table C.2.

Gender		Age		Education Level		Income		IUIPC factors	
Man	230 (50%)	Range	18-56	No high school	4 (¡1%)	Less than $25,000	182 (39%)	*IUIPC_Collection*	
Woman	222 (48%)	Mean (SD)	27.78 (7.95)	High school	173 (37%)	$25,000-$49,999	151 (33%)	Range	(1.25 - 7)
Non-binary	11 (2%)			Associates	30 (7%)	$50,000-$99,999	86 (19%)	Mean (SD)	5.69 (1.14)
Prefer not to say	1 (¡1%)			Bachelors	162 (35%)	$100,000-$199,999	19 (4%)	*IUIPC_Control*	
				Professional	94 (20%)	More than $200,000	5 (1%)	Range	(3 - 7)
				No answer	1 (¡1%)	Prefer not to say	21 (5%)	Mean (SD)	5.78 (0.92)
								IUIPC_Awareness	
								Range	(3 - 7)
								Mean (SD)	6.29 (0.74)

(see response counts in Figure 4.4). The two researchers independently coded about 10% of the data, discussed and resolved conflicts, and repeated this process twice until finalizing the codebook. Using the codebook, we developed and refined themes, summarized in Section C.2.

4.3 Findings

In this section, we describe our results on participants' awareness of data collection practices, comfort with data sharing, and coping strategies.

4.3.1 RQ4.1: How much are people aware of the data collected through Immersive Technologies?

Figure 4.2 shows the distribution of responses from our participants on the types of data they believed immersive technologies could collect. The majority of participants (84%) recognized the collection of *physical movements and characteristics*, while 74% acknowledged *environment information and dimensions*. A large proportion of participants realized these technologies can track their *visual attention* (65%), *identifying in-app/in-world assets* (48%), and *non-identifying virtual assets* (46%). Some participants mentioned *mannerisms* (32%),

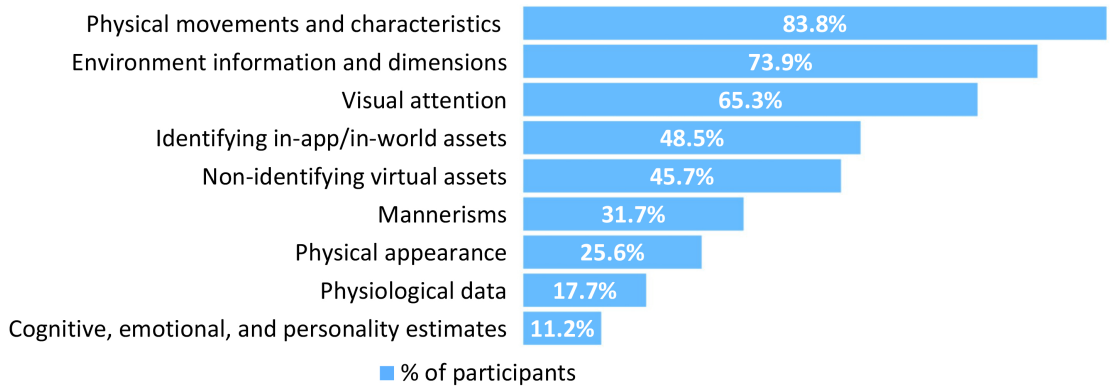


Figure 4.2: Percentage of participants' ($N = 464$) perceived data collection of various data types through immersive technologies.

physical appearance (26%), and *physiological data* (18%). Only 11% thought *cognitive, emotional, and personality estimates* were tracked. A small number ($\leq$ 1%) mentioned other data, such as purchases, while 1% were uncertain.

4.3.2 RQ4.2: To what extend are people concerned about their privacy regarding data collection in Immersive Technologies?

Figure 4.3 shows participants' `COMFORT_LEVEL` across different data types and device statuses. We validated the observed differences through Wilcoxon signed-rank comparisons [283] with Bonferroni correction [34] (see Table C.3 and Table C.4), and we report P values for significant pairwise comparisons in "()".

Participants reported the highest discomfort when scenarios involved *cognitive, emotional, and personality estimates*, with 29% selecting "very uncomfortable" and 35% selecting "uncomfortable" ($P \leq .007$). This data type was also rated the most sensitive (47% "very sensitive") and the least likely to occur today (40% "extremely unlikely") ($P < .001$). In contrast, participants were most comfortable when *non-identifying virtual assets* was observed, with only 9% selecting "uncomfortable" and 3% "very uncomfortable" ($P \leq .005$), and 43% rated it as not sensitive ($P < .001$). Furthermore, a slightly greater number of

Data Type	1- Very uncomfortable	2 - Uncomfortable	3 - Neutral	4 - Comfortable	5 - Very comfortable	1 - Not at all sensitive	2 - Slightly sensitive	3 - Somewhat sensitive	4 - Sensitive	5 - Very sensitive	1- Extremely unlikely	2 - Unlikely	3 - Neutral	4 - Likely	5 - Extremely likely
Physical appearance	14%	34%	25%	21%	5%	11%	16%	21%	32%	21%	18%	26%	21%	24%	10%
Identifying in-app/in-world assets	7%	17%	30%	32%	13%	25%	27%	23%	18%	8%	11%	14%	22%	30%	23%
Environment info & dimensions	10%	27%	35%	22%	6%	7%	22%	23%	30%	17%	13%	17%	20%	34%	15%
Physical movements/characteristics	14%	23%	26%	28%	9%	12%	20%	25%	25%	18%	11%	16%	21%	36%	16%
Physiological data	21%	30%	33%	14%	2%	6%	13%	20%	33%	28%	30%	28%	19%	19%	4%
Visual attention	11%	28%	30%	23%	9%	14%	24%	28%	23%	12%	13%	28%	19%	27%	14%
Mannerisms	14%	31%	32%	19%	4%	10%	19%	29%	27%	15%	19%	24%	19%	33%	5%
Cognitive/emotional/personality	29%	35%	18%	15%	4%	2%	7%	13%	31%	47%	40%	30%	17%	12%	2%
Non-identifying virtual assets	3%	9%	33%	32%	24%	43%	20%	19%	11%	8%	10%	7%	17%	27%	39%
Devices Status															
Running in the background	18%	27%	27%	19%	8%	15%	21%	23%	24%	17%	21%	24%	21%	24%	11%
In-use	9%	24%	32%	27%	9%	14%	16%	22%	27%	21%	15%	18%	18%	30%	17%

Figure 4.3: Participants' ($n = 464$) comfort level, perceived data sensitivity, and scenario realism across data types and device statuses. Darker cells indicate higher percentages. For example, 29% of participants selected "very uncomfortable" when their *cognitive, emotional, and personality estimates* were observed.

participants expressed discomfort when the device operated in the background (18% "very uncomfortable," 27% "uncomfortable"). On the other hand, scenarios with active device interaction were perceived as more sensitive (27% "sensitive," 21% "very sensitive") and more realistic (30% "likely," 17% "extremely likely") ($P \leq .005$).

4.3.3 RQ4.3: What factors contribute to user privacy concerns in Immersive Technologies?

We examine how participants' perceptions of scenario realism, general online privacy concerns, and experience with immersive technologies influence their comfort with data collection. We used Cumulative Link Mixed Model (CLMM) regression[3] with a random intercept for each participant. CLMM is well-suited for analyzing repeated measures experiments with ordinal dependent variables, such as our study, where participants

[3]We used the Ordinal R-package (https://cran.r-project.org/web/packages/ordinal/)

evaluated multiple scenarios [38]. We first conducted a set of univariate CLMM regressions, each using COMFORT_LEVEL as the dependent variable and one of the factors as the predictor, to identify significant relationships for our multivariate model. As shown in Table 4.4, COMFORT_LEVEL was significantly associated with DATA_TYPE ($P < .001$), DEVICE_STATUS ($P < .001$), perceived DATA_SENSITIVITY ($P < .001$), LIKELY_TODAY/IN_2YRS/IN_10YRS ($P < .001$), general privacy concerns on the Internet (IUIPC scores $P < .001$). However, no significance was found from demographic factors or prior experience with these technologies.

We conducted a multivariate CLMM regression with COMFORT_LEVEL as the dependent variable, using significant predictors from the univariate analyses (see Table 4.4). We applied backwards elimination, sequentially removing the variable with the least significance until reaching the lowest Akaike Information Criterion (AIC) [123], to obtain the best-fit model. The final model (Table 4.5) ranks predictors with the highest contribution (lowest AIC in univariate CLMM) to COMFORT_LEVEL appearing first, based on their independent AIC values in the univariate CLMM.

As shown in Table 4.5, the perceived DATA_SENSITIVITY had the greatest negative effect on participants' COMFORT_LEVEL ($P < .001$), and the perceived likelihood of occurring today (LIKELY_TODAY, $P < .001$) positively influenced COMFORT_LEVEL. This suggests that higher data sensitivity lowers participants' comfort, whereas greater perceived realism increases participants' comfort with data collection. However, not all data types showed significant effects. Compared to Scenarios with *non-identifying virtual assets*, participants reported lower COMFORT_LEVEL when *visual attention* ($P=.007$), *mannerisms* ($P=.002$), *physical appearance* ($P=.02$), and *physiological data* ($P=.02$) were collected. On the other hand, scenarios involving *identifying in-app/in-world assets*, *physical movements and characteristics*, and *environment information and dimensions* showed no significant impact on COMFORT_LEVEL. This aligns with our results in Figure 4.3, where participants exhibited neutral COMFORT_LEVEL for these data types, likely due to their unclear DATA_SENSITIVITY perceptions and limited understanding of privacy implications. Participants' qualitative responses further support this, as participants frequently sought more information on data collection and privacy laws (i.e., "comprehend and control what happens to my data") when these data types were involved (see Figure 4.4).

Table 4.4: Univariate Cumulative Linked Mixed Model analyses of factors impacting participants' comfort level (5-point Likert data, from 1-very uncomfortable to 5-very comfortable), with a random intercept per participant. Ordinal data are used as is. Participants demographics and experience with immersive devices were considered in the analysis but are not presented as they did not show significance ($P > .05$).

Predictor						**AIC**
data_type	**Estimates**	**Std. Error**	**z**	***P* value**	**OR (95%CI)**	5185.92
Non-identifying virtual assets	Reference					
Identifying in-app/in-world assets	-0.84	0.20	-4.13	< .001***	0.43 (0.29, 0.64)	
Visual attention	-1.67	0.21	-8.05	< .001***	0.19 (0.13, 0.28)	
Physical movements and characteristics	-1.45	0.20	-7.14	< .001***	0.23 (0.16, 0.35)	
Mannerisms	-2.09	0.21	-10.10	< .001***	0.12 (0.08, 0.19)	
Environment information and dimensions	-1.72	0.20	-8.57	< .001***	0.18 (0.12, 0.27)	
Physical appearance	-2.10	0.21	-10.13	< .001***	0.12 (0.08, 0.18)	
Physiological data	-2.54	0.21	-12.08	< .001***	0.08 (0.05, 0.12)	
Cognitive, emotional, and personality estimates	-3.17	0.22	-14.41	< .001***	0.04 (0.03, 0.07)	
device_status	**Estimates**	**Std. Error**	**z**	***P* value**	**OR (95%CI)**	5442.24
In-use	Reference					
Running in the background	-0.55	0.09	-5.94	< .001***	0.58 (0.48, 0.69)	
data_sensitivity	**Estimates**	**Std. Error**	**z**	***P* value**	**OR (95%CI)**	4442.67
1 - Not sensitive	Reference					
2	-2.25	0.20	-11.09	< .001***	0.11 (0.07, 0.16)	
3	-3.57	0.22	-16.52	< .001***	0.03 (0.02, 0.04)	
4	-5.12	0.24	-21.64	< .001***	0.01 (0.00, 0.01)	
5 - Very sensitive	-6.74	0.27	-24.72	< .001***	0.00 (0.00, 0.00)	
likely_today	**Estimates**	**Std. Error**	**z**	***P* value**	**OR (95%CI)**	4984.37
1 - Extremely unlikely	Reference					
2 - Unlikely	0.40	0.18	2.26	.02*	1.49 (1.05, 2.11)	
3 - Neutral	1.21	0.19	6.46	< .001***	3.34 (2.32, 4.82)	
4 - Likely	2.22	0.19	11.85	< .001***	9.17 (6.36, 13.23)	
5 - Extremely likely	4.12	0.23	17.61	< .001***	61.44 (38.85, 97.15)	
likely_in_2yrs	**Estimates**	**Std. Error**	**z**	***P* value**	**OR (95%CI)**	5097.70
1 - Extremely unlikely	Reference					
2 - Unlikely	0.61	0.34	1.81	.07	1.84 (0.95, 3.58)	
3 - Neutral	1.21	0.34	3.59	< .001***	3.37 (1.73, 6.53)	
4 - Likely	2.37	0.33	7.18	< .001***	10.68 (5.59, 20.40)	
5 - Extremely likely	3.75	0.34	10.94	< .001***	42.31 (21.62, 82.73)	
likely_in_10yrs	**Estimates**	**Std. Error**	**z**	***P* value**	**OR (95%CI)**	5305.95
1 - Extremely unlikely	Reference					
2 - Unlikely	-0.26	0.51	-0.50	0.62	0.77 (0.28, 2.11)	
3 - Neutral	0.58	0.49	1.18	0.24	1.78 (0.69, 4.62)	
4 - Likely	1.10	0.47	2.35	.02*	3.01 (1.20, 7.54)	
5 - Extremely likely	2.31	0.47	4.91	< .001***	10.04 (4.00, 25.22)	
IUIPC scores	**Estimates**	**Std. Error**	**z**	***P* value**	**OR (95%CI)**	5409.70
IUIPC_CONTROL	-0.34	0.08	-4.45	< .001***	0.71 (0.61, 0.83)	
IUIPC_AWARENESS	-0.36	0.10	-3.80	< .001***	0.70 (0.58, 0.84)	
IUIPC_COLLECTION	-0.50	0.06	-8.37	< .001***	0.61 (0.54, 0.68)	

*Note. Significance are displayed as: *** P< .001, ** P < .01, * P < .05. OR=Odds Ratio, CI=Confidence Interval. The Reference categories were selected to enhance result interpretability. For OR, a value greater than 1 indicates a positive relationship, and a value less than 1 indicates a negative relationship.*

Table 4.5: Multivariate Cumulative Linked Mixed Model analyses of factors impacting participants' comfort level (1-very uncomfortable to 5-very comfortable), with a random intercept per participant. Ordinal data are used as is. Only variables showed significance are presented ($P \leq .05$).

Predictor	Estimates	Std. Error	z	*P* value	OR (95%CI)
data_sensitivity					
1 - Not sensitive	Reference				
2	-1.83	0.21	-8.66	< .001***	0.16 (0.11, 0.24)
3	-2.92	0.23	-12.93	< .001***	0.05 (0.04, 0.08)
4	-4.27	0.25	-17.13	< .001***	0.01 (0.01, 0.02)
5 - Very sensitive	-5.66	0.29	-19.54	< .001***	0.00 (0.00, 0.01)
likely_today					
1 - Extremely unlikely	Reference				
2 - Unlikely	0.29	0.19	1.54	.13	1.33 (0.92, 1.92)
3 - Neutral	0.81	0.20	4.09	< .001***	2.25 (1.53, 3.33)
4 - Likely	1.44	0.20	7.22	< .001***	4.22 (2.85, 6.23)
5 - Extremely likely	2.52	0.25	10.10	< .001***	12.44 (7.63, 20.31)
data_type					
Non-identifying virtual assets	Reference				
Identifying in-app/in-world assets	-0.25	0.22	-1.17	.24	0.78 (0.51, 1.19)
Visual attention	-0.61	0.23	-2.71	.007**	0.54 (0.35, 0.84)
Physical movements and characteristics	-0.25	0.22	-1.10	.27	0.78 (0.51, 1.21)
Mannerisms	-0.72	0.23	-3.17	.002**	0.49 (0.31, 0.76)
Environment information and dimensions	-0.38	0.22	-1.71	.09	0.69 (0.45, 1.06)
Physical appearance	-0.55	0.23	-2.42	.02*	0.58 (0.37, 0.90)
Physiological data	-0.56	0.23	-2.38	.02*	0.57 (0.36, 0.91)
Cognitive, emotional, and personality estimates	-0.47	0.25	-1.85	.06	0.63 (0.38, 1.03)
IUIPC scores					
IUIPC_COLLECTION	-0.38	0.09	-4.26	< .001***	0.68 (0.57, 0.82)
IUIPC_CONTROL	-0.22	0.11	-2.02	.06	0.80 (0.65, 0.99)
device_status					
In-use	Reference				
Running in the background	-0.40	0.10	-3.86	< .001***	0.67 (0.55, 0.82)

Note. final AIC = 4244.43. Significance are displayed as follows: *** *P*< .001, ** *P* < .01, * *P* < .05. *OR=Odds Ratio. CI=Confidence Interval. The Reference categories were selected to enhance result interpretability. For OR, a value greater than 1 indicates a positive relationship, and a value less than 1 indicates a negative relationship.*

Participants expressed strong discomfort with scenarios involving *cognitive, emotional, and personality estimates* and considered these data types the most sensitive. Their

qualitative responses described such data collection as *"too much intrusion"* compared to others. This discomfort may also be related to the trust issues with data recipients and the perceived purpose of data use [77, 197], as some participants sought clarity on data practices and expressed distrust toward manufacturers and device systems (see Figure 4.4).

Lastly, participants' `COMFORT_LEVEL` was negatively associated with their `IUIPC_COLLECTION` score ($P < .001$), suggesting that concerns about the fairness of data collection (i.e., cost vs. benefits) negatively impacted comfort. `DEVICE_STATUS` also had a negative effect ($P < .001$), with participants reporting greater discomfort when the device operated in the background. These findings align with our qualitative results, where participants expressed fears of surveillance, data misuse, and distrust in how data can be used (see Section 4.3.4).

4.3.4 RQ4.4: What coping strategies (if any) do people use to mitigate their privacy concerns?

We discuss themes from participants' qualitative responses (Figure 4.4) and their connection to our quantitative findings. For clarity, themes are in quotations, and participant quotes are in *italics*. We report percentage ranges (e.g., 7% $\sim$ 28%) to show variation across scenarios and single percentages (e.g., 3%) for themes specific to a scenario or participant group. The full list of questions and themes is available in Section C.1 and Section C.2.

Across all 18 scenarios, a large portion of participants expressed an inability to mitigate their discomfort with data collection and intended to continue using the device ("ignore or give up"). Their responses reflected a sense of pessimism about privacy in immersive environments and had become accustomed to the absence of privacy.

> *"Technology will overcome us. I think I would feel strange at first, but eventually I would get used to, even tho I would rather not share this information with unknowned entities. We don't have privacy anymore, I realize that."*
>
> — *Participant 313*

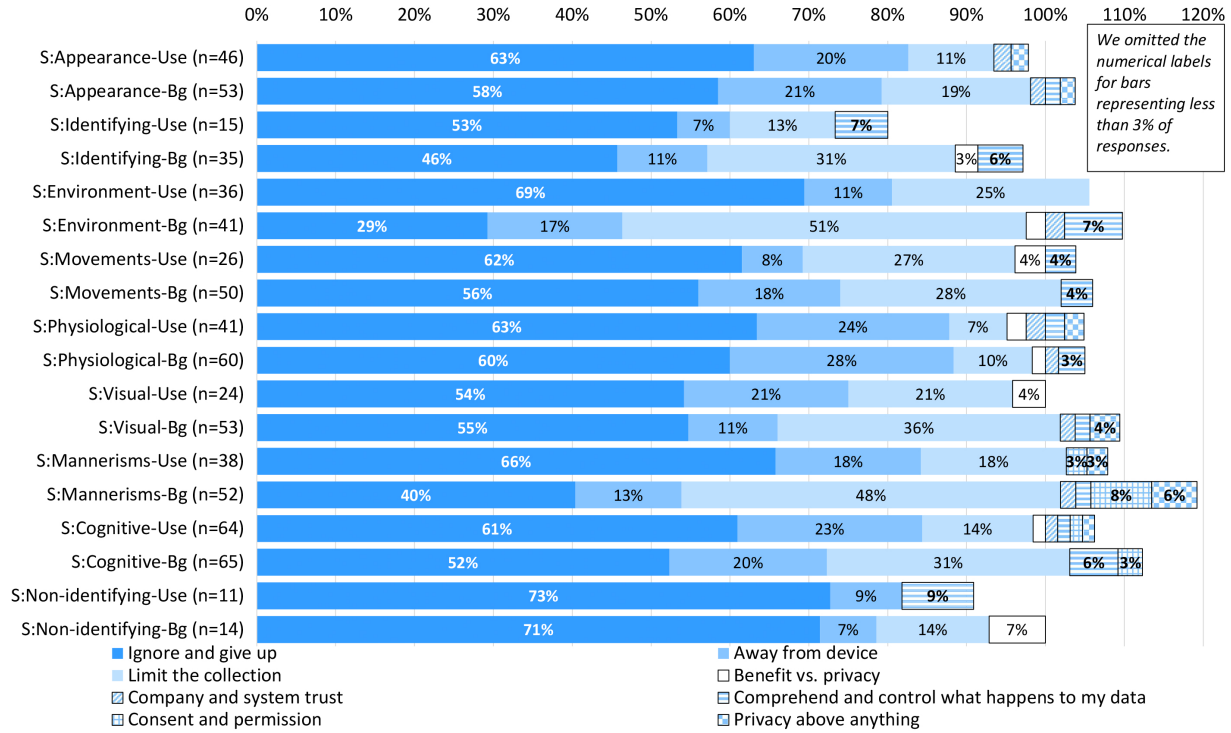


Figure 4.4: n = number of participants who answered the conditional open-ended question: "What would you do (if any) to mitigate the discomfort raised?" (Q5). This question was shown only to those who selected as "1-very uncomfortable" or "2-uncomfortable" (Q3) in each scenario. Total percentages exceed 100% as a participant may mention multiple coping strategies.

Notably, for scenarios involving the same data type, participants were more likely to disregard data collection when actively using the device. This aligns with our findings Figure 4.3, where more participants expressed discomfort when the device operated passively in the background. In addition, a significantly lower number of participants expressed discomfort when *non-identifying virtual assets* were collected ($n = 11$ in `S:NON-IDENTIFYING-USE`, $n = 14$ in `S:NON-IDENTIFYING-BG`), with most choosing to "ignore and give up" (73% and 71%, respectively). This finding supports our quantitative results that *non-identifying virtual assets* were perceived as the least sensitive.

While the majority of participants chose to *"give up,"* some simultaneously stated that *"unless I'm aware of data collection,"* suggesting that transparency about data collection might facilitate actions of privacy protection. In addition, in contrast to other data

types, 29% ignored discomfort when *environment info & dimensions* was collected in `S:ENVIRONMENT-BG`, as they viewed tracking of environmental data as more controllable. Most (51%) suggested isolating the device in a designated, non-personal room to *"limit the data collection."* In all scenarios, 7% $\sim$ 51% of participants suggested the strategy to protect their privacy, such as disabling sensors, placing devices in low-privacy areas, unplugging them, uninstalling invasive apps, adjusting privacy settings, or using specialized tools to block data collection. Some participants engaged in self-censorship, such as using devices only when necessary, altering mannerisms, or suppressing emotions to avoid monitoring.

> *"I would probably change my mannerism and try to limit my displays of any sort of emotions from time to time to feel like my 'real me' is not being monitored."*
>
> — *Participant 215*

Some participants (7% $\sim$ 28%) preferred to stay "away from the device," either by discontinuing use or disposing of it, while a few (3%) stated they would have avoided purchasing it had they known about the data collection. Conversely, six participants (1%) weighed the device's benefits against potential privacy risks before deciding to use it. About $\sim$ 9% sought greater control over their data and reported actively reading privacy policies, laws, and online resources, and exploring ways to limit or delete collected data. They emphasized the need for anonymization and viewed the data use for targeted ads or behavior manipulation as inappropriate. In addition, $\sim$ 8% of highlighted the importance of informed consent. In general, participants expressed a desire to understand what is being collected, how it is used, and with whom their data is shared.

> *"I don't like the idea of my personal data being collected by other companies for their own profit. Show the users that data is only being used for their interest and not with second intentions."*
>
> — *Participant 163*

Lastly, $\sim$ 18% of the participants prioritized privacy above all other features, expressing a willingness to switch to manufacturers that better protect their data. In contrast, $\sim$ 2% fully trusted the manufacturer and accepted all data-related processes.

4.4 Discussion

Literature emphasizes the need for user education on deceptive design in immersive technologies [169, 27, 45] and emphasizes the importance of understanding users' mental models to support effective education and risk communication [79]. Since data collected through immersive technologies can be a powerful source to enable deceptive design [27, 139, 173], we conducted a scenario-based online survey with 464 immersive technology users to explore their awareness and concerns about specific data collection practices in immersive technologies.

Many of our findings align with prior research on IoT (e.g., [180, 140, 198]), mobile (e.g., [147, 267]), and web privacy (e.g., [142]), suggesting a convergence in users' privacy concerns across different technologies. Our regression analysis revealed that users' comfort with data collection was influenced by perceived data sensitivity (e.g., [111, 190]), data type (e.g., [180]), perceived equity of data collection (i.e., the IUIPC_collection [111]), and the perceived realism of the scenario (e.g., [180]). Our study also found a significant association between privacy concerns and device status, aligning with concerns about "always-on" devices from prior literature [3, 216]. While demographic factors and prior experience with immersive technologies did not significantly impact privacy concerns, we suspect this is due to participants' limited exposure to newer commercial immersive devices.

4.4.1 Users' Resignation and Limited Mitigation Strategies

Despite widespread discomfort, most participants felt that protecting their privacy in immersive technologies was too difficult. Pessimistically, many participants also expressed a sense of privacy resignation, believing they had already lost control over their data in other digital environments and ultimately *"give up."*

Participants also lacked effective privacy-protective strategies. Our qualitative analysis revealed that their approaches largely mirrored those used in non-immersive contexts. For example, participants reported self-censorship in response to nearby immersive devices, experiencing a "chilling effect" that made them more conscious of their speech and emotions [139, 200]. Some attempted to limit data collection by physically blocking sensors, self-censoring, or discontinuing use altogether. We suspect that familiarity with other technologies led participants to rely on prior privacy experiences, potentially underestimating the unique risks of immersive environments, especially as these technologies process data in increasingly novel and sophisticated ways. Participants' reliance on strategies such as removing devices or blocking sensors aligns with previous findings on how users attempt to manage personal space and privacy in IoT surveillance [198].

4.4.2 Limited User Awareness of Data Practices

Our findings reveal that participants were largely unaware of the granular data collected by immersive technologies, particularly data types uncommon in non-immersive systems, such as physiological inputs, physical movements, and inferred cognitive states, emotions, and personality traits (see Figure 4.2). These data make immersive technologies potentially more invasive than web and mobile devices, as they can serve as behavioral identifiers [94, 173, 206] and expose users to privacy risks and emotional manipulation [169]. This lack of awareness can contribute to users' misconceptions about privacy risks and benefits [55].

Many participants expressed discomfort with passive data collection and inferences drawn from unconscious actions (e.g., emotional inferences from facial expressions or physiological sensors), likely because these data are harder to assess than those actively shared (e.g., deliberately smiling to signal agreement). More participants sought to *"comprehend and control what happens to my data"* when the scenario involved a background-running device (see Figure 4.4), suggesting that both the *type* and *method* of data collection influence user comfort. Thus, effective communication about data collection in immersive technologies is essential, especially for passively collected data that are not typically required for 2D web and mobile applications (e.g., cognitive, emotional, and personality estimates) and can

enable new forms of user manipulation. Therefore, in Chapter 7, we examine how deceptive design manifests in privacy communication and decision-making in immersive environments. The presence of such design patterns can undermine users' ability to make informed choices and increase privacy risks.

4.4.3 Limitations

Our study has limitations. First, our sample does not include non-English speaking users, non-users, and is not representative of North America and Europe. Despite this, our findings offer valuable insights into experienced users' perspectives. Future research could explore non-users, non-English speakers, and user vs. non-user differences. Second, our survey-based approach relies on self-reported concerns and behaviors, which may not reflect actual usage. Participants' lack of experience with certain circumstances described in scenarios could also affect response accuracy. Third, we recognize that mentioning data collection could influence participants' privacy concerns. To minimize this impact, we framed the study around user experience and avoided terms like "privacy," "risk," and "concern" in recruitment and questionnaires. Finally, the factors we examined in our scenarios were not an exhaustive list. Currently, much information regarding immersive technologies' data practices is unclear [259]. We hope that our study can provide valuable insights for future discussions and encourage researchers to explore user privacy concerns in more complex situations, such as bystander involvement, multiple user scenarios, and other related factors.

4.5 Conclusion

Overall, our findings reveal a critical gap in users' awareness of immersive technology data practices and their ability to effectively protect their privacy. While participants expressed concerns, many felt powerless, leading to privacy resignation and reliance on coping strategies borrowed from non-immersive contexts. This lack of understanding is particularly concerning given the sophisticated ways immersive technologies passively collect and infer sensitive data. As these technologies evolve, stronger privacy communication, greater transparency, and

improved user controls are essential. Build on these insights, Chapter 6 explores privacy issues as one of several influences of deceptive design in immersive technologies, with a focus on how limited user awareness can be exploited. These observations laid the groundwork for our investigation in Chapter 7, where we specifically explore deceptive design in commercially available VR applications, with a particular focus on how it manifests in mechanisms that communicate privacy information and support user privacy decision-making.

Chapter 5

Developing an Assessment Guide for Investigating Deceptive Design in Immersive Environments

---

Suggested Citation:

Hadan, H., Zhang-Kennedy, L., & Nacke, L. E. (2024, October). 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* (pp. 109-123). https://doi.org/10.1145/3665463.3678820

5.1 Introduction

Building on Chapter 3, in this chapter, we address Objective 2 by constructing a *Deceptive Design Assessment Guide* (referred to as the *Assessment Guide*) that systematically captures deceptive design patterns by synthesizing taxonomies from foundational literature in the field (e.g., [89, 287, 129]). This *Assessment Guide* builds on existing taxonomies of

deceptive design from web, mobile, and immersive environments, enabling the analysis of both deceptive strategies that migrate directly from non-immersive platforms and those that may emerge from the unique properties of immersive technologies, as hypothesized in the literature (see Chapter 3). This *Assessment Guide* served as a standardized framework to ensure consistency in our analyses and comparisons presented in Chapter 6 and Chapter 7.

5.1.1 Motivation and Gaps in Existing Research

The overarching research goal of this thesis is to investigate deceptive design patterns in commercially available immersive applications and compare them to those found in traditional computer applications. However, a standardized foundation for identifying and analyzing deceptive design remains lacking. As discussed in Section 2.3.1, academic research and regulatory bodies have proposed various taxonomies that classify deceptive design using different terminologies, definitions, and illustrative examples (e.g., [89, 162, 287, 25]). For instance, Mathur et al. [162] categorized patterns such as sneaking and urgency based on how they manipulate users' choice architecture, while Brignull [25] offered a practitioner-oriented classification that includes patterns like Bait and Switch and Disguised Ads. In the context of video games, Zagal et al. [287] introduced a taxonomy focused on game-specific mechanics, such as Grinding and Playing by Appointment, but it does not address deceptive design patterns that manifest in general user interface elements or system-level interactions. Without a standardized and comprehensive framework that integrates these diverse perspectives while accounting for the unique properties of immersive technologies, it is difficult to rigorously assess deceptive design practices across platforms and produce findings that extend beyond the studied contexts.

5.1.2 Chapter Research Goal and Contribution

To establish a standardized foundation for our analysis, we constructed a *Deceptive Design Assessment Guide* (referred to as the *Assessment Guide*), which systematically captures deceptive design patterns in both computer and immersive applications [106]. Building

upon established classifications from our Chapter 3 and prior research (e.g., [89, 287, 129]), the *Assessment Guide* provides a standardized framework to ensure consistency in our comparisons. It also allows us to examine how deceptive design strategies in immersive environments include both those that migrate from traditional computer applications and those that may emerge from the unique properties of immersive technologies, as well as their unique impact on users compared to traditional 2D experiences.

In this chapter, we present the initial version of our *Assessment Guide*, which is then applied and refined in a comparative analysis of deceptive design patterns in a computer application and 12 commercial immersive applications in Chapter 6 and Chapter 7.

5.2 Constructing Deceptive Design Assessment Guide Based on Literature

To ensure consistency in identifying and analyzing deceptive design in computer and immersive applications, we developed an initial version of a *Deceptive Design Assessment Guide* (see Table 5.1). This process was inspired by literature's deductive codebook method for comparing deceptive design in mobile and web-based applications [96]. To bootstrap our *Assessment Guide* and make our study comparable to existing deceptive design literature, we adopted Gray et al. [89]'s ontology (see Table 2.1) of deceptive design patterns as our starting point—the most recent and comprehensive framework at the time of our study—grounded in foundational literature (e.g., [24, 87, 163]) and regulatory efforts (e.g., [82, 192]) in the field. However, as this ontology was not specifically tailored to immersive environments, we expanded it with insights from our systematic literature review in Chapter 3 and frameworks that focus on 3D [129] and game-specific [287, 129] deceptive designs.

We began by reviewing deceptive design strategies from our Chapter 3 and the gathered literature [89, 287, 129]. Using an affinity diagramming approach [110] in Miro[1], we compared and organized diverse definitions and examples of each pattern into structured categories.

[1]Miro — The Innovation Workspace. https://miro.com/

Table 5.1: This table presents our *Deceptive Design Assessment Guide* and the source literature of themes and codes [89, 287, 129, 100]. This *Assessment Guide* served as the foundation of our identification of deceptive designs in the selected VR-based and computer-based games.

***Theme*/Subtheme**	**Code**	**Definition**	**Correspondence to Taxonomies from Literature**
Theme 1: Sneaking			
Bait and Switch	Disguised Ads	❶ Disguise ads as genuine content, trick users into clicking on it.	❯ Disguised Ads [89]
Hiding Information	Sneak into Basket	❶ Sneak items into a user's cart, lead to unintended purchases.	❯ Sneak into Basket [89]
	Drip Pricing, Hidden Costs, or Partitioned Pricing	❶ Gradually reveal additional costs, delaying the full price until after effort is invested in the purchase process.	❯ Drip Pricing, Hidden Costs, or Partitioned Pricing [89]
	Reference Pricing 🥽	❶ Include a price-inflated item or a poorer-quality item with same price, making a current price seem like a better deal.	❯ Reference Pricing [89], Cheap Item Placed Next to Expensive Item [129], Physical Placement of Items [129], Anchoring Tricks (Anchoring, Decoy Effect) [287]
Perception Hacking ⬡	-	❶ Alter visuals or display out-of-sight ads, causing unwanted and unintentional interaction with objects (e.g., ads)	❯ Perception Hacking [100], Obscuring Reality [100]
(De)contextualizing Cues	Conflicting Information	❶ Confuse users by presenting contradictory details, making them unsure and likely to accept potentially unfavorable defaults.	❯ Conflicting Information [89]
	Information without context	❶ Hide relevant information or controls, making it difficult for users to find what they need.	❯ Information without context [89]
Theme 2: Obstruction			
Roach Motel	Immortal Accounts	❶ Trap users by making account deletion difficult or impossible.	❯ Immortal Accounts [89]
	Dead Ends	❶ Frustrate users by hiding information behind broken links or redirects, preventing them from finding desired information.	❯ Dead Ends [89]
Creating Barriers	Price Comparison Prevention	❶ Hide information or block copying/pasting, making it difficult to compare prices across vendors.	❯ Price Comparison Prevention [89]
	Intermediate Currencies 🥽	❶ Hide the real price behind a virtual currency, making informed purchase decisions difficult.	❯ Intermediate Currencies [89], Use of Multiple Currencies [129], Premium Currency [287]
Adding Steps	Privacy Mazes	❶ Bury privacy controls under layers of confusing menus, hindering users from making informed choices.	❯ Privacy Mazes [89]
Reality Distortion ⬡	-	❶ Conceal parts of reality with digital objects, through daily wear and photorealistic graphics, leading to false perception and change of behaviours.	❯ Reality Distortion [100], Obscuring Reality [100], Persistent Exposure to Manipulation [100]
Theme 3: Social Engineering			
Scarcity or Popularity Claims	High Demand 🥽	❶ Create a false sense of urgency by exaggerating product popularity, tricking users into rushed purchases.	❯ Anchoring Tricks (item popularity) [287] ❯ High Demand [89]
Social Proof	Low Stock 🥽	❶ Pressure users into impulsive purchases by falsely indicating limited product availability.	❯ Low Stock [89],Artificial Scarcity (only a certain number of items available) [287]
	Endorsements and Testimonials	❶ Portray biased or fabricated testimonials as genuine to influence users' purchase decisions.	❯ Endorsements and Testimonials [89], Friend Spam / Impersonation (friends follow your endorsement) [287]
	Parasocial Pressure 🥽 ⬡	❶ Exploit users' trust in celebrities or other entities with inauthentic endorsements to influence users' decisions.	❯ Parasocial Pressure [89], Anchoring Tricks (friends' purchase activities) [287], NPC Asks or Suggests a Purchase [129], Hyperpersonalization (recreations of their trusted people) [100], Instructed/Told to Do [129]
Urgency	Activity Messages	❶ Create urgency with fake activity notifications of others.	❯ Activity Messages [89]
	Countdown Timers 🥽	❶ create urgency with fake countdown timers.	❯ Countdown Timers [89], Artificial Scarcity [287]
	Limited Time Messages 🥽	❶ Create urgency with fake limited-time offers.	❯ Limited Time Messages [89], Artificial Scarcity [287]
	Fear of Missing Out (FOMO) 🥽	❶ Exploit anxiety about missing exciting or valuable experiences.	❯ Fear of Missing Out [287, 129]
Personalization	Confirmshaming	❶ Guilt-trip users with manipulative language.	❯ Confirmshaming [89]
	Social Obligation 🥽	❶ Create a sense of obligation to avoid letting down friends in the game or to return a favor.	❯ Aesthetic Manipulations (feel bad for not helping team) [287], Social Obligation / Guilds [287], Players Feels Ashamed/Guilty [129], Reciprocity [287]
	Competition 🥽	❶ Foster envy and competitions between players.	❯ Competition [287]
Encourage Anti-Social Behavior 🥽	-	❶ Incentivize users' dishonest or harmful actions to gain benefits.	❯ Encourages Anti-Social Behavior [287]

Note. 🥽 denotes deceptive designs mentioned in the game-related literature [287, 129]. ⬡ denotes deceptive designs mentioned in VR-related literature [100].

Table 5.1 Continued. This table presents our *Deceptive Design Assessment Guide* and the source literature of themes and codes [89, 287, 129, 100]. This *Assessment Guide* served as the foundation of our identification of deceptive designs in the selected VR-based and computer-based games.

Theme/Subtheme	Code	Definition	Correspondence to Taxonomies from Literature
Theme 4: Interface Interference			
Manipulating Choice Architecture	False Hierarchy	Prioritize certain options, making it difficult to compare choices and potentially leading to unintended selections.	False Hierarchy [89], Anchoring Tricks (False Hierarchy) [287], Aesthetic Manipulations (bigger checkbox) [287], "Premium Value" or "Rare" Items [129]
	Visual Prominence	Highlight distracting elements, causing users to forget or lose focus on their initial intent.	Visual Prominence [89], Exciting Sound Effect [129], Aesthetic Manipulations (red "yes" button) [287], UI Colours/Animation [129]
	Bundling	Group products at a "special" price, potentially hiding individual costs and leading to uninformed purchases.	Anchoring Tricks (Discount Bundles) [287] Bundling [89], Bulk-buy Discount [129]
	Pressured Selling	Highlight or pre-select expensive options, potentially leading users to overlook more affordable choices.	Pressured Selling [89]
Bad Defaults	-	Set default options that benefit the company, forcing users to manually change settings to avoid privacy risks.	Bad Defaults [89], Accidental Purchase (expensive ones selected by default) [287], Aesthetic Manipulations (checkbox opt-in by default) [287]
Misclick	-	Exploit strategic button placement and absence of confirmation screen, leading to accidental actions.	Obscuring Reality [100], Perception Hacking (offset visual cue in cursor-jacking) [100], Accidental Purchase (accidental stray tap of the screen) [287]
Emotional or Sensory Manipulation	Adorable design	Exploit user preference for adorable design to make the game appealing, fostering trust in characters, and obscuring risks.	Cuteness [89], NPC is cute or very likeable [129], Hyperpersonalization (content tailored to preference of an individual) [100], Aesthetic Manipulations (Subconscious Associations) [287]
	Positive or Negative Framing	Hide or downplaying crucial information through visual cues, leading to biased or distracted decisions.	Positive or Negative Framing [89], Users Images Associated with Wealth [129], Aesthetic Manipulations (Toy with Emotions) [287]
	NPC/Narrative Manipulation*	Exploit self-satisfaction, sympathy, or reverse psychology to cause unintended actions.	Players Feel Good for Helping NPC [129], Sympathy/pity for NPC [129], Want to Prove NPC Wrong (to counter NPC's taunt) [129], Hyperpersonalization (idealized interaction partners) [100], Artificial Prosthetic Memory/Empathy-Based Manipulation [100]
	General Emotional Manipulation	Non-specific descriptions of emotional manipulation.	General Emotional Manipulation [129]
Trick Questions	-	Use confusing wording or double negatives to manipulate users' choices.	Trick Questions [89]
Choice Overload	-	Overwhelm users with too many options, hindering comparison and potentially causing them to miss important information.	Choice Overload [89]
Hidden Information	-	Obscure crucial details or disguising them as unimportant.	Hidden Information [89]
Language Inaccessibility	Wrong Language	Display crucial information in a foreign language, making it inaccessible to users.	Wrong Language [89]
	Complex Language	Use hard-to-understand words and sentence structures, hindering users' informed decisions.	Complex Language [89]
Feedforward Ambiguity	-	Create a gap between users' predicted result from the available information and the actual outcome of their actions.	Feedforward Ambiguity [89]
Theme 5: Distortion			
Cognitive Bias	Illusion of Mastery	Deceive players about their skill level, making them feel better than they actually are and encouraging more gameplay.	Illusion of Control (e.g., manipulated matchups, undisclosed random win chance) [287]
	Optimism and Frequency Biases	Exploit optimism bias, frequency bias, and clustering illusion to make players feel luckier and skilled, encouraging continued play.	Optimism and Frequency Biases [287]
	False Memory Implantation	Exploit users' memory flaw and source confusing to induce false memory and influence their behaviour.	False Memory Implantation [100]
	The illusion of objectivity	First-person experiences inherently biased by creator influence, creating a false sense of objectivity.	The illusion of objectivity in XR experience [100]

Note. *NPC = Non-Player Character. denotes deceptive designs mentioned in the game-related literature [287, 129]. denotes deceptive designs mentioned in VR-related literature [100].

Table 5.1 Continued. This table presents our *Deceptive Design Assessment Guide* and the source literature of themes and codes [89, 287, 129, 100]. This *Assessment Guide* served as the foundation of our identification of deceptive designs in the selected VR-based and computer-based games.

***Theme*/Subtheme**	**Code**	**Definition**	**Correspondence to Taxonomies from Literature**
Theme 6: Forced Action			
Nagging	-	Disrupt user focus with repeatedly unwanted interruptions to push actions they would rather avoid.	Nagging [89], Badges / Endowed Progress (red dot reminder of left off progress) [287], Prompted to Buy Robux [129], Aesthetic Manipulations (Over-the-top Feedback) [287]
Forced Continuity	-	Continuity traps users in unwanted subscriptions by making cancellation difficult and auto-renewal opaque.	Forced Continuity [89]
Forced Registration	-	Require account creation for tasks that shouldn't need it, potentially extracting unnecessary personal data.	Forced Registration [89]
Forced Communication or Disclosure	Privacy Zuckering	Trick users into thinking it's essential for the service, leading to overshare personal data.	Privacy Zuckering [89]
	Friend Spam	Exploit social connections by sending spam to users' contact lists and resulting in unwanted contact to other users.	Friend Spam [89], Friend Spam/Impersonation [287], Hyperpersonalization (recreate trusted people) [100]
	Address Book Leeching	Steal users' contact information under their false impression that only vital information will be collected.	Address Book Leeching [89]
	Social Pyramid	Push users into recruiting others by tying it to desired features.	Social Pyramid [89], Social Pyramid Scheme [287]
Gamification	Pay-to-Play	Initially advertised as free, later restricts core functionalities or progress unless players pay to bypass limitations (limited actions, timers, ads).	Pay-to-Play [89], Pay Wall [287], Pay to Skip [287], Recurring Fee [287], Real Money Spend Expected [129], Purchase Feels Part of Narrative [129]
	Pay to Win	Real-money purchases grant significant in-game advantages.	Pay to Win [287]
	Power Creep	Diminish obtained item values over time to drive new purchase.	Power Creep [287]
	Grinding	Force users into repetitive tasks to access features.	Grinding [89], Grinding [287]
	Random Rewards	Encourage users to spend money on chance-based rewards.	Variable Rewards [287], Gambling/LootBoxes [287], Gacha/lootbox/random [129], "Gambling" [129]
	Can't Pause or Save	Force users to continue playing before they can save progress.	Can't Pause or Save [287]
	Daily Challenges	Encourage players to revisit the game daily.	Daily Challenges [287]
	Playing by Appointment	Force players to adhere to the game's schedule.	Playing by Appointment [287]
	Wait To Play	Impose arbitrary wait times on players through in-game timers.	Wait To Play [287]
Sunk Cost Fallacy	Endowed Value	Trap users with their previous investment (time, money, effort).	Invested / Endowed Value [287]
	Endowed Progress	Exploit users' aversion to incompleted progression.	Badges / Endowed Progress [287]
	Waste Aversion	Set small differences between in-game currency and item costs, prompting additional currency purchases.	Must Buy More Robux (currency) Than Needed [129], Waste Aversion [287]
Attention Capture	Auto-Play	Auto-start videos, causing excessive or unwanted views.	Auto-Play [89]
	Interest Exploitation	Leverage users' interests to capture their attention.	Hyperpersonalization (idealized partners) [100]
Theme 7: Facilitation			
Low Barrier	Low Barrier Purchase	Minimize steps, and complexity during spending actions, encouraging impulsive purchases.	Purchasing Is Too Easy [129], Purchase Prompt is Immediate [129]
Infinite Treadmill	-	Continually expanding the game (e.g., new levels, new content).	Infinite Treadmill [287]
Theme 8: Other			
Complete the Collection	-	Exploit users' desires of completing game item collections.	Complete the Collection [287]
Data Fueled Manipulation	-	Capture extensive user data (movement, behavior, surroundings) enabling potential deanonymization and tailored manipulation.	Data Fuels Privacy Risks and Manipulation [100], Undesired Access and Data Use [100], Insecurity Worsen Manipulation [100]
Blurry Boundary	-	Photorealistic visual designs blur the lines between reality and ads, potentially misleading users about product quality.	Extreme Realism blurs the boundary between virtual and reality [100], Obscuring Reality [100], Persistent Exposure to Manipulation [100]

Note. denotes deceptive designs mentioned in the game-related literature [287, 129]. denotes deceptive designs mentioned in VR-related literature [100].

Throughout this process, we constantly compared definitions, descriptions, and examples of the same pattern across different sources, and challenged and refined our analysis based on our researchers' critical thoughts, interpretations, and expertise in deceptive design. Our research team collectively discussed the results to identify any potentially overlooked aspects of the analysis. To minimize complexity where appropriate, we merged variances of deceptive designs that shared similarities in their definition and examples. Overall, our *Assessment Guide* contained eight synthesized themes and 71 distinct deceptive design patterns, as summarized in Table 5.1.

To offer transparency in our interpretations [211], we provide a *Reflexivity Statement* in Appendix A to critically acknowledge the potential biases in our analysis from our researchers' background and experience, following the recommendations for qualitative research [164, 221, 287, 129].

5.3 Discussion and Conclusion

Building on our *Assessment Guide*, our next step is to validate, refine, and enhance its comprehensiveness through an analysis of real-world computer applications and commercially available immersive applications. We discuss our study in these areas in Chapter 6 and Chapter 7, which allowed us to understand how deceptive design manifests across these environments, explore how the unique properties of immersive technologies influence the effectiveness of deceptive tactics, and identify deceptions that may not exist in traditional 2D interfaces. In addition to examining design mechanisms, we also investigated user perspectives on immersive technologies, which we report in detail in Chapter 6 and Chapter 7. As we compared users' experiences with our findings on deceptive design, we developed a deeper understanding of how users perceive and experience deceptive tactics and how different manifestations shape user perceptions.

Chapter 6

A Preliminary Exploration on Deceptive Design in Immersive Environments

---

Suggested Citation:

Hadan, H., Sgandurra, S. A., Zhang-Kennedy, L., & Nacke, L. E. (2024). From Motivating to Manipulative: The Use of Deceptive Design in a Game's Free-to-Play Transition. *Proceedings of the ACM on Human-Computer Interaction, 8*(CHI PLAY), 1-31. https://doi.org/10.1145/3677074

6.1 Introduction

In this chapter, we take our first step towards addressing Objectives 3 and 4 through a mixed-method study that investigates the manifestation of deceptive design and users' perceptions, experiences, and responses in commercially available VR applications, compared to those observed in an exemplary computer application. As discussed in Chapter 3, much of the

existing literature relies on hypothetical scenarios, expert predictions, or controlled lab studies that take a broad view of immersive technologies without considering the distinct characteristics and properties of different immersive devices (e.g., [100, 133, 245]). Therefore, it is essential to conduct investigations that capture how deceptive design manifests within real-world VR applications. Such investigations can identify both deceptive strategies that migrate from non-immersive environments and those that may emerge based on the unique properties of immersive technologies. This also reveals context-specific risks that cannot be fully addressed through hypothetical or lab-based studies alone.

6.1.1 Motivation and Gaps in Existing Literature

Before examining deceptive design in immersive technologies, we first explore a baseline understanding of how deceptive patterns appear in traditional computer applications. Prior research has identified a wide range of deceptive design strategies employed in computer and mobile environments to influence user behavior and decision-making (e.g., [70, 177, 52, 127]). These tactics can have negative consequences on users' financial, social, privacy, and psychological well-being [287, 129, 205]. In response, both academic researchers and regulatory bodies have begun addressing these practices [89, 196, 62, 193], and several companies have faced legal and public scrutiny for their use of such tactics [66, 195, 41, 257]. For instance, the U.S. Federal Trade Commission (FTC) took action against Fortnite for using deceptive designs to encourage unwanted purchases and compromise user privacy [66]. Similarly, the European Consumer Organisation (BEUC) and the Office of Privacy Commissioner of Canada (OPC) have warned that user data collected in applications can be leveraged to enable further manipulative tactics [257, 196]. Although these issues have primarily been examined in the context of traditional digital platforms, research suggests that deceptive design strategies may also extend into immersive environments [27, 169, 11]. Moreover, the unique properties of immersive technologies, such as spatial display, realistic simulation, and sensory data collection, may also lead to novel forms of deceptive design [169, 134]. Therefore, as proposed in Chapter 3, it is critical to investigate how deceptive design patterns manifest in commercially available immersive applications, how

they compare to those in conventional platforms, and how emerging properties of immersive technologies can be exploited to implement new deceptive tactics.

6.1.2 Chapter Research Goal and Context

To explore how deceptive design manifests in both traditional and immersive environments, we conducted a preliminary analysis of three commercial applications. For traditional computer environments, we selected *Overwatch2* (OW2), a cross-platform first-person team-based shooter game, as a case study for our investigation of deceptive design in computer applications [103] (see Figure 6.1, right). In October 2022, OW2's business model transition led to the introduction of various deceptive design elements that sparked widespread criticism in online reviews[1], which provides an opportune moment to study how users experience and respond to deceptive design practices before and after their integration. In comparison to OW2, we chose two additional commercial VR applications: (see Figure 6.1, left and center): *Moss: Book II* (*Moss2*), a VR puzzle adventure game; and *Beat Saber*, a VR rhythm game. These games are selected because of their critical acclaim in the VR player community and significant player bases[2]. This comparative approach allowed us to examine how deceptive design tactics are adapted across environments, assess the impact on users, and serve as an initial validation of our *Assessment Guide* developed in Chapter 5.

As we discussed in Chapter 3, user perspectives are a valuable resource for understanding the impact of design mechanics [205, 232, 146]. Such perspectives offer valuable insight into practices that may not be explicitly illegal but still raise ethical concerns [83, 88]. Therefore, beyond analyzing application design mechanisms, we conducted an investigation of user perceptions and lived experiences. This allowed us to examine how users perceive and respond to certain mechanics that may be perceived as deceptive, unfair, or problematic.

[1]As of May 4, 2024, OW2 holds the sixth position on the list of worst games on Steam with 82% of negative reviews, resulted in an overall rating of "overwhelmingly negative". Currently, OW2 See: https://store.steampowered.com/app/2357570/Overwatch_2/ and https://steam250.com/bottom100

[2]As of May 10, 2024, *Beat Saber* has about 862,000 active players; *Moss Book: II* has been played by 33,000 players. See https://playtracker.net/insight/game/5.



Figure 6.1: Left: sample gameplay moment in *Moss2*, a VR puzzle adventure game where players guide a tiny mouse character through a fantastical world. Quill, the main character, gives the player a full-body hug, with her tiny arms wrapped tightly around the controller pointers. Center: sample gameplay moment in *Beat Saber*, a VR rhythm-based block-slashing game, when players are required to physically move left, right or squat down to avoid oncoming obstacles (semi-transparent walls). Right: sample gameplay moment in OW2, a first-person team-based shooter game, when players is using ability to heal (restore) the health of allies at the front by holding down the right-click on mouse.

For this, we address the following chapter research questions (RQ6.1-6.2):

RQ6.1) What deceptive design patterns are currently present in commercial computer and VR applications?

RQ6.2) How do users perceive and react to the deceptive design mechanisms in these applications?

6.1.3 Chapter Contributions

In this chapter, we outline our methodology and findings. Rather than assigning blame or criticism, our research seeks to learn from users to better understand how deceptive design manifests in computer and VR applications and how it affects user experience. Our work makes several **contributions**: *First*, we present the *VR Deceptive Game Design Assessment Guide*, which builds on established taxonomies to provide a standardized framework for identifying and categorizing deceptive tactics in immersive environments. This *Assessment Guide* can support future research, and immersive technology design, development, and regulation in conducting consistent evaluations. *Second*, through a Reddit analysis and an autoethnography method, we uncover how users perceive and respond to deceptive design, revealing that such tactics can lead to user frustration,

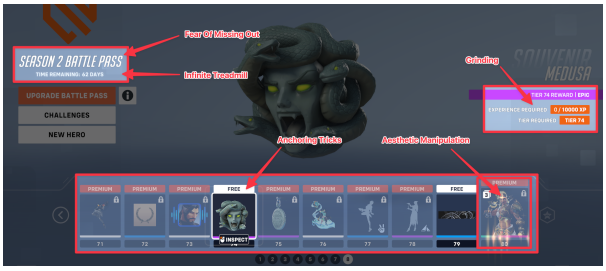


Figure 6.2: Battle Pass from OW2 season 2. Each level requires 10,000 XPs (*Grinding*) and rewards players with an item (*Adorable Design*). A total of 80 "premium" items are only for players who paid premium fee (*Bundling*). The progress resets every season [61] (*Fear of Missing Out* and *Infinite Treadmill*).

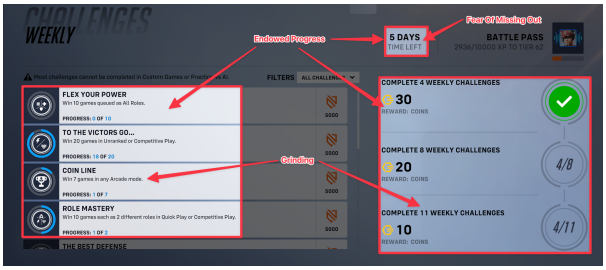


Figure 6.3: Weekly Challenges from OW2. The completion of each challenge offers 5,000 XPs (*Grinding*). Upon the completion of 4, 8, and 11 challenges, players can obtain 30, 20, and 10 OW coins (*Endowed Progress*). The progress resets every week (*Fear of Missing Out*).

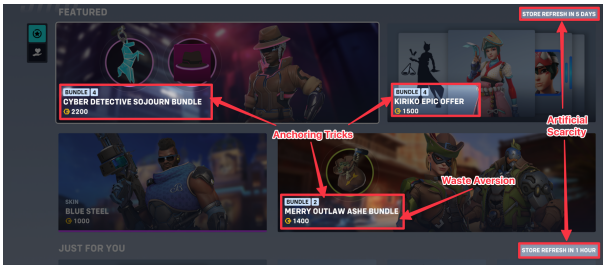


Figure 6.4: OW2 Game Shop from season 2 with bundles (*Bundling*) and "featured" items in a price that is different from amount of purchasable coins (*Waste Aversion*). Items refreshes periodically (*Countdown Timers*).

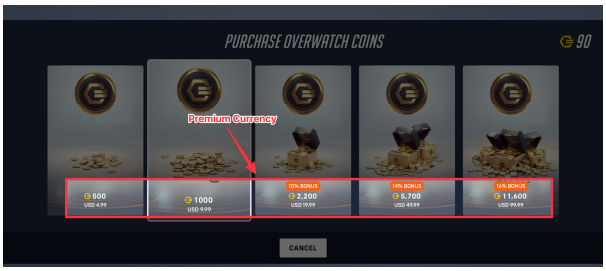


Figure 6.5: OW coins purchasable with real money (*Premium Currency*).

disappointment, and even discontinued engagement, which can negatively impact application sustainability and publishers' brand reputation. *Third*, our use of autoethnography offers a novel methodological perspective that can guide future research on immersive technologies, as it captures users' first-person live experiences of deceptive design in immersive contexts while preserving a researcher's expert knowledge in the analysis. *Fourth*, comparative analysis identifies various manifestations of deceptive designs across modalities, which suggests that VR's unique properties amplified the impact of emotional and sensory manipulations and presented a potential for more sophisticated manipulation in future VR applications.

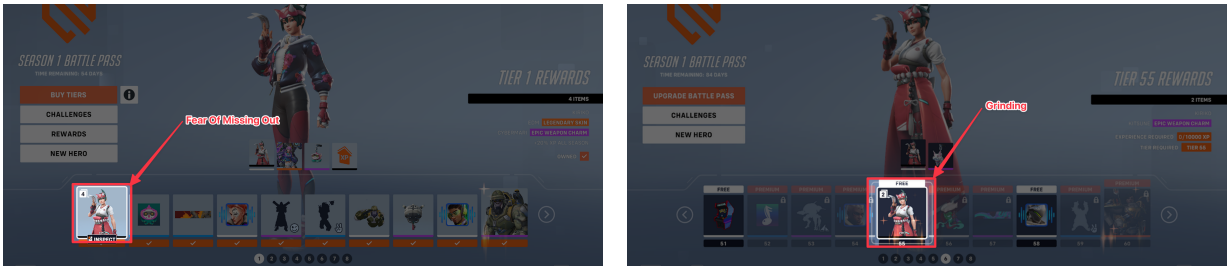


Figure 6.6: The new unlockable character from OW2 season 1. Players who have purchased the premium Battle Pass can unlock this character once they complete level 1. Other players can unlock this character once they complete level 55 (*Grinding*). Players who miss this opportunity will complete character-specific challenges in later seasons, a much lengthier and more difficult path of obtainment (*Fear of Missing Out*).

6.2 Methodology

Following established methods in the literature [171, 127, 52, 129], we adopted a two-phase approach to analyze the selected commercial VR and computer applications: (1) an analysis of design mechanics to identify those exhibiting deceptive design characteristics, and (2) a thematic analysis of user experiences and perceptions related to these potentially deceptive designs. The first phase examines each application as a structured system with a focus on the underlying rules and mechanisms that shape user interaction, while the second phase investigates how these mechanisms are interpreted and experienced by users [127]. For clarity, we use "design mechanisms" to refer to the rules that govern user interaction, and "design patterns" to denote recurring structures that implement these mechanisms [4].

6.2.1 Analyzing Design Mechanics in the Computer Application

Our analysis of the selected computer application (i.e., OW2) focused specifically on the design mechanisms introduced after its business model transition. We excluded mechanisms that were already present in its earlier versions to reduce the influence of habituation and long-term exposure on user self-reported responses [2]. Using the *Assessment Guide* developed in Chapter 5, we then systematically evaluated the design mechanisms and identified those that exhibited characteristics of deceptive design.

Data Collection

We recorded a 30-minute video capturing interactions with all OW2 interfaces and extracted multiple screenshots to document user interaction sequences. We sourced OW1 interface screenshots from the *Game UI Database*[3], *Interface In Game*[4], and recorded streams on *Youtube*[5] and *Twitch*[6]. A researcher with five years of experience in OW1 and OW2 reviewed the screenshots to ensure the comprehensive coverage of commonly used design mechanisms. We then *excluded* screenshots of shared mechanisms between OW1 and OW2. The remaining 62 screenshots were uploaded to Dovetail[7] for analysis.

Data Analysis

We analyzed the design mechanics using a deductive approach, guided by our *Assessment Guide* from Chapter 5. In a collaborative review, five researchers evaluated 62 screenshots and labeled them based on the patterns in the *Assessment Guide*. Drawing on prior research [52, 171], we coded the screenshots based on perceived issues in the design mechanisms—those that harm users' "best interests" while benefiting the game and publisher, rather than focusing on designer intent. This approach helped us identify deceptive design elements resulting from both intentional manipulation and unintended harmful outcomes. The researchers iteratively discussed and refined the labels until full consensus was reached. For each design mechanism, we began with the core interfaces and expanded the analysis to other related design elements encountered during interactions. Our process is illustrated in Section D.1. In total, we identified nine potentially deceptive design mechanisms with 14 deceptive patterns. Table 6.1 shows a summary of these OW2 design mechanisms, which formed the basis for our investigation into users' perceptions.

[3]Game UI Database. https://www.gameuidatabase.com/gameData.php?id=1341
[4]Interface In Game. https://interfaceingame.com/games/overwatch/
[5]https://www.youtube.com/
[6]https://www.twitch.tv/directory/gaming
[7]Dovetail — Qualitative Coding Platform. https://dovetail.com/

6.2.2 Analyzing User Perspectives on the Computer Application

The second part of our research focused on analyzing users' perceptions and experiences of the 14 potentially deceptive design mechanisms identified, using data from two subreddits: *r/Overwatch* and *r/Overwatch2*. This step helped mitigate the subjectivity in our design analysis and identify instances where users felt manipulated during interactions. We excluded Blizzard's official forums due to potential censorship or removal of controversial topics[8]. The two subreddits were selected for their large, active followings—*r/Overwatch* had over 4 million followers, and *r/Overwatch2* had more than 115,000, both ranking in the top 1% of all subreddits as of April 2023.

Data Collection

Using keywords related to deceptive design (as discussed in Chapter 2) and the nine potentially deceptive design mechanisms from Section 6.2.1, we created variations of search terms and performed iterative test searches on *r/Overwatch* and *r/Overwatch2*. This led to a final set of *63 search keywords* (listed in Section D.2), which were used to retrieve data via a Python script with the Reddit API (PRAW[9]). Data was collected from October 4, 2022, to April 27, 2023, resulting in 64,042 candidate posts. After eliminating duplicates, posts marked as "[deleted]" or "[removed]", and those containing irrelevant images or videos, we retained 22,575 posts. To avoid data over-saturation and to prioritize valuable content, we excluded posts with a Reddit score < 5[10]. We also excluded posts discussing general feelings of manipulation or deception without reference to specific design mechanisms, as these posts lacked sufficient details for analysis. Our final dataset contained $n = 346$ highly relevant and highly rated posts.

[8]This is evident by several Reddit posts where creators assert that they were "silenced" for discussing their experience with Blizzard support.

[9]PRAW 7.7.1 Documentation. https://praw.readthedocs.io/en/stable/

[10]Reddit score, or "submission score," is the difference between upvotes and downvotes on a Reddit post. For instance, if five users upvote and three users downvote a post, its score would be 2. See: https://www.reddit.com/wiki/faq/

Qualitative Data Analysis

We analyzed the Reddit posts on Dovetail. Three researchers conducted an iterative inductive *Thematic Analysis* [39], focusing on emergent themes rather than the keywords used for data retrieval. First, the researchers reviewed the posts to familiarize themselves with the data. Then, each independently open-coded 10% of the posts (35 posts). In subsequent meetings, they discussed the codes, resolved conflicts, and developed an initial codebook. The coders continued weekly meetings for 10 weeks to refine the codebook, ensuring all posts were coded, no new codes were developed, and conflicts were resolved. Finally, the researchers collaboratively developed themes and sub-themes, presented in Table D.5.

6.2.3 Autoethnographic Analysis of Deceptive Design in VR Applications

Drawing from HCI, deceptive design, and security and privacy research (e.g., [127, 136, 64, 268]), we employed an autoethnographic approach to evaluate the selected VR applications. This method positions the researcher as both the "protagonist" and observer and enables a first-person engagement and understanding of the virtual environment [211]. Immersive technologies can embed deceptive design elements that persist over time and gradually fade from user awareness [133, 100], making them particularly challenging to detect through conventional evaluation methods. Autoethnography offers a valuable methodology to address this issue by allowing researchers to experience these environments directly, document potentially manipulative strategies as they emerge, and critically reflect on their own perceptions and assumptions over time [211, 5]. The combination of extended user engagement and structured introspection makes autoethnography a powerful method for analyzing deceptive design practices in immersive environments.

Data Collection

The lead researcher, H. Hadan, with expertise in deceptive design, VR, and immersive technologies, was fully immersed in the selected VR applications to systematically document

diary entries reflecting on moments where design mechanics appeared to employ deceptive patterns or result in manipulative experiences. *Moss2* was completed over nine days with approximately eight hours of use and nine diary entries. *Beat Saber* was explored over ten days, generating 18 hours of use and nine diary entries. Each application was used until no new design mechanics or insights emerged, following the principle of saturation. All VR sessions were recorded using the Meta Quest 3 headset's built-in screen recording. In total, 24 diary entries were created and organized using Miro[11] to capture detailed observations, supported by screenshots from the recorded sessions. These entries and recordings were then uploaded to Dovetail for thematic analysis.

Data Analysis

We conducted data analysis iteratively alongside collection to refine our approach to documenting diary entries. We noticed that our early diary entries consistently focused on how deceptive design manifested, the contexts in which it appeared, and its impact on the immersive experience. We therefore structured our subsequent entries into two parts: (1) the researcher's experiences, reactions, thoughts, and feelings when encountering specific design elements, and (2) reflections on the possible presence and context of deceptive design. An example diary entry is provided in Section D.4.

Given the autoethnographic nature of the study, we applied a *deductive reflective thematic analysis* method [39], which supports personal and reflexive insights while maintaining theoretical grounding [211, 64, 268]. To enhance transparency in our analysis [211], we provide a *Reflexivity Statement* in Appendix A, following qualitative research guidelines [164, 221]. Our analysis involved three stages. First, the researcher reviewed the data based on our *Assessment Guide*, focusing on potential deceptive design elements. Second, diary entries and supporting screenshots were deductively coded, informed by the researcher's critical reflections and domain expertise. Third, the research team collaboratively reviewed the results for additional interpretations or insights.

[11] Miro—the Virtual Workspace for Innovation. https://miro.com/

6.2.4 Ethical Considerations

Our analysis was conducted by researchers not considered "human subjects" [31, p. 14]. n subjects" [23, p. 14]. Reddit data was drawn from two public subreddits that require no registration and are considered "publicly available" content [31, p. 17]. To protect post creators' anonymity, we excluded their identifying information, removed subreddit names, and paraphrased quotes to avoid traceability. Our autoethnographic analysis focused on single-player modes to avoid involving others without consent. For OW2, where multiplayer interaction is required, we analyzed only H. Hadan's single-user experience and excluded any references to other users. Thus, deceptive designs relying on social relationships were excluded from our analysis due to privacy and ethical considerations.

6.3 Findings

We present our analysis of design mechanisms and user perspectives, and explore how deceptive design strategies manifest and vary between computer and VR applications.

6.3.1 RQ6.1: Deceptive Design Patterns and User Impacts in the Computer Application

We identified six OW2 design mechanisms introduced after the business model transition that exhibited characteristics of 14 deceptive design patterns. Notably, the Social Obligation pattern was revealed through our analysis of user perspectives shared on Reddit, but was not apparent in our design mechanisms analysis. As a design mechanism may demonstrate multiple deceptive patterns and a deceptive pattern may appear across various design mechanisms, we organize our findings based on the user impacts these mechanisms produce. A brief description of these mechanisms and corresponding deceptive patterns is provided in Table 6.1 and we include detailed codebooks in Section D.5. For clarity in the paragraphs below, design mechanisms are in monospace font (e.g., `Battle Pass`), deceptive patterns

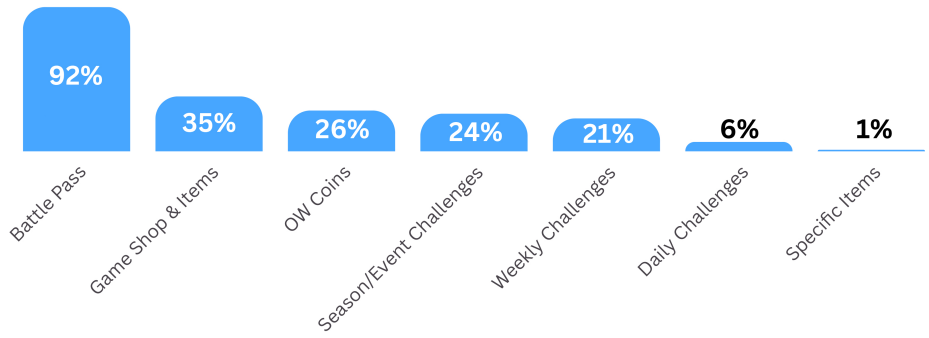


Figure 6.7: Percent of Reddit posts that mentioned each OW2 design mechanic.

are in title-case italics *italics* (e.g., *Grinding*), descriptions directly from the application are in quotation marks, and Reddit excerpts in *italics* and quotation marks.

Time-sinking experiences.

We found several design mechanisms with deceptive patterns that intended to encourage users' prolonged and repeated engagement [287]. For example, `DAILY/WEEKLY/SEASONAL CHALLENGES` and `Battle Pass` demonstrated the characteristics of `Grinding`, `Infinite Treadmill`, and `Countdown Timers`. As shown in Figure 6.2 and Figure 6.3, these mechanisms require regular participation (i.e., daily, weekly, or seasonally) to complete time-limited tasks, with progress frequently reset to force users to accomplish the never-ending goals. Within the `Battle Pass`, a `NEW CHARACTER` is available every two seasons (see Figure 6.6). Users without a premium `Battle Pass` must grind to a specific tier (e.g., tier 55) or complete post-season challenges to unlock the character, reinforcing the characteristic of `Grinding` pattern. The `DOUBLE XP WEEKEND` mechanism reflected the `Playing-by-Appointment` pattern, as it prompts user engagement during limited time windows.

Our Reddit analysis confirmed the perceived impact of these mechanisms. As shown in Figure 6.7, 92% of posts expressed frustration with the `Battle Pass` and the `NEW CHARACTER` it offers. Users described it as the worst among comparable free-to-play systems, citing a *"extensive 56-hour grinding"* to complete all 80 tiers. Many posts criticized on the locking of the `NEW CHARACTER`, a *"core game element"* behind such an intensive

Table 6.1: This table presents the 24 deceptive design patterns we identified in *Overwatch2* (OW2), *Beat Saber* (BS), and *Moss Book: II* (*Moss2*) based on our *Assessment Guide* (see Chapter 5). Fourteen patterns from in OW2 and 14 patterns across the two VR games. See Section D.5 for specific game mechanics associated with each deceptive pattern and corresponding synthesized diary entries.

***Theme*/Subtheme**	**Code**	**Description from *Assessment Guide***	**OW2**	**BS**	**Moss2**
Theme 1: Sneaking					
Hiding Information	Reference Pricing 🎮	Include a price-inflated item or a poorer-quality item with same price, make a current price seem ideal.	☑	-	-
Theme 2: Obstruction					
Creating Barriers	Price Comparison Prevention	Hide information or block copying/pasting, make it difficult to compare prices across vendors.	-	☑	-
	Intermediate Currencies 🎮	Hide the real price behind a virtual currency, make informed purchase decisions difficult.	☑	-	-
Theme 3: Social Engineering					
Social Proof	Parasocial Pressure	Exploit users' trust in celebrities or other entities with inauthentic endorsements to influence decisions.	-	☑	-
Urgency	Countdown Timers 🎮	Create urgency with fake countdown timers.	☑	-	-
	Limited Time Message 🎮	Create urgency with fake limited-time offers.	-	☑	-
	Fear of Missing Out (FOMO)	Exploit anxiety about missing exciting or valuable experiences.	☑	-	-
Personalization	Social Obligation 🎮	Create a sense of obligation to avoid letting down friends in the game or to return a favor.	☑	-	-
Theme 4: Interface Interference					
Manipulating Choice Architecture	False Hierarchy 🎮	Prioritize certain options, make it difficult to compare choices.	☑	☑	-
	Visual Prominence 🎮	Highlight distracting elements, causing users to forget or lose focus on their initial intent.	-	☑	-
	Bundling 🎮	Group products at a "special" price and hide individual costs.	☑	☑	-
Emotional or Sensory Manipulation	Adorable Design 🎮 ⬡	Exploit user preference for adorable and appealing design, foster trust in NPCs* and obscure risks.	☑	☑	☑
	NPC/Narrative Manipulation 🎮 ⬡	Exploit self-satisfaction, sympathy, or reverse psychology to cause unintended actions.	-	-	☑
	Trick Questions	Use confusing wording or double negatives to manipulate users' choices.	-	☑	-
	Hidden Information	Obscure crucial details or disguising them as unimportant.	-	☑	☑

*NPC = Non-Player Character.

🎮 denotes deceptive designs mentioned in the game-related literature [287, 129].

⬡ denotes deceptive designs mentioned in VR-related literature [100].

Table 6.1 Continued. This table presents the 24 deceptive design patterns we identified in *Overwatch2* (OW2), *Beat Saber* (BS), and *Moss Book: II* (*Moss2*) based on our *Assessment Guide* (see Chapter 5). Fourteen patterns from in OW2 and 14 patterns across the two VR games. See Section D.5 for specific game mechanics associated with each deceptive pattern and corresponding synthesized diary entries.

***Theme*/Subtheme**	**Code**	**Description from *Assessment Guide***	**OW2**	**BS**	**Moss2**
Theme 5: Distortion					
			-	-	-
Theme 6: Forced Action					
Forced Communication or Disclosure	Privacy Zuckering	Trick users into thinking it's essential for the service, lead to overshare personal data.	-	☑	-
Gamification	Pay-to-play 🎮	Restricts core functionalities or progress unless players pay to bypass limitations.	☑	☑	-
	Power Creep 🎮	Diminish obtained item values over time to drive new purchase.	-	☑	-
	Grinding 🎮	Force users into repetitive tasks to access features.	☑	-	-
	Can't Pause or Save 🎮	Force users to continue playing before they can save progress.	-	-	☑
	Playing by Appointment 🎮	Force players to adhere to the game's schedule.	☑	-	-
Sunk Cost Fallacy	Endowed Progress 🎮	Exploit users' aversion to incompleted progression.	☑	-	-
	Waste Aversion 🎮	Set small differences between in-game currency and item costs, lead to additional currency purchases.	☑	-	-
Theme 7: Facilitation					
Infinite Treadmill 🎮		Continually expand the game (e.g., new levels, new content) so it never ends.	☑	-	-

🎮 denotes deceptive designs mentioned in the game-related literature [287, 129].

⬡ denotes deceptive designs mentioned in VR-related literature [100].

progression system. Furthermore, 24% of posts discussed issues with `SEASONAL CHALLENGES`, particularly the first event following the business model transition. `WEEKLY CHALLENGES` appeared in 21% of posts, with users highlighting the difficulty and low coin rewards. Another 6% noted `DAILY CHALLENGE`, expressing frustration with the need to log in daily to gain experience points for the `Battle Pass` progression. Although `WEEKLY CHALLENGES` allowed the accumulation of OW coins, casual players perceived that an estimated 32 weeks of constant grinding to get a Legendary skin was a *"huge ask"* for their time. `SEASONAL CHALLENGES` further contributed to user dissatisfaction as it requires them to play unfamiliar roles or complete tasks in limited-time modes. Overall, many users felt trapped in repetitive cycles, describing the experience as tedious and obligatory rather than enjoyable.

"Why limit currency rewards to weekly challenges? People don't have the time to complete most of them, and even finishing one is a lot for casual players."

— *Reddit post 192*

Money-sinking experiences.

Our analysis identified multiple monetary deceptive design patterns within OW2 design mechanics that aim to get players spending more than they intend [287]. For example, the `Battle Pass` mechanism exhibited `Bundling` and `Pay-to-Play` patterns. Users who purchase a premium `Battle Pass` are incentivized to grind through its content before the season ends to maximize its value. To accommodate different user behaviors, OW2 allows users to either purchase tiers directly or invest time to progress. The inclusion of 80 items within 80 tiers for a $10 USD premium fee creates a perception of value, as individual purchases through the shop would cost significantly more.

The `IN-GAME SHOP` (see Figure 6.4) mechanism further employed `Bundling`, `Reference Pricing`, `Countdown Timer`, and `Waste Aversion`. Its rotating inventory creates urgency, encouraging impulsive purchases. Bundles placed next to individually priced items enhance perceived savings, while bundle prices are also priced differently than purchasable OW coins (see Figure 6.5), resulting in leftover coins and leading players to buy more. This `Premium Currency` establishes an exchange rate with real money, hiding the true prices of items.

Reddit posts supported these findings. Many premium `Battle Pass` buyers felt pressured to play excessively to avoid wasting their purchase. While the `Battle Pass` includes limited free rewards (see Figure 6.2), many users reported feeling that meaningful progress required buying the premium version. In addition, 35% of Reddit posts raised concerns about the item pricing within `IN-GAME SHOP`. An additional 26% mentioned frustrations with `OW COINS`, calling the pricing *"insane,"* compared to other free-to-play systems. Users noted significant price hikes. For example, an animation that once cost 250 coins now costs 750. Paying $19 USD for a skin previously earned through gameplay was viewed as

exploitative. Blizzard's 2022 fourth-quarter financial report proves that these tactics are financially successful.[12]

> *"Shop prices are ridiculous. I don't understand why they don't make skins more affordable and accessible instead of charging players $20 for each."*
>
> — *Reddit post 322*

Social consequences.

Our analysis identified that `DAILY/WEEKLY/SEASONAL CHALLENGES`, the `Battle Pass`, and the `NEW CHARACTER` further demonstrated `Fear of Missing Out` (FOMO). However, insights from Reddit posts revealed that users often felt discouraged from engaging with these mechanisms due to their repetitive nature, high difficulty, and underwhelming rewards. For example, multiple posts criticized the limitation of earning XP from only the first three `DAILY CHALLENGES`, which hindered progress and increased frustration. Users also described the 60 `OW COINS` earned from `WEEKLY CHALLENGES` as *"pathetic"* and *"abysmal"* compared to the price of `IN-GAME SHOP` items. In contrast to earlier versions where users could earn skins through gameplay, the `HALLOWEEN EVENT CHALLENGE` now offered only minor rewards such as weapon charms, voice lines, and sprays (see Section D.3 in Appendix), leading many to express disappointment over the *"little reward for the effort required."*

From our analysis of Reddit posts, we further found the `Social Obligation/Guilds` pattern, as users frequently felt social pressure for unlocking the `NEW CHARACTER`, especially when teams expected them to use it in response to opponents.

> *"I can easily foresee a time when my team would blame me of not investing enough money or time to unlock a character."*
>
> — *Reddit post 279*

[12] Blizzard 2022 Financial Report." https://investor.activision.com/news-releases/news-release-details/activision-blizzard-announces-fourth-quarter-and-2022-financial

Psychological impacts.

Several design mechanisms leveraged psychological tactics [287]. For example, the `Battle Pass` exhibited characteristics of `False Hierarchy` and `Adorable Design`, as it offers an exclusive, visually enhanced mythic skin at tier 80 to premium users (see Figure 6.2). In addition, the `DAILY/WEEKLY/SEASONAL CHALLENGES` and the `Battle Pass` also demonstrated `Endowed Progress`, as they create progressions that are difficult to abandon. Non-premium `Battle Pass` users rarely receive lower-quality items that are displayed alongside premium-only items, which increases the pressure to upgrade. However, Reddit posts revealed user dissatisfaction with these mechanisms. Many users felt that the time, money, and cognitive effort invested were not adequately compensated. Rewards were frequently described as *"random"* and *"unsatisfactory,"* compared to the grind. Since most items are character-specific, receiving a reward for an infrequently used character felt unrewarding.

Users motivated by collection completion also expressed frustration. While the `Complete the Collection` pattern was used in OW1, our analysis of Reddit posts indicated that the current reward system amplifies its psychological effects. Users calculated that it would take up to 326 years of grinding or $10,200 USD to complete collections. Many posts also criticized predatory marketing tactics. These included starting with inflated prices and later reducing them to simulate responsiveness, creating urgency, and prompting impulse purchases. The `GAME SHOP` was called out for *"fake"* bundles containing items never sold individually, forcing users to buy entire bundles for one desired item. Similarly, *"Fake"* discounts were reported on items never actually sold at full price. Users argued that such tactics violated consumer protection regulations in several countries. Some users reported losing interest in cosmetics altogether, preferring default options due to unfair pricing and low item quality. Others described feeling embarrassed using expensive skins because the $19 USD price tag diminished their perceived appeal. The overall lack of valuable rewards undermined user enthusiasm and led many to question if the application is truly free-to-play, with several posts stating that free users were left with only "crumbs from the plate."

> *"Lets be honest, nobody envies the loser who spent money on a bad deal."*
>
> — *Reddit post 9*

6.3.2 RQ6.2: What deceptive design patterns are currently implemented in commercial VR games?

We found that *Moss2* and *Beat Saber* shared similarities in deceptive design patterns (see Table 6.1). Both used emotional and sensory manipulation (e.g., `Adorable Design`) with lovable character designs, eye-catching visuals, and vibrant map environments to create a strong emotional attachment to the game world, potentially leading to longer play sessions and in-game purchases that users may not have otherwise considered. Both games also used `Hidden Information` tactics through the fully immersive nature of VR and intense and deeply engaging gameplay. In *Beat Saber*, the absence of a progress bar could be frustrating for users, as they have to replay the entire song after failing and cannot locate specific parts where they fail. The intensity of gameplay could lead users to lose track of time and unintentionally extend the duration of play. In *Moss2* a progress indicator (`Stained Glass Windows`) is subtly integrated into the background map environment. This could cause users to completely miss its existence. As a result, users can feel lost in the engaging storyline and interactive gameplay, and continuously playing without a sense of progress. Moreover, *Beat Saber* and *Moss2* use `Complete the Collection` to fuel users' desire for completion. For instance, in *Beat Saber*, acquiring all songs in the player's favorite music packs could lead to unintentional overspending of money. Similarly, *Moss2* has collectible scrolls and character-enhancing armors. While the process of discovering these items by repeatedly revisiting completed maps can produce a sense of achievement and a thorough game experience, it could also lead to extensive playtime beyond what is necessary to enjoy the core game.

We also found that *Beat Saber*'s `Song Purchase System` incorporated `Price Comparison Prevention` that inhibits users from comparing the prices of songs and music packs, `Limited Time Message` and `Bundling` that encourage impulse purchases, `Visual Prominence` that attracts users' attention to *"buy music pack"* entirely instead of buying an individual song, and `Privacy Zuckering` that requires users to provide their payment information before displaying the prices of songs and music packs. This design compels users who are simply trying to check the price or are undecided about purchasing to provide their

payment information first, and may lead to surprise or frustration when they discover the actual prices afterward. On the other hand, *Moss2* has largely used deceptive game design patterns that encourage extended playtime and emotional investment from users, including `NPC/Narrative Manipulation` that attracts users with its VR-unique interactive elements, such as allowing users to *"pet," "hug," "high-five"* with main characters (see Figure 6.1) and protect them in battles. While VR technology's limitations prevent a truly tactile experience, the animation of *"hugging"* the player's controller pointers effectively conveys the warmth and gratitude. The main character's sign language communication added another layer of emotional bond and made users feel like they are a part of the adventure and not just outside observers. Interestingly, while *Moss2* incorporated `Can't Pause or Save` tactic to keep users continuously play until designated save points, this tactic clashed with the limited VR headset battery life and can frustrate users with significant loss of progress due to a dead battery. We include the detailed descriptions of patterns identified from VR games, with synthesized diary entries, in Table 6.1.

6.4 Discussion

Our analysis of design mechanisms and user perceptions across computer and VR applications revealed the manifestation of deceptive design practices and their impacts on users in both environments. The deceptive design patterns we identified largely aligned with user-reported experiences, which affirms the comprehensiveness of our *Assessment Guide*. For example, deceptive patterns such as `Grinding`, `Countdown Timers`, and `Adorable Design` were evident in both the design mechanisms analysis and user frustrations (see Table 6.1). Although our *Assessment Guide* captured most patterns, user perspectives revealed subtle dynamics like social pressure that were not observable through design mechanisms. This indicates the need to integrate user perspectives alongside design inspection to fully understand the psychological and social consequences of deceptive design.

Notably, our findings revealed that the same design patterns can lead to different user experiences in VR compared to computer-based environments. A key distinction lies in how

users interact with these digital environments. As shown in Table 6.1, while OW2, *Beat Saber*, and *Moss2* all incorporated `Adorable Design` and `Complete the Collection`, their impact varied across platforms. In OW2, visual effects such as cosmetic skins and cute weapon decorations are limited to a 2D screen, with user interaction occurring through a mouse, keyboard, or controller. This setup creates a clear separation between the user and the application environment. In contrast, *Beat Saber* and *Moss2* enable a more dynamic and immersive interaction with VR-unique properties. For instance, *Moss2* uses haptic feedback through VR controllers and spatial 3D visuals to enhance user engagement. Users can physically lean forward or look around corners to explore the virtual environment and locate hidden items. This form of discovery offers a more embodied experience than OW2's badge- or message-based collectible system on flat 2D screens.

Although *Beat Saber* also adopts a first-person perspective similar to OW2, unlike the static screen of OW2, users in *Beat Saber* are fully immersed in its unbounded display. Users must actively move their bodies to slash blocks, dodge obstacles, and turn to interact with elements from multiple directions (see Figure 6.1). This full-body involvement creates a stronger sense of presence than what is typically possible in traditional computer applications.

Literature has hypothesized that strong player attachment to NPCs can be exploited to encourage in-game purchases [129]. Although we did not observe such practices in the two VR games analyzed, the continuous evolution of immersive technologies and deceptive strategies may create opportunities for advanced exploitation. The enhanced emotional bounding and strong sense of presence enabled by VR immersion can be readily leveraged not only for monetization but also for other forms of user manipulation in the future.

Despite these differences, several deceptive design patterns embedded in the design mechanics appear consistently across VR and traditional computer applications. For example, OW2 and *Beat Saber* both used `Limited Time Message`, `Countdown Timer`, `Bundling`, and `Pay-to-play`. The commonalities are because many deceptive design patterns remain heavily reliant on 2D interfaces even within VR's 3D environments, and therefore, have no significant variations across modalities.

Lastly, mechanisms such as `NPC/Narrative Manipulation`, `Trick Questions`, and `Power Creep` and `Can't Pause or Save` were observed in both *Beat Saber* and *Moss2* but not in OW2. We believe it is due to differences in application genre rather than the platform.

6.4.1 Limitations

Our study has several limitations. First, one of our researchers had six years of experience with Overwatch, which helped identify deceptive design and its impact on users, but may have introduced bias. Second, we analyzed application design mechanisms and Reddit discussions during Overwatch 2's Seasons 1 and 2 (Oct-Dec 2022). While this provided insight into users' immediate reactions after the implementation of deceptive design mechanics, we acknowledge that user perceptions may change alongside the game's evolution. Third, our data came exclusively from Reddit, a platform with a skewed demographic (as of March 2024: 75% US, 63.6% male, 44% aged 18-29) [243]. To mitigate this, our research team included diverse gender and age perspectives, but our findings may still not generalize to the broader user population. Fourth, our dataset leaned toward negative opinions. While these posts reflect major trends within the studied communities, as evident by their high Reddit scores, prior research suggests user perceptions of deceptive design can vary [76, 287, 214]. Fifth, our data collection relied on keyword searches informed by our *Assessment Guide* and deceptive design literature (e.g., [287, 163]). However, this approach may have overlooked posts where users were unaware of manipulation or indifferent to it. Lastly, we acknowledge that there might be deceptive techniques that remain undetected by both researchers and users. Our *Assessment Guide* contributes to the ongoing discourse and encourages further research to expand the understanding and classification of deceptive design.

6.5 Conclusion

Our exploration validated the comprehensiveness and applicability of our *Deceptive Design Assessment Guide* in supporting the analysis of deceptive practices across both VR and

traditional computer applications. This *Assessment Guide* also offers a standardized framework that can inform future research, design, and policy efforts targeting deceptive tactics in digital environments. Our autoethnography methodology also demonstrated the value of first-person insights into users' lived experiences in uncovering subtle and experiential aspects of deceptive design that may not be observable through design mechanisms analysis alone. Notably, our preliminary exploration into VR applications suggests that VR's unique properties amplified the impact of emotional and sensory manipulations and presented a potential for more sophisticated manipulation in future VR applications. In Chapter 7, we expand on these observations through a deeper investigation of deceptive design in VR, using our *Assessment Guide* as a foundation.

Chapter 7

A Structured Investigation of Deceptive Design in Immersive Environments

---

Suggested Citation:

Hadan, H., Valiquette, M., Nacke, L. E., & Zhang-Kennedy, L. (2025). Immersive Invaders: Privacy Threats from Deceptive Design in Virtual Reality Games and Applications. Accepted and will be published at the *ACM SIGCHI Conference on Computer-Supported Cooperative Work & Social Computing (CSCW) 2025* (pp. 1-30).

7.1 Introduction

This chapter further addresses our Objectives 3 and 4 through a mixed-method approach that investigates how deceptive design manifests specifically in privacy communication and decision-making mechanisms (e.g., settings, and permission prompts) within VR applications. We examine both deceptive strategies that migrate from non-immersive environments and

those that may leverage the unique properties of immersive technologies. We also explores how these patterns affect VR users' understanding of privacy information and their ability to make informed privacy decisions.

7.1.1 Motivation and Gaps in Existing Literature

Virtual Reality (VR) introduces new opportunities for manipulative tactics through immersive visual, audio, and haptic feedback that disconnects users from the physical world [241]. While existing research on deceptive design in VR primarily relies on hypothetical scenarios, expert predictions, and controlled lab studies, it often overlooks the unique features of commercially available VR devices (e.g., [100, 133, 245]). User awareness, perception, and experiences of deceptive design in VR also remain underexplored. Furthermore, existing studies have primarily concentrated on temporal and monetary manipulation, with limited attention to privacy issues (e.g., [129, 205]). Users face privacy harms when deceptive tactics such as bad defaults, mandatory registrations, and social pyramid structures impair their decision-making and lead to unintended data disclosures [196, 22, 97, 87]. As discussed in Chapter 4, users are mostly unaware of the granular and often intangible data collection practices enabled by immersive technologies, many of which are uncommon in non-immersive systems. Our Chapter 3 further highlights that delivering immersive experiences requires extensive data gathering and information sharing to support core functionalities [20], which in turn elevates privacy risks and enables targeted manipulation based on people's preferences and vulnerabilities [169]. As commercial games and social platforms continue expanding into immersive environments, it is essential to investigate how deceptive practices in VR evolve and what implications they pose for user privacy.

7.1.2 Chapter Research Goal

In this chapter, we examine how deceptive design manifests in the privacy communication and interaction mechanisms of 12 top-rated commercial VR applications [11], with special attention to how these designs obscure or distort users' understanding of privacy information

and undermine their ability to make informed privacy decisions [97]. Such insights are essential for mitigating VR deceptive design and contribute to safer and privacy-respecting VR environments. With these objectives in mind, we address the following chapter research questions (RQ7.1-7.2):

RQ7.1) To what extent do commercial VR applications implement deceptive that might influence users' privacy decisions?

RQ7.2) To what extent are VR users aware of, perceive, and feel concerned about how deceptive design in VR threatens their personal privacy?

Building on deceptive design and privacy research [87] and our methodology in Chapter 6, we adopted a two-phase approach. We first conducted an autoethnographic evaluation of 12 VR apps to examine how deceptive design manifests in immersive environments. We then conducted a scenario-based online survey with $N = 424$ VR users to assess their awareness, perceptions, and experiences with deceptive design scenarios identified in the autoethnographic study.

7.1.3 Chapter Contributions

This chapter details our methodology and core findings. Our research makes the following **contributions**: *First*, we show that deceptive patterns commonly found on 2D platforms directly migrate into VR's registration and subscription processes, consent interactions, privacy settings, quality-of-life (QoL) features, and notification mechanisms. Although these patterns still heavily rely on 2D-style interfaces within the 3D space of VR, their presence in the privacy communication and interaction mechanisms of VR apps demonstrates how traditional manipulative tactics are being adapted in immersive environments. These tactics are amplified, not directly enabled, by VR-unique properties, with increased harm to users' privacy. *Second*, we provide empirical evidence from an online survey that users sense manipulation even without explicit knowledge of deceptive design. This can deter adoption and hints at a potential backlash against VR developers and publishers (as

discussed in Chapter 6). *Third*, we provide examples of how VR users' familiarity with deceptive design in non-VR privacy settings and trust in certain brands can lower their guard in immersive VR contexts. *Fourth*, we identify a paradox where participants remain aware of manipulation but still surrender personal privacy. This is symptomatic of a wider resignation across digital platforms. Based on these results, we make recommendations for the ethical design of applications in immersive environments that balance user experiences with strong privacy protections to guide future research, and immersive technology design, development, and regulation in creating privacy-preserving design strategies for the evolving immersive technologies.

7.2 Methodology

We adopted a two-phase methodology: (1) an autoethnographic evaluation of privacy communication and interaction design mechanisms in VR apps, and (2) a scenario-based online survey with $N = 424$ VR users on Prolific[1], focusing on their experiences with seven selected VR privacy mechanisms from the 12 applications, which incorporate 11 deceptive design patterns identified in phase (1).

7.2.1 Research Context

We analyzed the privacy communication and interaction mechanisms of 12 top-rated VR apps. These applications represent the most highly recommended[2], top-rated[3], and widely downloaded products on major VR platforms[4]. Spanning genres from puzzle and adventure to productivity, fitness, and social interaction, these applications offer a broad perspective on privacy practices across various VR contexts. This selection helps us identify

[1]Prolific. https://www.prolific.com/

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

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

[4]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/

Table 7.1: Summary of Selected Virtual Reality (VR) Applications.

Title (acronym[a])	Genre[b]	Publisher	Year	Description	Platforms[d]	Hours	Diaries
Beat Saber (BS)	Rhythm	Beat Games	2019	Players slash incoming beat cubes to the rhythm of the music.	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.	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.	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.	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.	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.	PCVR, CVR, SAVR	31	8

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 stand-alone 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) [196] 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 [46].

deceptive design patterns affecting mainstream VR users. The selected applications are available on multiple VR platforms and are widely accessed by millions of users worldwide. Table 7.1 summarizes the VR apps' publisher, initial release year, core design mechanics, and supported platforms.

Table 7.1 Continued. Summary of Selected Virtual Reality (VR) Applications.

Title (acronym[a])	Genre[b]	Publisher	Year	Description	Platforms[d]	Hours	Diaries
The Climb 2 (CLIMB)	Sports	Crytek	2021	Users climb mountains, skyscrapers, and caves, and find their way to the top and enjoying the views.	PCVR, SAVR	9	4
VRChat (CHAT)	Social	VRChat Inc.	2019	Users create avatars, explore diverse virtual worlds, and interact with others.	PCVR, SAVR	4	3
Meta Horizon Worlds[f] (HRZ)	Social	Facebook	2020	Users explore, build, and interact in immersive, user-created worlds.	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.	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.	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.	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 stand-alone 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) [196] 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 [46].

7.2.2 Design Mechanics Evaluation

Following Chapter 6, we adopted an autoethnographic method [211] in our VR design mechanics evaluation.

Ethical Considerations and Limitations

Following research ethics guidelines [31], we carefully designed our methodology to prioritize ethical considerations. Before data collection, we consulted our institution's Research Ethics Board (REB) and confirmed that formal review was not required. To protect user privacy, we focused on single-user modes in VR apps and, for social platforms (e.g., VRChat, Meta Horizon Worlds, Immersed), centered our analysis on our researcher's experience while avoiding recordings involving other users. We also consulted our university library on the appropriate use of screenshots under Fair Dealing guidelines in the Copyright Act. While our autoethnographic study provides valuable insights, it has limitations. We have provided a detailed reflexivity statement (see Appendix A) to address potential biases from H. Hadan's background. However, we recognize that our findings may not fully represent users with varying levels of awareness and perceptions of deceptive design [287, 52, 149, 76]. Nevertheless, our study of 12 cross-platform VR applications captures a broad range of deceptive tactics and privacy issues within VR privacy communication and interaction mechanisms, which we then examine with VR users in Section 7.2.3.

Data Collection

Over six months, H. Hadan, engaged and fully immersed in all 12 VR apps using a Meta Quest 3 headset. For applications with a clear endpoint, exploration continued until completion, while for open-ended applications (e.g., Beat Saber), it followed the principle of saturation—stopping once no new privacy issues or deceptive designs emerged. Our focus was on design mechanisms that (1) provide privacy information and (2) allow users to make and express privacy choices. Following an established method in our Chapter 6, the researcher documented each session in two parts: (1) detailed observations of privacy communication and interaction mechanisms incorporating deceptive design, and (2) reflections on experiences, thoughts, and emotional responses. Video recordings were captured to document instances of deceptive designs and user interactions in VR. 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 (see Section E.2). This process resulted in 59 diary entries, 55 video recordings, and 146 screenshots. Data were first organized on Miro[5] for visual interpretation and then transferred to Dovetail[6] for thematic analysis. Table 7.1 details hours spent and diary entries for each VR application, an example diary entry in Section E.1.

Data Analysis

H. Hadan conducted *deductive reflective thematic analysis* method [39] using our *Assessment Guide*, to maintain the personal and reflexive nature of the autoethnographic study [211, 64, 106] while enabling a "theoretically-informed exploration of qualitative data" [39, p. 263]. To enhance the rigor of our qualitative research, we provide a *Reflexivity Statement* for our autoethnographic evaluation of VR apps in Appendix A to acknowledge potential biases in data coding and theme development, following guidance from the literature [164, 221, 39]. The researcher started by reviewing data based on the *Assessment Guide*, coding diary entries while verifying observations with video recordings and screenshots through an iterative process, and discussing findings with our research team. This process led to the identification of 14 deceptive design patterns from privacy communication and interaction mechanisms of the 12 VR apps (see Table 7.4).

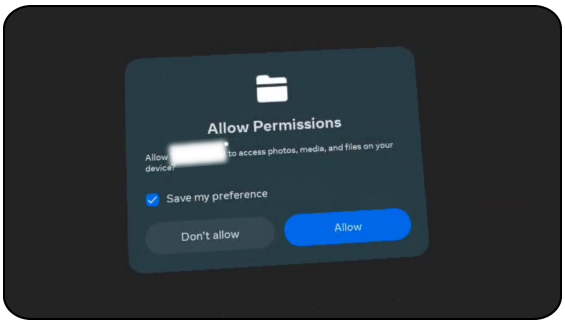
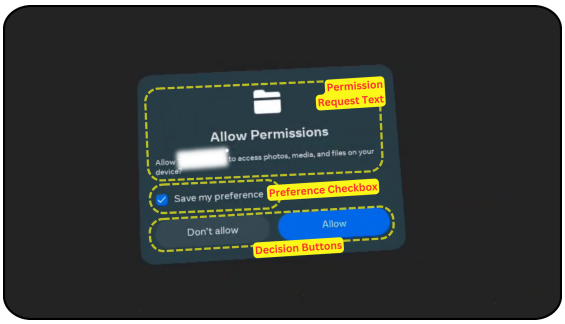
7.2.3 Scenario-Based User Survey

Following methods for studying user privacy perceptions in immersive technologies in our Chapter 4, and deceptive design in computer and mobile environments [19, 52, 99, 84], we conducted a scenario-based online survey with $N = 424$ VR users. We developed seven scenarios based on four VR applications from our autoethnographic evaluation, each illustrating an exemplary privacy mechanism incorporating 11 deceptive design patterns. Each scenario included a questionnaire to assess participants' recognition of and reactions to subtle manipulations, providing qualitative and quantitative insights into user choices and

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

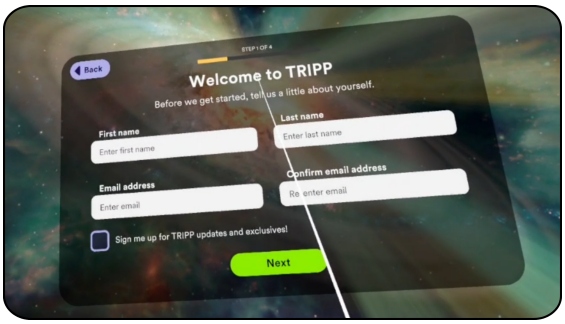
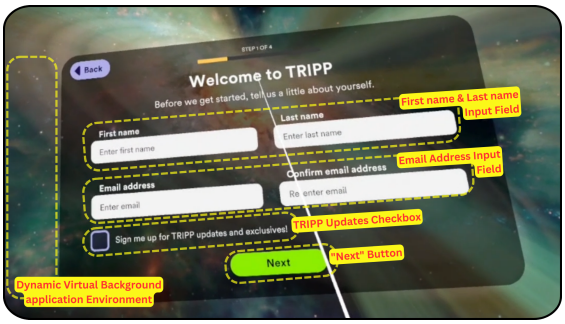
behaviors. Participants were required to be 18 years or older and have experience with one of the four applications. They were recruited separately for each scenario and viewed only one to ensure demographic diversity and minimize response bias. Before recruitment, our study received Research Ethics Board approval (#47320) from the University of Waterloo. The survey, conducted on Prolific[7] in late 2024, received 424 complete and valid responses. This thesis presents preliminary findings from $n = 182$ (43% of 424) participants across the first three scenarios. Table 7.3 summarizes participant demographics (details in Section E.4).

Table 7.2: Scenario 1-3 presented in our thesis. For the details of all seven scenarios, refer to Section E.6.

ID	Scenario
S1	 *Description:* Imagine you are about to use **VRChat**, a social VR application. Upon entering the application, you are immediately presented with a **Permission Request** asking whether to grant permissions for accessing your photos, media, and files. You must decide whether to approve or deny these permissions before proceeding further into the application.
	 • False Hierarchy/Visual Prominence: Highlight the "Allow" option that is invasive to user privacy. • Bad Default: Set default options that benefit the company but risky for users' privacy. • Privacy Zuckering: Trick users into thinking this permission is essential for the service. • Hidden Information: Obscure crucial details of the purpose of data collection.

[7]Prolific. https://www.prolific.com/

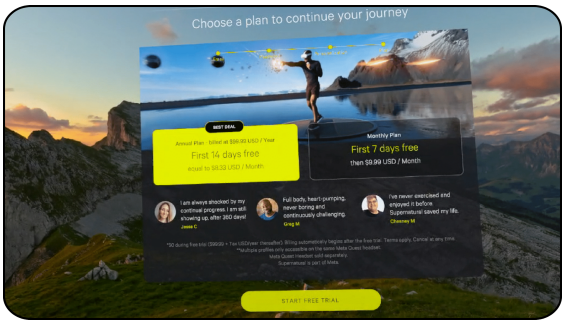
Table 7.3 Continued. Scenario 1-3 presented in our thesis. For the details of all seven scenarios, refer to Section E.6.

ID	Scenario	
S2		
	Description: Imagine you are about to use **TRIPP**, a VR wellness application. As you begin, you are presented with a **Registration Form**. Before accessing any functions, you are required to either enter your email address or register an account by providing your firstname and lastname to unlock all features.	• Forced Registration: Require account creation for tasks that should not need it, potentially extracting unnecessary personal data • Privacy Zuckering: Trick users into thinking this permission is essential for the service.

Scenario Construction

We selected seven privacy mechanisms from four popular VR applications—VRChat, TRIPP, Supernatural, and The Climb 2. Identified in our autoethnographic analysis, these mechanisms demonstrated 11 deceptive design patterns, including False Hierarchy & Visual Prominence, Bad Default, Privacy Zuckering, Hidden Information, Forced Registration, Endorsements & Testimonials, Positive or Negative Framing, Privacy Maze, Complex & Lengthy Language, Trick Questions, and Nagging (see Section E.6). These seven mechanisms provided broad coverage of the deceptive patterns we identified while keeping the study manageable for participants. To help participants recall their initial perceptions and experiences during their own experience, scenario included a description, two screenshots, and a 10-second video of a pre-recorded interaction with the VR mechanism (see Section E.7). This thesis presents findings from the first three scenarios: the data permission request in

Table 7.3 Continued. Scenario 1-3 presented in our thesis. For the details of all seven scenarios, refer to Section E.6.

ID	Scenario
S3	  *Description:* Imagine you are about to use **Supernatural**, a VR fitness application that offers a subscription-based experience set in a photorealistic, immersive virtual landscape. As you start, you are presented with **Subscription Form** with two subscription plans and showcasing three testimonials. Before accessing any features, you are required to select and pay for a subscription. • Endorsements and Testimonials: Use fabricated testimonials to influence users' purchase decisions. • False Hierarchy/Visual Prominence: Highlight the acceptance option that transmits user data. • Positive or Negative Framing: Use vibrant green to communicate emotional safety on options that transmit user data.

VRChat[8] (Scenario 1), the registration form in TRIPP[9] (Scenario 2), and the subscription form in Supernatural[10] (Scenario 3).

Survey Design

To minimize bias, we framed the study as an exploration of user experience with VR applications and avoided terms like "privacy," "manipulation," and "deceptive design" in our materials and most questions. Only at the end of the survey did participants reflect on their privacy decisions and general concerns before being debriefed on the study's true purpose and rationale. The full questionnaire is in Section E.7.

[8]VRChart. https://hello.vrchat.com/. Last accessed on Jan 21, 2025
[9]TRIPP: The Future of Wellness. https://www.tripp.com/. Last accessed on Jan 21, 2025
[10]Supernatural VR. https://www.meta.com/ca/quest/supernatural/. Last accessed on Jan 21, 2025

The survey began with an information sheet, consent form, and screening questionnaire. We recruited participants aged 18 and older from North America with prior experience using one of the four VR applications. Eligible participants were directed to the main survey, where we assessed their familiarity with VR environments and deceptive design, as these factors influence their privacy concerns and susceptibility [159, 151, 52]. Then, each participant viewed a scenario consisting of a 10-second auto-replaying video, a description, and two screenshots of a VR privacy mechanism (see Section 7.2.3 and Section E.6). Participants were then asked to recall their interactions with the mechanism and explain their reasoning in an open-ended response. To guide participants' focus on privacy, we asked them to identify privacy-related decisions during their interaction and rated the privacy impact of their choices on a 5-point scale ("1-not at all" to "5-significantly"), and provided follow-up explanations if their rating was moderate or higher ($\geq$"3-moderately").

Participants then identified design elements influencing their decisions by selecting from a labeled screenshot of the VR privacy mechanism. Unlike prior research [52, 19], we avoided framing these elements as "deceptive" or "manipulative" to prevent bias. Instead, we provided a neutral definition: *"UI elements are the components of an interface that users interact with directly. Examples of UI elements include buttons, drop-down menus, sliders, text fields, checkboxes, toggles, and VR-specific properties like realistic virtual objects or dynamic 3D environments."* For each selected element, participants explained its influence in an open-ended response and rated its perceived benefits for themselves, the application's designer or publisher, and third-party stakeholders on a 5-point Likert scale ("1-strongly disagree" to "5-strongly agree"), as their perceived benefits can shape privacy concerns [180]. To assess whether participants perceived the mechanism as manipulative, they answered an open-ended question about its purpose [83, 52].

At the end of our survey, we measured participants' awareness and concerns about VR deceptive design using an adapted scale from the literature [19], where participants rated six paired statements contrasting personal ("my/me") and external ("people/others") perspectives on a 5-point scale ("-2-strongly disagree" to "2-strongly agree"). The questions were adjusted to the VR context and linked deceptive design to personal information sharing (see Section E.7.3). To ensure consistency and clarity, we reported these responses using

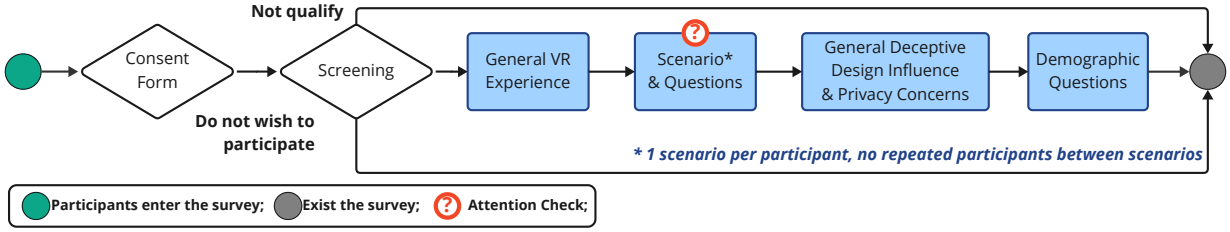


Figure 7.1: Survey flow: After passing the screening questionnaire, participants answered about their experience with VR devices and the presented application. They were then shown a VR privacy mechanism scenario, followed by questions about their reactions, decision-making, the role of specific design elements in their decisions, and perceived privacy impacts. Lastly, participants answered their general concerns about online design influences, internet privacy, and demographic details. In total, we received $N = 424$ valid responses, with $n \approx 61$ per scenario. The full survey questionnaire is in Section E.7.

Table 7.3: Participant demographics (n = 182), including gender, age, education level, professional VR work experience, IUIPC scores, and awareness and concerns about deceptive design. A detailed overview of participants' demographic is located in Section E.4. Participants received £8 for survey completion or GBP £0.80 if screened out. *DD=Deceptive Design.*

Gender	
Female	86 (47%)
Male	94 (52%)
Non-binary	2 (1%)
Prefer not to say	0

Age	
Range	18-64
Mean	35.08
SD	11.02

Education	
High school diploma, GED, or less	31 (17%)
Associates or technical degree	20 (11%)
Bachelor's degree or equivalent	102 (56%)
Graduate or professional degree	29 (16%)

Country	
Canada	42 (23%)
USA	140 (77%)

Profession VR Job	
Developer/Engineer	7 (4%)
Researcher	12 (7%)
Designer (e.g., UI, UX)	9 (5%)
Product Manager	15 (8%)
Data Analyst	11 (6%)
Never	152 (84%)

IUIPC Scores	
Control	
Range	2-7
Mean (SD)	5.60 (1.02)
Awareness	
Range	1-7
Mean (SD)	6.11 (0.98)
Collection	
Range	1-7
Mean (SD)	5.29 (1.46)

DD Awareness & Concern	
Others' perspective	
Mean (SD)	2.97 (0.95)
Median	3
Mode	4
Personal perspective	
Mean (SD)	2.88 (0.94)
Median	3
Mode	4

a standard 5-point Likert scale ("1-strongly disagree" to "5-strongly agree"). Finally, we assessed participants' general privacy concerns [156], including their perceived *control* over personal data, *awareness* of data practices, and *concerns* about data collection. Our survey concluded with demographic questions.

Data Analysis

We detail our quantitative data analysis alongside the results. For open-ended responses, two researchers used inductive thematic analysis [39]. After data cleaning, the researchers familiarized themselves with the data. Each researcher then independently coded 11%

($n = 50$) of the data, and then iteratively discussed and resolved disagreements. This process was repeated weekly, with an additional 11% of data being coded each week.

7.3 Findings

We first present findings from our autoethnography evaluation of design mechanisms, followed by insights from our thematic analysis of user perceptions and experiences.

7.3.1 RQ7.1: Deceptive Design in VR Privacy Communication Design Mechanics

Our analysis of 59 diary entries identified five categories (themes) of 14 deceptive design patterns that influence user privacy decisions[11].

In this section, we illustrate the 11 deceptive design patterns identified in the seven selected privacy mechanisms to form the foundation for our analysis of user perceptions and experiences. For clarity, VR application titles appear in italics (e.g., *Beat Saber*), deceptive design patterns appear in `monospace` (e.g., `Privacy Mazes`), and direct descriptions from VR design mechanisms appear in quoted italics. To provide context for findings in Table 7.4, we include each application's unique icon upon its first mention (e.g., 

for *TRIPP*).

Scenario 1—Registration Mechanism

The VR application *TRIPP* (

) requires users to create accounts independent of their VR platform and submit personal information that may not be essential for the app's functionality. This exemplifies the characteristics of `Forced Registration` and `Privacy Zuckering`. For instance, users must provide an email address even to access demo sessions, and unlocking the full set of features requires creating an account and purchasing a

[11]We include the screenshots and short video clips of our researcher's interactions at OSF public repository: https://osf.io/axzve/.

Table 7.4: Using our *Assessment Guide* from Chapter 5, this table presents deceptive design we identified in the privacy communication and interaction mechanisms of 12 VR applications from our diary evaluation.

Theme/Subtheme	**Pattern**	**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*

Note. Themes and codes in this table follow the sequence in our *Assessment Guide*. *QoL features = Quality-of-Life features.

a. VR games and apps acronyms match those in Table 7.1. 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 *Assessment Guide*.

c. We renamed the theme to highlight the "lengthy" issue in privacy policy language, in addition to the complexity noted in our *Assessment Guide*.

Table 7.4 Continued. Using our *Assessment Guide* from Chapter 5, this table presents deceptive design we identified in the privacy communication and interaction mechanisms of 12 VR applications from our diary evaluation.

Theme/Subtheme	**Pattern**	**Synthesized diary entries**[a]	**Mechanisms**
Interface Interference			
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
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 *Assessment Guide*. *QoL features = Quality-of-Life features.

a. VR games and apps acronyms match those in Table 7.1. 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 *Assessment Guide*.

c. We renamed the theme to highlight the "lengthy" issue in privacy policy language, in addition to the complexity noted in our *Assessment Guide*.

subscription, which involves sharing their name and credit card details. The mechanism visually uses a bright green button to emphasize the *"start demo"* option and options that require financial commitment and careful consideration. This design exemplifies the characteristics of `Visual Prominence` and `Positive or Negative Framing`, as green evokes emotional safety and subtly encourages users to accept privacy-invasive options without fully understanding the implications of their choices.

Scenario 2—Subscription Mechanism

The VR application *Supernatural* (SN) requires a paid subscription, and our evaluation reveals the use of `Endorsements and Testimonials` in its subscription mechanism to entice potential subscribers to provide credit card information. These endorsements, which showcase glowing user experiences alongside professionally produced photos, appear highly polished with professional-looking photos far exceeding the quality of typical user uploads (see Section E.2), raising questions about their authenticity. 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 based on perceived social proof. *Supernatural*'s *"sign up"* and *"pairing additional user account"* options, which request users' personal information and details about others, are brightly colored in green and prominently positioned at the top. These elements reflect the characteristics of `Visual Prominence`, `False Hierarchy` and `Positive or Negative Framing`, subtly influencing users' privacy decisions.

Scenario 3—Permission Request

Upon launch, the VR application *VRChat* (CHAT) prompts users to grant access to their *"photo, media, and files"* on their VR device. This interface reflects the characteristics of `Bad Defaults`, as the *"Save my preference"* option is pre-selected, and `Visual Prominence` is used to highlight the *"Allow"* option, making it more visually noticeable than other choices. This combination may cause users to grant access without fully considering or remembering their decision, potentially forgetting to revoke it later. In *VRChat*, the privacy policy is presented only after permission requests. This lack of crucial privacy information demonstrates `Hidden Information`. Requesting such access before users engage with relevant features also exemplifies `Privacy Zuckering`, as it may lead to unnecessary exposure of personal data. Although 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 E.10 in the Appendix), which can cause the link to go unnoticed.

Scenario 4—Privacy Settings

Accessible privacy settings are essential for maintaining user privacy during interactions with VR applications. However, our evaluation found the presence of `Privacy Mazes` in *The Climb 2*, where the privacy policy is buried three layers deep within the settings menu. Users must first navigate to *"Options"* from a list of six items, then locate *"Privacy Policy"* in the second layer to finally access the full document. This complex navigation makes privacy information difficult to access and may discourage users from reviewing important details about data practices and risks.

Scenario 5—Privacy Policy

In addition to buried settings, some VR applications, such as *VRChat*, present in-app privacy policies upon first entry. However, these documents are often long and difficult to read, which can discourage users from engaging with them and hinder their understanding of potential privacy risks. To assess the complexity of these policies, we used Microsoft 365's Flesch Reading Ease Score, following established methods in the literature [82] (see Section E.3). We found that the policy of *VRChat* scored 35.9, which is classified as *"difficult to read"* and understanable only for those with at least a *"college-level"* education[12]. This reflects characteristics of `Complex & Lengthy Language`, which can reduce users' ability to make informed decisions about their privacy.

Scenario 6—Avatar Creation Mechanism

Several quality-of-life (QoL) features, which are designs that make interaction smoother, more customizable, and enjoyable in VR 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 was meant for avatar customization, the wording demonstrates the characteristic of `Trick Questions`. As users see the realistic

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

rendering of their "hands" in the avatar creation process from a first-person perspective (see Section E.2), 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.

Scenario 7—Notification Design Mechanism

The use of excessive permission notifications is also 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.

7.3.2 RQ7.2: Awareness, Perceptions, and Concerns about deceptive design and online privacy

We developed seven scenarios based on selected privacy mechanisms, each comprising a 10-second auto-replaying video, a brief description, and two illustrative screenshots of the VR privacy mechanism (see Section 7.2.3). These scenarios are presented in Section E.6.

General Awareness and Concerns

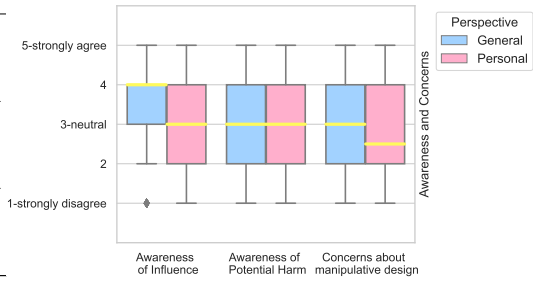
We calculated the mean, standard deviation, median, and mode for participants' general deceptive design awareness and concern scores [19]. Table 7.5 shows the distribution of participants' responses across the six statements. To validate differences between participants' awareness and concerns about deceptive design from personal and general perspectives, we performed Wilcoxon signed-rank comparisons [282] with Bonferroni correction [34].

We found that participants were aware that VR designs can *influence* privacy choices and behavior (Personal: $median = 4$) but perceived a significantly greater influence on others (Others: $median = 3$) than on themselves ($P = .012$). Participants were less

Table 7.5: Scenarios 1-3 participants' awareness and concerns about the influence of VR application design on their choices and behaviors in personal information sharing decisions across six statements from the personal and the general perspectives.

Variable	Perspective	n	Median	Mode	Mean	SD	Min	Max	Wilcoxon test
Awareness	Others	182	4	4	3.33	1.070	1	5	W = 8295,
of influence	Personal	182	3	4	3.23	1.088	1	5	**P = .012**,
									r=-.122
Awareness of	Others	182	3	2	2.79	1.163	1	5	W = 6301.5,
potential harm	Personal	182	3	2	2.83	1.143	1	5	P = .341,
									r=-.046
Concerns about	Others	182	3	2	2.75	1.162	1	5	W = 8533.5,
manipulative	Personal	182	2.5	2	2.62	1.161	1	5	**P = .004**,
design									r=-.142

*Note. *P adjusted with Bonferroni correction. SD=Standard Deviation, W=test statistic, r=effect size.*



concerned about being manipulated personally (Personal: $median = 2.5$) but were neutral regarding whether others' choices on personal information sharing might be manipulated (Others: $median = 3$). This difference was statistically significant ($P = .004$). On the contrary, participants were uncertain about whether manipulative VR designs can *harm* their (Personal: $median = 3$) or others' (Others: $median = 3$) personal information, with no statistically significant difference between the perspectives ($P = .341$).

We further used Kendall's τ correlation tests [68] to explore how participants' awareness and concerns about VR deceptive design relate to demographics and online privacy concerns [156]. As shown in Section E.5, participants with *professional VR work experience* had a positive correlation with *concerns* about VR deceptive design ($\tau = .107$), suggesting those who work in the field of VR are more likely to concern about the power of VR design practices on their privacy choices and behaviors. Conversely, increased *experience using VR devices* correlated with lower *concerns* ($\tau = -.081$), possibly indicating that people's VR familiarity can diminish perceived privacy risks. In addition, participants' level of privacy concerns (control, awareness, data collection) had positive correlations with participants' awareness of VR deceptive design's *influence* ($\tau = .13$, $\tau = .117$, and $\tau = .09$, respectively) and *harm* ($\tau = .111$, $\tau = .092$ and $\tau = .158$, respectively) on their privacy choices and behavior. These findings suggest that participants with higher online privacy concerns are more aware of VR's manipulative potential. Additionally, participants' privacy concerns (control, awareness, data collection) positively correlated with *concerns* about manipulation

by VR designs ($\tau = .084$ and $\tau = .178$ respectively), indicating those who value privacy are more vigilant about manipulative risks in VR.

Our findings suggest that people with higher online privacy concerns and those working in professional VR design, development, and research positions exhibit greater awareness and concerns about the impact and potential harms of deceptive designs on their personal privacy decisions and behaviors. However, greater familiarity with VR devices appear to reduce awareness and concerns towards deceptive design.

User Perceptions and Experiences with the Seven Scenarios

In this section, we presents preliminary findings from our thematic analysis of participants' open-ended responses to the first three scenarios. For clarity, deceptive pattern names are in `monospace`, descriptions directly taken from the VR mechanisms are in quotation marks, and participant quotes are *italicized* within quotation marks followed by scenario and participant identifiers (e.g., "..." — S3-P1).

Finding 1: Visual manipulation and attention direction lead users to hastily grant permissions. Although our participants did not explicitly understand the concept of deceptive design, they described its effects on their decision-making and the disruption it caused to their VR experiences. This observation aligns with our quantitative findings In S1's permission request mechanism, the `false hierarchy and visual prominence` highlighted the "Allow" button in bright blue, overshadowing the "Don't Allow" option. Participants noted the bright blue button *"catches attention"* and *"expedites"* their decision-making. Some participants admitted they were more inclined to allow permission when navigating quickly, as it *"felt natural and easier to allow access"* (S3-P2). Others noted that the blue button's prominence led them to unknowingly select "Allow" when *"not paying attention"* (S3-P44). Similarly, in S3, participants' attention was drawn to the yearly subscription plan due to its bright green highlighting. They noted that the *"contrast and location"* of the bright green button naturally *"draws attention first"* (S2-P28), making them favor the yearly plan over the other option. Participants further noted that they often associate the bright green color in S3 with the universal meaning of *"go,"* which *"made me want to press*

it" (S2-P43). This reflects the impact of the `positive or negative framing` that evokes emotions and directs user choices.

Finding 2: Bad defaults, forced registration, and vague policies trigger privacy concerns and user frustration. Participants' responses also provided insights into their experiences with the `bad default` and `forced registration`. In S1's VR permission request mechanism where the "save my preference" checkbox was pre-checked by default, participants expressed concerns about accidentally leaving the checkbox selected and *"forgetting it's on,"*, potentially leading to unintended data sharing (S3-P55). Participants in S2 expressed frustration that they were required to provide personal information for registration without knowing what the application offered. Many are concerned about risking their privacy for potentially disappointing experiences, with one participant stating it felt like *"signing up for data harvesting and advertising"* (S1-P45). Others wished for better designs that allowed them to preview the application before sharing their information, noting that requiring registration upfront *"put me off the application"* (S1-P3). The `privacy zuckering` and `hidden information` complicated participants' privacy decision-making. In S1, the VR application requested access to users' media files. While many participants questioned why the permission was necessary, some assumed it was essential for functionality. Nevertheless, some raised privacy concerns, describing the request as "vague and broad" (S3-P42). One participant preferred to "select don't allow" before understanding what it entails (S3-P44), while another always *"allow the minimum number of permissions"* when trying new apps (S3-P18).

Finding 3: Polished testimonials and false free trials lead to user skepticism despite persuasion. Our findings revealed participants' mixed reactions to the `endorsement and testimonials` deceptive design pattern. Many participants were skeptical about the authenticity of the testimonials, with some describing them as *"too polished"* (S2-P22) or highlighting that other users' experiences *"may not be mine, so I want to try it myself"* (S2-P19). However, several participants found the positive testimonials persuasive, making them more inclined to subscribe and trust the application. One participant noted that the testimonials *"gave me a positive view... and made me trust them more"* (S2-P55), while another stated they were *"very persuasive"* in their decision to pay the subscription

(S2-P35). However, this decision requires sharing their payment information with the VR application. Interestingly, while S3 offered a free trial to promote subscriptions, many participants felt it was not truly free since starting it required payment information. Concerns included automatic payment detail saving and unwanted subscription renewals, with one participant stating, *"If it's a free trial and then asks for your payment information, it doesn't feel like a free trial"* (S2-P18). Another noted it relies on users *"forgetting to cancel before the trial ends"* (S2-P15). Similarly, in S2, participants viewed the intention of the mandatory registration as *"to collect data and possibly sell it to third parties"* (S1-P5). To mitigate privacy threats from these deceptive patterns, participants employed coping strategies such as using fake names in S2's registration or avoiding storing personal files on devices in S1's permission request. These actions reflect their concerns about privacy invasion and the perceived unnecessary collection of information.

Finding 4: Personal characteristics and VR immersion influence user privacy decisions. We observed other factors affecting participants' privacy concerns and perception of being manipulated. The dynamic VR environment, for instance, appeared to amplify the effects of VR deceptive design. Participants noted that the *"calming and peaceful"* in S2's registration form and S3's subscription form made them more willing to share information (S1-P25). Others found the environments enticing, providing *"a glimpse of what I could experience,"* which made them *"excited to sign up"* (S2-P19). VR application's reputation and popularity also appeared to increase trust, as many participants believed well-known brands handle personal information responsibly. One participant explained, *"I trust they use it mainly for my account and workouts,"* despite they are *"moderately concerned"* about their privacy (S2-P44).

In all three scenarios, participants constantly noted that VR privacy mechanisms resembled those on computers and mobile devices. This familiar, standardized appearance made the mechanisms seem trustworthy and non-threatening, as *"we already allow this with our phones, so I pretty much have enough trust"* (S3-P11). However, this familiarity also led to privacy resignation, with participants believing *"all platforms operate the same way"* (S3-P55), making concerns seem futile, even though many feared losing personal information when interacting with VR privacy mechanisms.

7.4 Discussion and Future Work

Our findings show that deceptive designs in VR are primarily those that have directly migrated from 2D platforms and continue to rely on 2D interface elements within the 3D virtual space. Although the literature hypothesizes deceptive designs that leverage VR's unique properties (see Chapter 3), we did not observe such patterns in our analysis. Our survey with VR users shows that although VR-specific properties can enhance the effectiveness of deceptive designs in influencing users' privacy decisions, they did not enable those designs in VR mechanisms. We found that even though we did not introduce the participant to deceptive designs to avoid biases, most recognized how these design choices influenced their privacy-related behaviors and preferences.

Our participants' responses demonstrated how their familiarity with similar privacy mechanisms in non-VR environments and trusted brand reputations reduced privacy concerns, aligning with prior findings on the role of perceived trustworthiness and exposure frequency in users' vulnerability to deceptive design in non-VR environments [151, 52, 149] and VR user privacy perception research [159, 111, 3]. Our study extends these findings to the VR context, where we observed that the immersive nature of the environment, particularly through dynamic backgrounds and spatial design, created additional layers of manipulation that affected users' privacy decisions. This extends literature review studies [100, 134] by demonstrating how VR's unique characteristics can enhance the effectiveness of deceptive design patterns based on evidence from VR users' personal experiences.

Furthermore, our findings highlight a concerning paradox in VR privacy decision-making that extends beyond mere privacy resignation we found in Chapter 4. While participants expressed high privacy concerns and developed various coping strategies, they often resigned themselves to accepting privacy-invasive options, perceiving such mechanisms as *"typical," "standard,"* and inevitable across both VR and non-VR environments. This behavior may be a key factor that contributes to previous research's finding that users feel powerless to counter deceptive design even when aware of their presence [218, 19, 83, 21]. Our findings show that this sense of powerlessness is migrated to VR contexts, as users' repetitive

exposure to and familiarity with such mechanisms create a false sense of normalcy that further erodes users' resistance to manipulation and privacy risks.

7.4.1 Limitations

Our study has several limitations. First, as an early exploration of deceptive design in VR, expert analysis was crucial in identifying patterns that non-expert users often overlook [52], but further research is needed to assess their impact across diverse user groups. Second, our autoethnographic evaluation, guided by our *Assessment Guide*, may have missed previously unrecognized patterns, though H. Hadan's expertise in user-centric privacy research helped document privacy expectations and explore beyond existing literature. However, blind spots may persist [52, 96], and we welcome future research to confirm and expand on our findings. Third, due to ethical concerns about including other users without consent, our research focused on deceptive patterns that invade user privacy in single-user VR 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 the literature [133]. Fourth, to deepen our analysis of each VR game and app, we sacrificed the breadth of our study and analyzed fewer total VR apps than prior work (e.g., [52, 96]). Although we included at least one application from each genre, our limited scope prevents us from assessing the prevalence of deceptive design patterns in VR. Fifth, 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 present in other VR ecosystems. Lastly, our data was collected in 2024. We acknowledge that these applications 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 properties in

current VR privacy mechanisms.

7.5 Conclusion

In conclusion, our research sheds light on the presence of deceptive design patterns in VR apps 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 properties, 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 future VR research, design, development, and regulation 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.

Chapter 8

Contributions, Implications, and Future Work

Deceptive design distorts or impairs users' ability to make informed decisions [149, 22, 25]. As immersive technologies become increasingly popular, their sensory stimulation and extensive data collection capabilities have the potential to not only amplify the impact of traditional deceptive patterns but also introduce novel and more subtle manipulations that extend beyond 2D interfaces [27, 169, 97, 87]. This thesis investigates how deceptive design manifests in immersive digital environments, including both patterns that migrate from non-immersive platforms and those that may emerge from the unique properties of immersive technologies, and how these designs impact user autonomy in immersive contexts.

In this chapter, we discuss how our findings across the chapters in this thesis contribute to our four research objectives and address our overarching research statement in Chapter 1. We also discuss the broader implications of our work, which offer recommendations for future research to further investigate deceptive design in immersive technologies and develop targeted user educational interventions, for future immersive application designs that incorporate privacy-respecting principles, and for building regulations that mitigate deceptive design practices.

8.1 Contributions to Research Objectives

8.1.1 Objective 1: Understand the existing state-of-the-art research of deceptive design in immersive environments

In Chapter 3, we conducted a systematic literature review to examine the state-of-the-art research on deceptive design in immersive environments. Drawing from hypothetical scenarios, expert predictions, and controlled in-lab experiments, literature suggested that many deceptive strategies from web, game, and mobile contexts (e.g., interface interference, emotional manipulation, disguised data collection) could be adapted to immersive environments [87, 227, 169]. Beyond these, immersive technologies' unique properties, such as realistic simulation, unbounded display, and sensor data-driven hyperpersonalization, can enable novel and more subtle forms of deceptive design beyond those relying on traditional 2D interface elements [169, 227, 137]. Through our synthesis, we developed a categorization of deceptive design strategies discussed in the literature and analyzed how these strategies interact with the specific properties of immersive technologies to amplify potential user harms (e.g., Table 3.2). Through this work, we also identified several gaps in the current literature. First, there is a limited understanding of the data practices specific to immersive systems that enable targeted deceptive design. Second, user-centered perspectives are largely missing from discussions in the analyzed literature, despite the importance of users' perceptions in identifying borderline manipulative practices that may not be explicitly unethical or illegal [83, 88]. Third, little is known about how deceptive design patterns manifest in commercially available immersive technologies, as existing research in our analysis focused on theoretical or controlled scenarios. These gaps informed the direction of our subsequent studies. In Chapter 4, we explored user awareness and concerns regarding data collection practices in immersive technologies. In Chapter 5, we developed an *Assessment Guide* that offers a consistent and structured framework for identifying deceptive design patterns, including both patterns that migrate directly from non-immersive environments and those that may emerge from the unique properties of immersive technologies. Using this *Assessment Guide* as a foundation, Chapter 6 and Chapter 7 investigate and compare

how deceptive design manifests in real-world commercial computer and VR applications, considering both design mechanisms and user perspectives.

8.1.2 Objective 2: Develop a structured guide for assessing deceptive design in VR based on foundational literature.

To address Objective 2, in Chapter 5, we developed a *Deceptive Design Assessment Guide*, a structured framework for the consistent analysis of deceptive design across both immersive and traditional computing environments. Building on the synthesized deceptive design strategies identified in immersive contexts in Chapter 3 and foundational deceptive design taxonomies on the web and computer applications (e.g., [89, 287, 129]), our *Assessment Guide* captures a comprehensive range of deceptive design patterns spanning both 2D interfaces and 3D immersive environments. This *Assessment Guide* was testified and refined through a preliminary analysis of two VR applications in Chapter 6 and then served as a consistent baseline for our systematic in-depth examination of deceptive patterns and their user impacts in commercial VR applications in Chapter 7. Through this approach, we validated and refined our *Assessment Guide* and illustrated how deceptive design tactics emerge and evolve in real-world commercial immersive environments, and how these tactics align with or differ from those in traditional web, mobile, and computer environments.

Our preliminary investigation in Chapter 6 also identified a range of manipulative marketing practices that extended beyond the design mechanisms within the applications. Many of these tactics aligned more closely with broader predatory marketing taxonomies identified in recent literature [205, 70, 177]. For instance, OW2's distribution of shop items through Twitch drops corresponds with the strategy of *Separate Re-Release of Product as Free, Cheaper, or Easier to Get* [205]. Similarly, the lack of clarity around the value and usability of OW1 coins in OW2 reflects the *Lack of Information About Condition of Product* strategy [205]. While these tactics fall outside the current scope of this thesis and our *Assessment Guide*, their presence in computer environments raises the possibility that such practices may increasingly appear in VR systems. Although this thesis focused on deceptive design within VR applications, we encourage future work to examine how external

economic structures and marketing tactics shape user experience and decision-making in immersive environments.

8.1.3 Objective 3: Investigate and compare the manifestation of deceptive design in commercially available VR and computer applications.

To address Objective 3, we applied our *Assessment Guide* from Chapter 5 in Chapter 6 through a preliminary exploratory comparison of deceptive design in a widely used computer application and two VR applications. The *Assessment Guide* was then refined in Chapter 7 through a detailed investigation of 12 commercially available VR applications. In this section, we summarize our findings and discuss how deceptive design patterns manifest similarly or differently across VR and traditional computer environments. For clarity, deceptive pattern names are presented in `monospace` in the following paragraphs. Table 8.1 provides a summary of the deceptive design patterns observed in the VR applications in this thesis.

Persistent Reliance on 2D Interface Elements

Our analysis revealed a concerning migration of deceptive patterns from mobile and web platforms into immersive VR contexts. These included assumed consent (`submissive acceptance`), `mandatory acceptance` without opt-out options, convoluted privacy settings (`privacy maze`), `hidden information`, and `bad defaults` [97, 96, 82]. Many VR apps lacked accessible in-app privacy policies, and those that did include them often used `complex & lengthy language` that echoed the information overload challenges found in website and game privacy policies [97, 82, 219]. Such a lack of transparency can cause users' to have misconceptions on privacy risks and mislead them into making choices they might not otherwise make. We also identified `nagging` notifications in VR, similar to those seen in mobile and web contexts [96]. In addition, we observed `false hierarchy` and `visual prominence` in VR, such as bright-colored buttons, echoing the grayed-out options that

Table 8.1: Summary of observed deceptive design patterns in commercial VR applications in this thesis. See our *Assessment Guide* in Chapter 5 for the definition of each pattern.

***Theme*/Subtheme**	**Code**	**Amplification Through VR Features****	**Chapter 6**	**Chapter 7**
Theme 1: Sneaking				
Hiding Information	Submissive Acceptance	Full immersion creates friction and discourages users from seeking external references for the omitted information from the VR environment.	-	☑
Theme 2: Obstruction				
Creating Barriers	Price Comparison Prevention	Full immersion creates friction and discourages users from seeking external references for the omitted information from the VR environment.	☑	-
Adding Steps	Privacy Maze	-	-	☑
Theme 3: Social Engineering				
Social Proof	Endorsement and Testimonials	Full immersion creates friction and discourages users from seeking external references for information presented in VR. Realistic simulation creates lifelike virtual environments that enhance the credibility of social proof.	-	☑
	Parasocial Pressure	Coherent 3D interactions makes celebrity simulations feel more responsive and real, enhancing users' emotional connections and compelling them toward purchase decisions.	☑	-
Urgency	Limited Time Message	-	☑	-
Theme 4: Interface Interference				
Manipulating Choice Architecture	False Hierarchy	-	☑	☑
	Visual Prominence	-	☑	☑
	Bundling	-	☑	-
Bad defaults	Bad defaults	-	-	☑
Emotional or Sensory Manipulation	Adorable Design	Multi-sensory feedback and unbounded display make cute elements more engaging, increasing users' emotional attachment and reducing their resistance to manipulative prompts.	☑	-
	Positive or Negative Framing	-	-	☑
	NPC*/Narrative Manipulation	Multi-sensory feedback and unbounded display make cute elements more engaging, increasing users' emotional attachment and reducing their resistance to manipulative prompts.	☑	-

*NPC = Non-Player Character. ** - indicates that no amplification effect from VR properties was observed for this type of deceptive design in the VR applications analyzed in this thesis.

denotes deceptive designs mentioned in the game-related literature [287, 129].

denotes deceptive designs mentioned in VR-related literature [100].

Table 8.1 Continued. Summary of observed deceptive design patterns in commercial VR applications in this thesis. See our *Assessment Guide* in Chapter 5 for the definition of each pattern.

***Theme*/Subtheme**	**Code**	**Amplification Through VR Features****	**Chapter 6**	**Chapter 7**
Theme 4: Interface Interference				
Trick Questions	Trick Questions	Realistic simulation and coherent 3D interactions enhance users' perceived self-representation through full-body avatars, blurring the line between users' voluntary choices and subtle manipulation.	☑	☑
Hidden Information	Hidden Information	Full immersion creates friction and discourages users from seeking external references for the omitted information from the VR environment.	☑	☑
Language Inaccessibility	Complex & Lengthy Language	-	-	☑
Theme 6: Forced Action				
Nagging	Nagging	-	-	☑
Forced Registration	Forced Registration	-	-	☑
Forced Communication or Disclosure	Privacy Zuckering	-	☑	☑
	Mandatory Acceptance	Full immersion creates friction and discourages users from seeking external references for the omitted information from the VR environment.	-	☑
Gamification	Pay-to-play 🎮	-	☑	-
	Power Creep 🎮	-	☑	-
	Can't Pause or Save 🎮	VR device constraints, such as limited battery life, reduced the impact of temporal patterns by requiring users to exit the VR environment every 2-3 hours.	☑	-

*NPC = Non-Player Character. ** - indicates that no amplification effect from VR properties was observed for this type of deceptive design in the VR applications analyzed in this thesis.

🎮 denotes deceptive designs mentioned in the game-related literature [287, 129].

⬡ denotes deceptive designs mentioned in VR-related literature [100].

subtly steer user behavior in non-VR environments [97, 96]. Despite the differences in modality, these VR deceptive patterns relied on 2D interface elements, such as menu screens and pop-up notifications, rather than fully capitalizing VR-specific properties, such as unbounded displays, whole-body interaction, and motion tracking (as discussed in Section 2.2). Specifically, the deceptive design strategies hypothesized by the literature in Chapter 3, such as false memory implantation, perception hacking, and reality distortion, were not observed in our analysis of current VR applications. We suspect that the prevalent use of 2D

interface elements in these applications originates from designers' reliance on conventional UI paradigms and the absence of widely adopted VR design standards, which might have led them to replicate existing design in 2D environments. While this conservative approach may limit the potential for delivering immersive and novel user experiences, it also constrains the manifestation of novel and more subtle forms of deceptive design [100, 133].

VR Properties as Amplifiers, Not Enablers

While the deceptive design patterns observed in commercial VR applications largely resemble those found on traditional platforms, the unique properties of VR appear to amplify their impact rather than enable fundamentally new forms of deception. For instance, artificial `endorsement and testimonials` (see Chapter 7) used as social proof to encourage payment information disclosure [89, 162] become more problematic in VR. Unlike mobile or web contexts, where users can easily pause and verify claims using a secondary source, the blocking of reality when wearing the VR headset (as mentioned Section 2.2), combined with the cognitive disruption of taking off the headset or closing the application to switch to a browser in VR, create a much higher barrier between the virtual and physical worlds. This barrier pushes users to rely exclusively on in-app endorsements to assess the value of services.

Similarly, we observed that the VR application *TRIPP* provided hyperlinks to its privacy policy during user registration. While this is common in web and mobile environments (e.g., on Steam [23]), in those 2D settings, users can open a new tab to skim the content without significantly interrupting their experience. In VR, however, accessing external links requires exiting the application entirely, which introduces friction that originates from the high immersion and the physical-virtual barrier from the virtual experience. This disruption makes referencing external resources more difficult, inadvertently increasing user reliance on the VR interface itself.

As summarized in Table 8.1, the realistic simulation and the virtual self-representation in VR can also amplify the effectiveness of `trick questions` [25, 162, 192]. For example, the avatar creation mechanism in *The Climb 2* prompts users to select their real gender and

race while viewing realistic virtual "hands" from a first-person perspective (see Section E.2). Unlike avatar-based systems on 2D platforms, which typically support on-screen avatar customization with limited embodiment, VR supports full-body tracked avatars that facilitate real-time, immersive interactions akin to face-to-face communication [145, 59]. This avatar creation process leverages VR's immersion and coherence properties by blending visual fidelity with egocentric embodiment and consequently blurs the line between voluntary user choices and subtle manipulation more strongly than in 2D settings [133, 100]. Literature suggests that this fusion of virtual representation and physical identity can increase the likelihood of disclosing sensitive personal traits without fully realizing how such data may be shared with third parties [11].

We did not observe deceptive patterns that directly leveraged VR's "device sensing" property, nor did we find evidence of hyper-personalized manipulations as hypothesized in prior work [133, 100]. This may be because most current VR applications prioritize functionality and basic user experience over advanced behavioral targeting. Although literature shows that VR data are used for marketing [11], these are legitimate business strategies when executed correctly [25]. Therefore, we argue that the current VR data collection appeared to primarily ensure safety and facilitate VR interaction rather than deceive users.

Absence of Patterns Due to Differences in Modality

Some deceptive patterns commonly found in traditional computing environments were noticeably absent in VR. For instance, we did not encounter problems with settings that cannot be saved [96], 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 [96, 196, 82], were mostly absent because most VR applications do not require separate accounts beyond the one tied to the VR headset. However, the challenge of data deletion remains. Cookie banners, common in web platforms [97, 82], 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. Such a lack of transparency can cause users' to have misconceptions on privacy risks and mislead them into disclosing personal information they might not otherwise disclose.

8.1.4 Objective 4: Contextualize VR deceptive design analysis in user experiences and perceptions.

Inspired by our findings in Chapter 3, we first investigated users' awareness and concerns regarding data collection in immersive technologies in Chapter 4. We found that users lack awareness that immersive technology sensors can capture highly granular data, including involuntary body signals of emotional responses, which could potentially make immersive technologies more invasive to their privacy than other types of devices they use on the web, mobile, and Internet of Things (IoT) devices. We also identified the impacts of various factors, such as data type and data sensitivity, on users' concerns regarding data practices. Although several of these privacy-related factors were also observed in non-immersive environments in previous research (e.g., [180, 140, 147, 267, 142]), our work provides a more precise understanding of the effects of the factors on users in immersive environments. We also show that participants lack sophisticated mitigation strategies to address their privacy concerns. For example, despite expressing discomfort with data collection, most of our participants opted to "give up" protecting their privacy. Qualitative feedback from participants indicates that they were very pessimistic about their privacy due to the belief that they had already lost privacy on other non-immersive devices they use. Furthermore, their limited privacy-protective strategies are likely based on their experience interacting with non-immersive devices. These findings further suggests the need to have effective communication about data collection in immersive technologies, where systems often gather sensitive data not typically required in 2D web and mobile applications, such as cognitive, emotional, and personality-related information. These types of data can open the door to new forms of user manipulation. Therefore, in Chapter 7, we examine how deceptive design manifests privacy communication and decision-making in immersive environments. The

presence of such design patterns can undermine users' ability to make informed choices and increase privacy risks.

Our findings in Chapter 6 and Chapter 7 provide evidence of how deceptive design practices can significantly affect the player experience, resulting in frustration, disappointment, and game abandonment. Through a neutral questioning, scenario-based approach, our analysis of VR user perspectives provide evidence that users sense manipulation even without explicit knowledge of deceptive design. This can deter adoption and hints at a potential backlash against VR developers and publishers (e.g., threaten brand sustainability [103]), who deploy such tactics. We also provide examples of how VR users' familiarity with non-VR privacy settings and trust in certain brands can lower their guard in immersive VR contexts. However, we also reveal a paradox in users' perception and behavior, where participants remain aware of manipulation but still surrender personal privacy, as the naturalization of manipulative mechanisms not only undermines user autonomy but also creates a dangerous precedent where being *"used to being manipulated"* becomes an accepted norm in digital interaction design.

8.2 Implications for Future Research, Immersive Technology Design, Development, and Regulation

In this section, we synthesize the core findings of this thesis and discuss their broader implications for the future research, design, development, and regulation of immersive technologies to support the advancement of scholarly understanding of deceptive design and inform ethical industry design standards and robust regulatory protections. Based on evidence gathered from our mixed-method investigations, each subsection offers actionable insights and guidance grounded in both the design mechanisms we examined and our analysis of user perspectives. The findings from this thesis contribute to the development of ethical immersive technologies that prioritize user autonomy, privacy, and well-being.

8.2.1 Implications for Future Researchers

Drawing on the findings from this thesis, we offer actionable guidance for future researchers to proactively address deceptive design in immersive technologies. Through incorporating user perspectives, advancing ethical design strategies, developing effective educational interventions, and refining assessment tools, we propose directions for future research to contribute to both the theory and practice of ethical immersive environment design.

Contextualize Deceptive Design Research in User Perspectives

Our two-phased methodology used in Chapter 6 and Chapter 7 contextualized our investigation of deceptive design in users' interactions, perceptions, and lived experiences. This user-centered approach allowed us to address the inherent subjectivity of deceptive design (see Section 2.1.2) as we identified design elements that users perceived as misleading or coercive [51]. For example, although in computer and web environments, `forced registration` is often designed to make the registration process easier after the trial [289], our Chapter 7 revealed that users felt frustrated when VR applications required their personal information before they could understand or evaluate the service being offered. This user response led us to classify such designs as deceptive in the VR context, and suggests that design practices considered acceptable in 2D environments may no longer be appropriate in immersive settings. Conversely, some design elements that seemed deceptive were ineffective, as their influence was diminished by external factors such as users' perceptions of low value or irrelevance (e.g., *Bundling* and *Adorable Design* in Chapter 6). Building on prior research emphasizing the importance of user perspectives in evaluating deceptive design [83, 88], demonstrates that such perspectives are equally critical in studying deceptive design in immersive environments. Based on these insights, we recommend that future research incorporate user perception studies and contrast them with evaluations of design mechanisms to holistically assess emerging deceptive design in immersive environments. To support this process, this thesis developed an *Assessment Guide* that provides a structured framework for identifying and analyzing deceptive design mechanisms.

Explore "Bright Patterns" as Ethical Design Strategies

Mitigation strategies such as browser alerts and warning messages have been proposed to counter deceptive design by prior research [225], but their effectiveness can be compromised by software bugs, poor maintenance, or conflicting business interests, as seen in the failure of malicious website interventions [101, 121]. Our findings in Chapter 4 revealed that users feel pessimistic about personal data in immersive technologies, and Chapter 7 further showed a growing sense of resignation, with users reporting they are *"used to being manipulated."* Research has also shown that users frequently adopt a resigned attitude towards deceptive design due to their reliance on digital services [154]. These insights suggest that reactive interventions are likely to be insufficient and that deceptive design should be addressed proactively during the design phase rather than relying on retroactive mitigation tools.

One proactive strategy is the adoption of "bright patterns", benevolent design alternatives that prioritize user needs [223, 266, 90]. This approach is essential, as research shows that many designers often lack awareness of deceptive design and may unknowingly adopt them [289, 36]. Thus, providing accessible, research-backed examples of "bright patterns" can raise designers' awareness, offer ethical alternatives, and strengthen their ability to advocate for user-centered decisions under organizational and business constraints [289]. However, while "bright patterns" have been proposed for websites and mobile environments [223, 266, 90], and more recently in VR [11], the possible solutions for broader immersive technologies remain understudied. To advance this direction, we recommend that future research move beyond "bright patterns" in conventional 2D and explore solutions that account for unique properties of immersive technologies, such as spatial interaction, embodied presence, and multi-sensory engagement. Prior research has already begun to identify examples of bright patterns in commercial VR applications [11], which offers valuable starting points for designers aiming to create more ethical and user-respecting immersive experiences that take full advantage of VR's unique properties. For example, VR applications can use spatially anchored consent prompts that users can walk around and inspect, rather than flat popups in a 2D dialogue window that mimics consent banners from web environments.

Foster User Awareness and Resilience Through Effective Education

Our Chapter 3 identified several forms of psychological manipulation and reality distortion that are unique to immersive environments and less common in non-immersive contexts. Theme 8 specifically emphasized the critical role of user education in fostering resilience against these manipulative practices and in addressing the unique data practices associated with immersive technologies [169, 27, 45]. Our user perspective investigations in Chapter 6 and Chapter 7 show that, while users are not familiar with the concept of deceptive design and often cannot pinpoint the specific design elements causing their discomfort, they are able to recognize its general impact on their privacy-related decisions and behaviors. Prior research also suggests users often fail to take protective action against deceptive design due to a lack of concrete awareness of its personal harms [19, 52]. These findings suggest a need for future research on educational strategies that help users recognize and resist manipulation in immersive settings. The deceptive design scenarios identified in our Chapter 3 provide a valuable source for educational materials. For example, such educational interventions can teach users about how their immersive experiences may intentionally blur the boundaries between fiction and reality, and how to distinguish simulated content from authentic representations. Users also need to learn how immersive systems collect data and may subtly encourage their disclosure of personal information, and understand the broader implications of these manipulative tactics, such as threats to privacy presented in Chapter 7 and Chapter 4. Future research is also needed to explore the design of effective educational content that can foster users' long-term resistance to deceptive strategies.

Explore Informed Data Collection without Sacrificing Enjoyment and Immersion

Our findings in Chapter 4 demonstrate that while users desire transparency regarding data collection practices in immersive environments, they often adopt coping strategies that sacrifice both their experience and the functionality of these technologies. One way to achieve informed data practices is through notifications and permission requests. However, our analyses in Chapter 6 and Chapter 7 show that existing implementations of these mechanisms in commercial VR applications frequently incorporate deceptive design elements

that impinge on user decision-making. Despite this, designing effective communication strategies in immersive settings also presents challenges. The sensory richness of these environments can lead users to ignore important notifications [220], whereas overly intrusive prompts can break users' sense of presence and disrupt their experience [80, 125]. Although prior research has proposed alternatives like on-body haptic feedback, floating displays [220], and context-aware timing for notifications [33, 288], these approaches remain largely absent from commercial immersive applications. Our observations in commercial VR applications in Chapter 6 and Chapter 7 indicate that many decision-making interfaces (e.g., menus and consent prompts) still rely heavily on conventional 2D interaction methods such as controller-based clicking. While existing research has introduced design spaces for privacy notices and controls that emphasize dimensions such as timing, modality, and delivery [226, 67], further research is needed to adapt this space for specific properties of immersive technologies, such as unbounded displays, whole-body interaction, motion sensing, and personalized and context-aware privacy controls enabled by granular sensor data [133, 105, 100]. For example, notifications may manifest as virtual objects within the user's field of view that subtly attract attention without overtly interrupting the experience. Gestural interactions, such as nodding to approve or swiping away to decline, can also be an alternative to controller-based clicking to make the decision-making process feel more natural immersive environments.

Augment the Assessment Guides with Broader and Immersive-Specific Insights

Our *Assessment Guide* (see Chapter 5) offers a structured foundation for identifying deceptive design patterns and examining their impact in immersive environments. As immersive technologies and associated deceptive tactics continue to evolve, there is a clear need to extend and refine this *Assessment Guide*. To achieve this, future research can expand its scope by integrating a broader scope of taxonomies from the literature [133, 205] and more explicitly mapping the unique properties of immersive technologies, such as those discussed in Section 2.2, for a more comprehensive view of how deceptive design operates in immersive settings. For example, future researchers may also create subcategories within the *Assessment Guide* to specifically address how properties such as unbounded display, whole-body engagement, and realistic simulations are leveraged for deceptive design in VR to

influence user behavior and emotional responses Chapter 3 and Chapter 6. Clarifying these properties will tailor the *Assessment Guide* more closely to users' immersive experiences and increase its robustness in evaluating deceptive design.

In addition, empirical validation across diverse VR applications and genres is also needed to improve the *Assessment Guide*'s broader applicability. Our analysis in Chapter 6 and Chapter 7 revealed that several deceptive patterns common in 2D environments were not observed in our sample VR applications. This finding indicates the need for broader exploration across more diverse VR applications. While our study of 12 applications provided valuable insights, it remains limited compared to typical web-based investigations (e.g., 11,000 websites [162], and 118 artifacts [87]). Thus, we suggest that researchers examine a wider range of application types, including not only entertainment genres, social VR platforms, and productivity tools as analyzed in Chapter 6 and Chapter 7 but also educational applications, travel and exploration simulators, and professional training tools. The larger-scale, genre-stratified analyses will allow researchers to better isolate and compare the presence of deceptive designs across similar genres or even examine the same application across different platforms. Such comparisons will improve the understanding of how deceptive designs are perceived and experienced in immersive environments and how their different manifestations influence user perception, behavior, and trust.

8.2.2 Implications for Immersive Technology Designers, Developers, and Publishers

The findings from this thesis offer practical guidance for designers and publishers aiming to create ethical, user-centered immersive experiences that respect user privacy and autonomy. We discuss how to proactive design approaches that move beyond mere compliance to support transparent data practices, clear communication, and alignment with user expectations, all of which contribute to sustained user loyalty and engagement, applications' success, and the creators' reputation and credibility in the long term.

Design to Avoid Manipulative Patterns and Protect Users

The findings from this thesis offer several design recommendations for mitigating deceptive practices and enhancing user protection in immersive environments. As discussed in Chapter 3, early research has emphasized designing for sympathy-based rather than empathetic responses when creating immersive user experiences. Other suggestions include the integration of deceptive design auditing systems [73, 186] and promoting trust and transparency in immersive content [45, 169]. Building on these insights, we propose that immersive systems be designed to help users differentiate between fictional simulations and representations of reality by incorporating unobtrusive visual indicators. [20]. For example, virtual elements that are fictional can be tagged with visual markers (e.g., color-coded borders, comic elements [14]) that remain visible during interaction without detracting from immersion.

In light of our findings, we also emphasize the importance of embedding proactive protections into immersive design. One example, as discussed in Chapter 3, is the implementation of robust security measures to protect users from privacy violations and targeted manipulation that may originate from security threats [105, 197, 159]. As researchers continue to explore "bright patterns" as ethical alternatives to deceptive design (see Section 8.2.1), we also recommend that designers actively integrate these patterns into their design practices. This way, designers can create immersive experiences that proactively respect user agency, rather than responding to harms after they occur [223, 266]. Given the increasing integration of immersive technologies into classroom education (e.g., [272, 155]), we further recommend that designers consider protections specifically tailored to younger users, who may be more susceptible to manipulation in these environments [218]. These can be parental control [194, 57], privacy prompts using age-appropriate language [62, 242], and mandatory educational onboarding modules that explain potential risks (as discussed in Section 8.2.1). Integrating these protections as standard design features can proactively protect younger users and foster safer engagement with immersive technologies.

Re-envision Data Practices in Immersive Environments

Our Chapter 4 showed that users frequently expected their data to be used only for functionalities aligned with their interests. At the same time, research indicates that data in immersive applications is often repurposed for commercial use without explicit user consent [264, 11, 3]. In addition, current privacy regulations are inadequate in addressing the unique challenges posed by the proliferation of sensors and opaque data practices in immersive environments [53]. As shown in Chapter 4, many of the data types used in commercial immersive technologies are not commonly seen in traditional digital environments. Moreover, Chapter 3, further shows that data traditionally considered non-sensitive, such as habitual movements and behavioral patterns, can uniquely identify users in immersive contexts and support hyper-personalization [173, 206, 169]. Although we did not observe instances of hyper-personalized manipulation in commercial VR applications in Chapter 6 and Chapter 7, such practice is likely to emerge in the near future without proper oversight and intervention. Thus, based on our findings, we recommend that designers, developers, and application publishers reassess data collection practices in their applications, with particular attention to how various data types contribute to privacy risks and whether they are essential for core functionality [63]. When making design choices, we recommend that designers move beyond minimum legal compliance and instead align system behaviors with users' mental models derived through user testing, interviews, or feedback loops. This approach can simultaneously reduce users' cognitive load, improve usability, and foster higher user satisfaction and more favorable public perception of both the product and its creator [199, 103, 274]. Our Chapter 4 of this thesis offers indications for the designers about the data types that users consider sensitive and suggests that particular attention should be paid to data types that are currently considered non-personally identifiable in non-immersive technologies [94, 173, 206]).

Cultivate User Trust through Open Communication and Active Listening

Our findings in Chapter 7 alert designers and publishers to the fact that users are acutely aware of the influence deceptive patterns have on their decisions and behaviors, even

if they cannot explicitly identify them as such. This implicit recognition shaped users' trust in the application and its creator, and influenced their long-term engagement. As further demonstrated in Chapter 6, users' perception of being manipulated diminished their overall experience and discouraged their continued use of the application, which can damage the applications' sustainability and brand reputation in the long term [103]. Prior research emphasizes that transparent communication can foster users' positive view, trust, and mutual understanding between developers and user communities [74], and is vital for ensuring long-term user support and loyalty [274, 275, 8], especially when new design mechanisms are introduced [103]. Combining insights from this thesis and from the literature, we thus suggest that publisher companies invest in dedicated and continuous user research that includes usability testing, behavioral analytics, and longitudinal feedback studies. This enables the identification of user concerns in real time and addresses deceptive design that was unknowingly adopted or as a result of following industry standards [289, 36]. At the same time, active communication with the user community is also an opportunity for designers and publishers to openly discuss why certain changes were made and how user concerns have shaped those updates. In doing so, designers and publishers can foster a participatory relationship in which users feel respected, involved, and valued in the application's evolution [103, 74].

Explore Effective Privacy Control and Notifications

Prior work suggests that users are not inherently opposed to data collection, but rather object to the collection of sensitive or non-consensual information [180]. Several studies reviewed in Chapter 3 and the participants in Chapter 4 emphasized a common demand for effective control and explicit consent for specific types of data collection, easily accessible opt-out options, and clear control over their personal virtual spaces and objects (e.g., [139, 20, 169]). However, our analysis of commercial VR applications in Chapter 7 revealed that many failed to provide critical privacy-related information (`Hidden Information`), or used deceptive design (e.g., `Bad Defaults` and `Visual Prominence`) to steer users toward permissions they might not otherwise grant.

As immersive technologies continue to evolve and integrate more bodily sensors, we recommend that designers adopt a privacy-protective default approach that minimizes users' cognitive load while supporting them in making "better" privacy choices [212]. For example, applications can be configured to default to require users to opt in rather than opt out of data sharing [285]. Rather than requesting broad consent during onboarding, applications can instead use tailored, permission prompts triggered by relevant user actions. Additionally, as literature shows that personalized data collection alerts can improve user awareness and comprehension [75, 23], future designers can also explore adaptive privacy settings that adjust to users' behavior patterns over time (e.g., frequency of app use, types of interactions, typical activity duration). For example, users who consistently deny access to a certain sensor may be presented with defaults reflecting this preference for a friction-free user experience, while still retaining users' ability to manually change these options at any time to avoid inadvertently engaging in coercive or forceful design [115, 247].

8.2.3 Implications for Immersive Technology Regulation

In this section, we outline the implications of the findings from this thesis for the regulation of immersive technology, is crucial in governing user privacy, security, safety, and industry standards. Specifically, we discuss how current regulations fall short in preventing harms from immersive technologies, and we provide actionable recommendations for expanding legal protections, improving transparency, and supporting ethical design practices across immersive environments.

Expand and Strengthen Regulations to Meet Emerging Risks

A recent analysis of privacy laws and regulations has shown that current regulatory frameworks are inadequate in addressing the privacy risks posed by immersive technologies [53]. Building on insights from both the literature and user perspectives, our findings in Chapter 3 and Chapter 4 further reveal the need for expanded and strengthened regulations governing immersive technologies' collection and use of data that are less commonly gathered by

non-immersive technologies [27, 94], biometric indicators, behavioral identifiers commonly considered non-sensitive [173, 206], and data from involuntarily involved parties such as bystanders and co-located users. As shown in Chapter 4, users exhibited a general lack of familiarity with the data practices associated with immersive technologies and the potential risks and consequences of such processing. This limited awareness increases users' vulnerability to a wide range of deceptive practices that exploit behavioral and emotional data [133, 218], beyond those we identified in current VR applications Chapter 6 and Chapter 7. Thus, regulatory updates need to go beyond addressing existing privacy risks in immersive technologies to also account for the potential manipulation of users enabled by immersive environments' data richness and sensory realism [44, 208, 45].

To effectively respond to the evolving concerns around privacy and user manipulation in immersive environments, we recommend that the legal definition of "sensitive data" should be expanded to include sensor-derived behavioral cues, gaze patterns, motion trajectories, and inferred emotional states, which were perceived to be sensitive by our participants (see Chapter 4) and hypothesized by the literature as could be exploited in deceptive design practices within immersive environments [169, 141, 132]. We also suggest that a thorough review of the existing regulatory frameworks is needed to assess whether existing rules sufficiently protect users' autonomy, safety, privacy, and security, particularly for vulnerable populations such as children [218]. Strengthened regulations also need to limit the use of deceptive design patterns [89, 192] in any interfaces in immersive environments and require privacy communications be embedded directly in immersive applications, such as in the menus or through spatial interactions or dynamic visual cues (e.g., icons that indicate data collection zones in virtual space), rather than solely linking to static policies on publishers' website [11]. The data types and risk scenarios identified in this thesis provide a foundation for classifying new categories of sensitive information and for developing regulatory frameworks around consent and manipulation in immersive systems. Additionally, literature documented regulatory gaps in U.S. legislation [53], the undisclosed data practices observed in Oculus VR privacy policies [265], and the disparities between privacy policy promises and actual service behavior [291] also offer concrete examples of areas where regulation must address to better protect users' rights and well-being in

immersive environments.

Create Dedicated Privacy Statements for Immersive Technologies and Apps

To create immersive experiences, immersive technologies require a large amounts of user data [27, 44]. Many participants in Chapter 4 reported relying on publishers' policies, laws, and regulations to understand the risks associated with immersive environments and trusting manufacturers to adhere to the statements in their policies. However, as demonstrated in Chapter 7, current VR applications integrate privacy policies with convoluted language or bury them deep within settings menus. In addition, research has further shown that many publishers of VR applications use a single privacy policy to cover all their (immersive and non-immersive) products' data practices, making the scope of data collection in immersive technologies unclear [11]. Such practices, combined with the deceptive design practices that deceptive design strategies that obscure critical information, discourage users from seeking information and hinder their ability to access the information they expect [97, 96].

Given these concerns, privacy policies in immersive technologies to should be clear, concise, and immediately accessible at the point of data collection or user onboarding, to ensure that users can quickly understand how their data are used without needing to navigate complex terminology or hidden interfaces [193]. For example, permission requests and privacy information can incorporate visual representations and interactive elements to enhance user comprehension [213, 280]. While Microsoft 365's Flesch Reading Ease Score, as used in Chapter 7 and established in prior research [82], offers a convenient measure of policy language complexity. It does not capture users' actual comprehension, detect omitted or misleading content, or flag manipulative framing techniques (e.g., positive/negative framing or selective emphasis) [271, 152]. Therefore, we further suggest the development of dedicated policies for immersive technologies (as discussed in Section 8.2.3) and universally accepted assessment tools and standards for evaluating privacy policy complexity, especially given that the publishers and developers of applications often operate globally. To ensure user comprehension of privacy policies in immersive technologies, future work could explore the development of user-centered feedback systems, similar to Mozilla's Privacy Not Included

scoring system [179], that capture real-world user perceptions of policy information clarity, accessibility, and transparency. Such systems may eventually inform broader efforts toward improving policy design and communication.

Shape Industry Ethics and Broader Implications for User Rights

Our findings revealed the broader and lasting impact of deceptive design on user perceptions of the industry and publisher reputations. The deceptive strategies employed in the exemplary computer application analyzed in Chapter 6 triggered widespread debate within the user community and provoked significant public backlash. Specifically, the launch of OW2 resulted in "overwhelmingly negative" user reviews[1] and a noticeable decline in engagement, as reported in Blizzard's 2023 second-quarter financial report [15]. These user reactions demonstrate the long-term risks of prioritizing short-term corporate gains through deceptive practices at the expense of user trust.

The observed ripple effect has a far-reaching consequence that specific design decisions can lead to on public trust in immersive technologies more broadly. As demonstrated in Chapter 7 that deceptive designs, even when not clearly recognized by users, can undermine users' experience, discourage their ongoing engagement, and evoke their skepticism toward a publisher's ethical standards. These findings indicate the need for industry actors to move away from deceptive practices and embrace more ethical design strategies. However, many designers remain disconnected from regulatory guidelines and often view legal compliance as a separate or obstructive concern [86]. To bridge this gap, and drawing on advances in "bright patterns" research discussed in Section 8.2.1, we recommend that it is necessary to establish practical, enforceable design frameworks that embed "bright patterns" as positive design choices that prioritize user well-being [266, 223] as baseline ethical design requirements for immersive applications. Further, such frameworks may adopt framing strategies that translate legal obligations into concrete reputational damage,

[1]As of August 18, 2023. Overwatch 2 on Steam has received 144,730 reviews from players, with 131,108 being negative (91%), resulting in a "overwhelmingly negative" rating towards the game overall and making it the top 1 worst game on Steam. See: https://store.steampowered.com/app/2357570/Overwatch_2/ and https://steam250.com/bottom100

business risks, and legal penalties to incentivize companies to actively adopt the ethical standards [281]. Such efforts can establish clearer boundaries around acceptable practices, protect vulnerable users (such as children), and foster healthier and ethical industry norms.

8.3 Future Work

To the best of our knowledge, this thesis is an early research-driven study to look into the manifestation of deceptive design directly encountered by market users in commercially available immersive applications. This includes both patterns that migrate from non-immersive platforms and those that may emerge from the unique properties of immersive technologies, and how these designs impact user autonomy in immersive contexts. Building on our preliminary findings in Chapter 7, our immediate next step is completing the data analyses of participants' responses in the remaining four scenarios with the additional four VR privacy mechanisms and deceptive design patterns. With data from all seven scenarios, we will conduct statistical analyses and triangulate the findings between the qualitative and quantitative data. For example, we plan to investigate how demographic characteristics and concerns about deceptive design and privacy influence participants' experiences with VR privacy mechanisms, as well as their perceptions of the privacy impacts of their choices and behaviors. Finally, to ensure our findings have practical relevance, we plan to contrast perspectives between participants who are VR professionals (designers, developers, and researchers) and general users, providing insights that bridge the gap between expert intentions and user experiences. This approach will help us derive guidelines for ethical and effective VR privacy mechanisms that can combat emerging VR deceptive design challenges.

Our research on VR deceptive design is still ongoing. As we write this paper, we are expanding our analysis of deceptive design into more VR applications from more diverse genres and applications from other forms of immersive technologies (e.g., AR, MR), which will allow us to analyze the prevalence of deceptive design that were not present in our Chapter 6 and Chapter 7. This will also enable us to contrast and isolate the manifestations of different types of deceptive designs in applications from similar genres,

or even the same application, across PC and immersive environments, which will result in more meaningful comparisons. We are also in the process of identifying and designing privacy-enhancing alternatives, leveraging the power of choice architecture, as proposed by the choice architecture and nudging literature (as we discussed in Section 2.1.2). In this regard, we have published our initial findings as part of the full papers resulting from Chapter 7.

8.4 Conclusion

Given the limited empirical research on deceptive design in immersive technologies, this thesis investigated how such practices manifest in VR applications and how they affect users' perceptions, behaviors, and digital privacy. We began with a systematic literature review to assess the state-of-the-art research, which revealed a lack of empirical evidence on real-world VR applications and raised concerns about how the vast data collection capabilities of immersive technologies could intensify the impact of deceptive design. To further explore these areas, we conducted an online survey to understand experienced users' awareness of data practices in these technologies. To investigate deceptive design in real-world VR applications, we developed a *Deceptive Design Assessment Guide* and applied it in two exploratory investigations of commercially available VR and computer applications. These studies revealed that many users are unaware of how their data is used in immersive environments and feel resigned to the presence of manipulative design, which they perceive as industry norms. Although many deceptive patterns in VR resemble those found on traditional 2D platforms, VR's sensory immersion, spatial interfaces, and realistic simulations amplify their effects, often leading to greater user discomfort, heightened feelings of manipulation, and a diminished sense of autonomy and trust. The findings from this thesis advance both theoretical understanding and practical approaches for identifying and addressing deceptive design in immersive technologies. It offers actionable recommendations for the future research, design, development, and regulation of immersive technologies to promote ethical design practices, strengthen the regulatory framework, and support user-centered protections. We emphasize that addressing deceptive design in immersive

environments demands interdisciplinary collaborations to protect user autonomy and privacy and create immersive experiences that prioritize user well-being, ethical standards, and transparency in increasingly complex digital environments.

References

[1] Melvin Abraham, Pejman Saeghe, Mark Mcgill, and Mohamed Khamis. Implications of xr on privacy, security and behaviour: Insights from experts. In *Nordic Human-Computer Interaction Conference*, NordiCHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Comput. Surv.*, 50(3), August 2017.

[3] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musabay, Kadeem Pitkin, and Elissa M. Redmiles. Ethics emerging: The story of privacy and security perceptions in virtual reality. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*, SOUPS '18, page 443–458, USA, 2018. USENIX Association.

[4] Ernest Adams and Joris Dormans. *Game mechanics: advanced game design*. New Riders, San Francisco, USA, 2012.

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

[6] Ademola Adeyoju. PRIVACY DARK PATTERNS: A CASE FOR REGULATORY REFORM IN CANADA. https://www.cba.org/Sections/Privacy-and-Access/Resources/Resources/2022/EssayWinner2022Privacy, September 2022. Last accessed on November 28, 2022.

[7] Christopher Alexander. *A pattern language: towns, buildings, construction*. Oxford university press, 1977.

[8] Kati Alha, Elina Koskinen, Janne Paavilainen, Juho Hamari, and Jani Kinnunen. Free-to-play games: Professionals' perspective. In *Proceedings of DiGRA Nordic 2014*, Tampere, Finland, 2014. Nordic Conference of Digital Games Research Association.

[9] Thomas Alsop. Virtual reality (VR) - statistics & facts. https://www.statista.com/topics/2532/virtual-reality-vr/, December 2024. Last accessed on April 29, 2025.

[10] Artillery Intelligence. VR Global Revenue Forecast: 2023-2028. https://artilleryiq.com/reports/vr-global-revenue-forecast-2023-2028/#:~:text=Specifically%2C%20global%20VR%20revenue%20is,as%20mobile%20and%20headworn%20AR., 2024. Last accessed on April 29, 2025.

[11] Anonymous Authors. Anonymous title. In *Proceedings of the 2025 ACM Conference on Computer-Supported Cooperative Work and Social Computing*, CSCW '25. Association for Computing Machinery, 2025. Under review.

[12] Mahdi Azmandian, Mark Hancock, Hrvoje Benko, Eyal Ofek, and Andrew D. Wilson. Haptic retargeting: Dynamic repurposing of passive haptics for enhanced virtual reality experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 1968–1979, New York, NY, USA, 2016. Association for Computing Machinery.

[13] Florian Bemmann, Maximiliane Windl, Jonas Erbe, Sven Mayer, and Heinrich Hussmann. The influence of transparency and control on the willingness of data sharing in adaptive mobile apps. *Proceedings of the ACM on Human-Computer Interaction*, 6(MHCI):1–26, 2022.

[14] Arpit Bhatia, Henning Pohl, Teresa Hirzle, Hasti Seifi, and Kasper Hornbæk. Using the visual language of comics to alter sensations in augmented reality. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery.

[15] Activision Blizzard. Activision blizzard announces second quarter 2023 financial results. https://investor.activision.com/news-releases/news-release-details/activision-blizzard-announces-second-quarter-2023-financial, 2023. Last accessed on July 28, 2023.

[16] Kirsten Boehner, Phoebe Sengers, and Simeon Warner. Interfaces with the ineffable: Meeting aesthetic experience on its own terms. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 15(3):1–29, 2008.

[17] Ian Bogost. *Persuasive games: The expressive power of videogames*. mit Press, 2010.

[18] Arianna Boldi and Amon Rapp. "is it legit, to you?". an exploration of players' perceptions of cheating in a multiplayer video game: Making sense of uncertainty. *International Journal of Human–Computer Interaction*, 0(0):1–21, 2023.

[19] Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig, and Gabriele Lenzini. "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*, DIS '21, page 763–776, New York, NY, USA, 2021. Association for Computing Machinery.

[20] Elise Bonnail, Wen-Jie Tseng, Eric Lecolinet, Samuel Huron, and Jan Gugenheimer. Exploring Memory Manipulation in Extended Reality Using Scenario Construction. *CHI'22 Workshop on Exploring Memory Manipulation in Extended Reality Using Scenario Construction*, 2022.

[21] Ida Borberg, Rene Hougaard, Willard Rafnsson, and Oksana Kulyk. So i sold my soul": Effects of dark patterns in cookie notices on end-user behavior and perceptions. In *Usable Security and Privacy (USEC) Symposium*, volume 2022, 2022.

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

[23] Amel Bourdoucen, Leysan Nurgalieva, and Janne Lindqvist. Privacy is the price: Player views and technical evaluation of data practices in online games. *Proc. ACM Hum.-Comput. Interact.*, 7(CHI PLAY), oct 2023.

[24] H Brignull, M Leiser, C Santos, and K Doshi. Deceptive patterns — user interfaces designed to trick you. https://www.deceptive.design/, April 2023.

[25] Harry Brignull. *Deceptive Patterns—Exposing The Tricks Tech Companies Use To Control You*. Testimonium Ltd, 2023. Upcoming in August 2023.

[26] William H Brown, Raphael C Malveau, Hays W" Skip" McCormick, and Thomas J Mowbray. *AntiPatterns: refactoring software, architectures, and projects in crisis*. John Wiley & Sons, Inc., 1998.

[27] Lauren Buck and Rachel McDonnell. Security and privacy in the metaverse: The threat of the digital human. *CHI EA*, 22, 2022.

[28] Scott Burk. A better statistical method for a/b testing in marketing campaigns. *Marketing Bulletin*, 17, 2006.

[29] California Secretary of State. Bringing Dark Patterns to Light. https://www.ftc.gov/system/files/ftc_gov/pdf/P214800/%20Dark/%20Patterns/%20Report/%209.14.2022/%20-/%20FINAL.pdf, September 2022. 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.

[30] James Calvert and Rhodora Abadia. Impact of immersing university and high school students in educational linear narratives using virtual reality technology. *Computers & Education*, 159:104005, 2020.

[31] Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council. Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans. https://ethics.gc.ca/eng/documents/tcps2-2018-en-interactive-final.pdf, 2018. Last accessed on April 27, 2023.

[32] Jacky C.P. Chan, Howard Leung, Jeff K.T. Tang, and Taku Komura. A virtual reality dance training system using motion capture technology. *IEEE Transactions on Learning Technologies*, 4(2):187–195, 2011.

[33] Kuan-Wen Chen, Yung-Ju Chang, and Liwei Chan. Predicting opportune moments to deliver notifications in virtual reality. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[34] Shi-Yi Chen, Zhe Feng, and Xiaolian Yi. A general introduction to adjustment for multiple comparisons. *Journal of thoracic disease*, 9(6):1725, 2017.

[35] Andrea Chirico, Fabio Lucidi, Michele De Laurentiis, Carla Milanese, Alessandro Napoli, and Antonio Giordano. Virtual reality in health system: beyond entertainment. a mini-review on the efficacy of vr during cancer treatment. *Journal of cellular physiology*, 231(2):275–287, 2016.

[36] Shruthi Sai Chivukula, Jason Brier, and Colin M. Gray. Dark intentions or persuasion? ux designers' activation of stakeholder and user values. In *Proceedings of the 2018 ACM Conference Companion Publication on Designing Interactive Systems*, DIS '18 Companion, page 87–91, New York, NY, USA, 2018. Association for Computing Machinery.

[37] Shruthi Sai Chivukula, Chris Watkins, Lucca McKay, and Colin M. Gray. "nothing comes before profit": Asshole design in the wild. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI EA '19, page 1–6, New York, NY, USA, 2019. Association for Computing Machinery.

[38] Rune Haubo B Christensen. A tutorial on fitting cumulative link mixed models with clmm2 from the ordinal package. *Tutorial for the R Package ordinal*, 1, 2019.

[39] Victoria Clarke, Virginia Braun, and Nikki Hayfield. Thematic analysis. *Qualitative psychology: A practical guide to research methods*, 222(2015):248, 2015.

[40] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. Informing the design of a personalized privacy assistant for the internet of things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery.

[41] Commission nationale de l'informatique et des libertés. 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, December 2021. Last accessed on August 14, 2024.

[42] Nicholas Confessore. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html, 2018. Last accessed on January 4, 2023.

[43] Kimberle Crenshaw. Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stan. L. Rev.*, 43:1241, 1990.

[44] James J Cummings and Jeremy N Bailenson. How immersive is enough? a meta-analysis of the effect of immersive technology on user presence. *Media psychology*, 19(2):272–309, 2016.

[45] James J Cummings and Alexis Shore. 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*, volume 29, 2022.

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

[47] Gregory Day and Abbey Stemler. Are Dark Patterns Anticompetitive? *Ala. L. Rev.*, 72:1, 2020.

[48] Jaybie Agullo de Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. Safemr: Privacy-aware visual information protection for mobile mixed reality. In *2019 IEEE 44th Conference on Local Computer Networks (LCN)*, pages 254–257, Osnabrueck, Germany, 2019. IEEE.

[49] Jaybie Agullo de Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. Security and privacy approaches in mixed reality: A literature survey. *ACM Computing Surveys (CSUR)*, 52(6):1–37, 2019.

[50] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, page 2377–2386, New York, NY, USA, 2014. Association for Computing Machinery.

[51] Christoph Sebastian Deterding, Jaakko Stenros, and Markus Montola. Against "dark game design patterns". In *DiGRA'20-Abstract Proceedings of the 2020 DiGRA International Conference*, Tampere, Finland, 2020. York, DiGRA.

[52] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 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*, CHI '20, page 1–14, New York, NY, USA, 2020. Association for Computing Machinery.

[53] Ellysse Dick. Balancing user privacy and innovation in augmented and virtual reality. Technical report, Information Technology and Innovation Foundation, 2021.

[54] Roberto Dillon. *The digital gaming handbook*. CRC Press, 2020.

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

[56] Youngwook Do, Frederik Brudy, George W Fitzmaurice, and Fraser Anderson. Vice vrsa: Balancing bystander's and vr user's privacy through awareness cues inside and outside vr. In *Graphics Interface 2023-second deadline*, Victoria, BC, Canada, 2023. Canadian Human-Computer Communications Society.

[57] Prakriti Dumaru, Hanieh Atashpanjeh, and Mahdi Nasrullah Al-Ameen. "it's hard for him to make choices sometimes and he needs guidance": Re-orienting parental control for children. *Proc. ACM Hum.-Comput. Interact.*, 8(CSCW1), April 2024.

[58] Ben Egliston and Marcus Carter. Examining visions of surveillance in oculus' data and privacy policies, 2014–2020. *Media International Australia*, 188(1):52–66, 2023.

[59] Stephen R Ellis. Nature and origins of virtual environments: a bibliographical essay. In *Readings in Human–Computer Interaction*, pages 913–932. Elsevier, 1995.

[60] Blizzard Entertainment. Welcome to overwatch 2. https://overwatch.blizzard.com/en-us/news/patch-notes/live/2022/10, October 2022. last accessed on April 12, 2023.

[61] Blizzard Entertainment. Overwatch 2 reveal event recap. https://overwatch.blizzard.com/en-us/news/23814218/overwatch-2-reveal-event-recap/, June 2023. Last accessed on July 4, 2023.

[62] European Parliament, Council of the European Union. 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, October 2022. Last accessed on December 7, 2023.

[63] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng#pbl_1, April 2016. Last accessed on April 29, 2025.

[64] Matthias Fassl and Katharina Krombholz. 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*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[65] Franz Faul, Edgar Erdfelder, Axel Buchner, and Albert-Georg Lang. Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior research methods*, 41(4):1149–1160, 2009.

[66] Federal Trade Commission (FTC). 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, December 2022. Last accessed on Jan 6, 2023.

[67] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 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*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[68] Andy Field, Zoe Field, and Jeremy Miles. *Discovering statistics using R*. Sage, USA, 2012.

[69] Janet Finch. The vignette technique in survey research. *Sociology*, 21(1):105–114, 1987.

[70] Dan Fitton and Janet C. Read. 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*, IDC '19, page 407–418, New York, NY, USA, 2019. Association for Computing Machinery.

[71] Brian J Fogg. Persuasive technology: using computers to change what we think and do. *Ubiquity*, 2002(December):2, 2002.

[72] United States Senator Deb Fischer for Nebraska. SENATORS INTRODUCE BIPARTISAN LEGISLATION TO BAN MANIPULATIVE 'DARK PATTERNS'. https://www.fischer.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns, April 2019. Last accessed on November 28, 2022.

[73] Matija Franklin. Virtual spillover of preferences and behavior from extended reality. In *CHI Conference on Human Factors in Computing Systems (CHI'22),. Association for Computing Machinery, New York, NY, USA*, 2022.

[74] Guo Freeman, Karen Wu, Nicholas Nower, and Donghee Yvette Wohn. Pay to win or pay to cheat: How players of competitive online games perceive fairness of in-game purchases. *Proceedings of the ACM on Human-Computer Interaction*, 6(CHI PLAY):1–24, 2022.

[75] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. Users' expectations about and use of smartphone privacy and security settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[76] Julian Frommel and Regan L Mandryk. 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):1–23, 2022.

[77] Andrea Gallardo, Chris Choy, Jaideep Juneja, Efe Bozkir, Camille Cobb, Lujo Bauer, and Lorrie Cranor. Speculative privacy concerns about ar glasses data collection. *Proceedings on Privacy Enhancing Technologies*, 4:416–435, 2023.

[78] Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides, and Design Patterns. Elements of reusable object-oriented software. *Design Patterns*, 1995.

[79] Vaibhav Garg and Jean Camp. End user perception of online risk under uncertainty. In *2012 45th Hawaii International Conference on System Sciences*, pages 3278–3287, 2012.

[80] Ceenu George, Manuel Demmler, and Heinrich Hussmann. 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*, CHI EA '18, page 1–6, New York, NY, USA, 2018. Association for Computing Machinery.

[81] Alberto Giaretta. Security and Privacy in Virtual Reality–A Literature Survey. *arXiv preprint arXiv:2205.00208*, 2022.

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

[83] Colin M. Gray, Jingle Chen, Shruthi Sai Chivukula, and Liyang Qu. End user accounts of dark patterns as felt manipulation. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW2), oct 2021.

[84] Colin M. Gray, Jingle Chen, Shruthi Sai Chivukula, and Liyang Qu. End user accounts of dark patterns as felt manipulation. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW2), October 2021.

[85] Colin M Gray, Shruthi Sai Chivukula, and Ahreum Lee. What kind of work do" asshole designers" create? describing properties of ethical concern on reddit. In *Proceedings of the 2020 acm designing interactive systems conference*, pages 61–73, 2020.

[86] Colin M. Gray, Ritika Gairola, Nayah Boucaud, Maliha Hashmi, Shruthi Sai Chivukula, Ambika R Menon, and Ja-Nae Duane. Legal trouble?: Ux practitioners' engagement with law and regulation. In *Companion Publication of the 2024 ACM Designing Interactive Systems Conference*, DIS '24 Companion, page 106–110, New York, NY, USA, 2024. Association for Computing Machinery.

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

[88] Colin M Gray, Lorena Sanchez Chamorro, Ike Obi, and Ja-Nae Duane. Mapping the landscape of dark patterns scholarship: A systematic literature review. In *Companion Publication of the 2023 ACM Designing Interactive Systems Conference*, pages 188–193, New York, NY, USA, 2023. Association for Computing Machinery.

[89] Colin M. Gray, Cristiana Teixeira Santos, Nataliia Bielova, and Thomas Mildner. An ontology of dark patterns knowledge: Foundations, definitions, and a pathway for shared knowledge-building. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery.

[90] Paul Graßl, Hanna Schraffenberger, Frederik Zuiderveen Borgesius, and Moniek Buijzen. Dark and bright patterns in cookie consent requests. *Journal of Digital Social Research*, 3(1):1–38, Feb. 2021.

[91] Saul Greenberg, Sebastian Boring, Jo Vermeulen, and Jakub Dostal. Dark patterns in proxemic interactions: A critical perspective. In *Proceedings of the 2014 Conference on Designing Interactive Systems*, DIS '14, page 523–532, New York, NY, USA, 2014. Association for Computing Machinery.

[92] The Guardian. 6x9: A virtual experience of solitary confinement. https://www.theguardian.com/world/ng-interactive/2016/apr/27/6x9-a-virtual-experience-of-solitary-confinement#gvr-more, 2016. Last accessed on January 4, 2023.

[93] Jan Gugenheimer, Wen-Jie Tseng, Abraham Hani Mhaidli, Jan Ole Rixen, Mark McGill, Michael Nebeling, Mohamed Khamis, Florian Schaub, and Sanchari Das. Novel challenges of safety, security and privacy in extended reality. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI EA '22, New York, NY, USA, 2022. Association for Computing Machinery.

[94] Jan Gugenheimer, Wen-Jie Tseng, Abraham Hani Mhaidli, Jan Ole Rixen, Mark McGill, Michael Nebeling, Mohamed Khamis, Florian Schaub, and Sanchari Das. Novel challenges of safety, security and privacy in extended reality. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 1–5, 2022.

[95] Aniket Gulhane, Akhil Vyas, Reshmi Mitra, Roland Oruche, Gabriela Hoefer, Samaikya Valluripally, Prasad Calyam, and Khaza Anuarul Hoque. Security, privacy and safety risk assessment for virtual reality learning environment applications. In *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–9. IEEE, 2019.

[96] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. A comparative study of dark patterns across web and mobile modalities. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW2), oct 2021.

[97] Johanna Gunawan, Cristiana Santos, and Irene Kamara. Redress for dark patterns privacy harms? a case study on consent interactions. In *Proceedings of the 2022 Symposium on Computer Science and Law*, CSLAW '22, page 181–194, New York, NY, USA, 2022. Association for Computing Machinery.

[98] Hana Habib and Lorrie Faith Cranor. Evaluating the usability of privacy choice mechanisms. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS)*, pages 273–289, Boston, MA, 2022. USENIX Association.

[99] Hana Habib, Megan Li, Ellie Young, and Lorrie Cranor. "okay, whatever": An evaluation of cookie consent interfaces. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[100] Hilda Hadan, Lydia Choong, Leah Zhang-Kennedy, and Lennart E. Nacke. Deceived by immersion: A systematic analysis of deceptive design in extended reality. *ACM Comput. Surv.*, 56(10), May 2024.

[101] Hilda Hadan, Nicolas Serrano, and L Jean Camp. A holistic analysis of web-based public key infrastructure failures: comparing experts' perceptions and real-world incidents. *Journal of Cybersecurity*, 7(1):tyab025, 12 2021.

[102] Hilda Hadan, Sabrina A. Sgandurra, Leah Zhang-Kennedy, and Lennart E. Nacke. Culture Clash: When Deceptive Design Meets Diverse Player Expectations. In *Companion Proceedings of the Annual Symposium on Computer-Human Interaction in Play*, CHI PLAY Companion '24, New York, NY, USA, 2024. Association for Computing Machinery.

[103] Hilda Hadan, Sabrina Alicia Sgandurra, Leah Zhang-Kennedy, and Lennart E. Nacke. 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), October 2024.

[104] Hilda Hadan, Derrick M. Wang, Reza Hadi Mogavi, Joseph Tu, Leah Zhang-Kennedy, and Lennart E. Nacke. The great ai witch hunt: Reviewers' perception and (mis)conception of generative ai in researchwriting. *Computers in Human Behavior: Artificial Humans*, 0(0):1–33, 2024.

[105] Hilda Hadan, Derrick M. Wang, Lennart E. Nacke, and Leah Zhang-Kennedy. Privacy in immersive extended reality: Exploring user perceptions, concerns, and coping strategies. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery.

[106] Hilda Hadan, Leah Zhang-Kennedy, and Lennart E. Nacke. 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*, CHI PLAY Companion '24, page 109–123, New York, NY, USA, 2024. Association for Computing Machinery.

[107] Jonathan Haidt, Craig Joseph, et al. The moral mind: How five sets of innate intuitions guide the development of many culture-specific virtues, and perhaps even modules. *The innate mind*, 3:367–391, 2007.

[108] Karin Hammarberg, Maggie Kirkman, and Sheryl de Lacey. Qualitative research methods: when to use them and how to judge them. *Human reproduction*, 31(3):498–501, 2016.

[109] Jon D Hanson and Douglas A Kysar. Taking behavioralism seriously: The problem of market manipulation. *NYUL rev.*, 74:630, 1999.

[110] Gunnar Harboe and Elaine M. Huang. Real-world affinity diagramming practices: Bridging the paper-digital gap. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, page 95–104, New York, NY, USA, 2015. Association for Computing Machinery.

[111] David Harborth and Sebastian Pape. Investigating privacy concerns related to mobile augmented reality apps–a vignette based online experiment. *Computers in Human Behavior*, 122:106833, 2021.

[112] Carrie Heater. Being there: The subjective experience of presence. *Presence Teleoperators Virtual Environ.*, 1(2):262–271, 1992.

[113] Morton L Heilig. Sensorama simulator. *US PAT. 3,050,870*, 1962.

[114] Brittan Heller. Watching androids dream of electric sheep: Immersive technology, biometric psychography, and the law. *Vand. J. Ent. & Tech. L.*, 23:1, 2020.

[115] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. Amazon vs. my brother: How users of shared smart speakers perceive and cope with privacy risks. In *Proceedings of the 2020 CHI conference on human factors in computing systems*, pages 1–13, New York, NY, USA, 2020. Association for Computing Machinery.

[116] Julien Huart, Christophe Kolski, and Mouldi Sagar. Evaluation of multimedia applications using inspection methods: the cognitive walkthrough case. *Interacting with computers*, 16(2):183–215, 2004.

[117] C. Hummels and P.J. Stappers. Meaningful gestures for human computer interaction: beyond hand postures. In *Proceedings Third IEEE International Conference on Automatic Face and Gesture Recognition*, pages 591–596, 1998.

[118] IGN Southeast Asia. Overwatch 2, world of warcraft, and hearthstone shut down in china. https://sea.ign.com/activision-blizzard/194620/news/overwatch-2-world-of-warcraft-and-hearthstone-shut-down-in-china, 2024. Last accessed on May 4, 2024.

[119] Brent Edward Insko. *Passive haptics significantly enhances virtual environments*. The University of North Carolina at Chapel Hill, 2001.

[120] Sven Joeckel, Nicholas David Bowman, and Leyla Dogruel. Gut or game? the influence of moral intuitions on decisions in video games. *Media psychology*, 15(4):460–485, 2012.

[121] Skyler Johnson, Katherine Ferro, L. Jean Camp, and Hilda Hadan. Human and organizational factors in public key certificate authority failures. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, CCS '21, page 2414–2416, New York, NY, USA, 2021. Association for Computing Machinery.

[122] Christine Jolls, Cass R Sunstein, and Richard Thaler. A behavioral approach to law and economics. *StAn. l. reV.*, 50:1471, 1997.

[123] Joseph B Kadane and Nicole A Lazar. Methods and criteria for model selection. *Journal of the American statistical Association*, 99(465):279–290, 2004.

[124] Daniel Kahneman and Amos Tversky. Prospect theory: An analysis of decision under risk. In *Handbook of the fundamentals of financial decision making: Part I*, pages 99–127. World Scientific, 2013.

[125] Kan_G3. Popup notification while playing vr. Reddit. https://www.reddit.com/r/HPReverb/comments/lrfcq0/popup_notification_while_playing_vr/, 2021. Last accessed on January 26, 2023.

[126] E Ann Kaplan. *Trauma culture: The politics of terror and loss in media and literature*. Rutgers University Press, 2005.

[127] Faltin Karlsen. 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, 02 2019.

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

[129] John King, Dan Fitton, and Brendan Cassidy. Investigating players' perceptions of deceptive design practices within a 3d gameplay context. *Proc. ACM Hum.-Comput. Interact.*, 7(CHI PLAY), oct 2023.

[130] Marshall Kirkpatrick. Your Memories Will Be Rewritten: Mozilla's Raskin Says Product Placement is Coming Soon to Your Facebook Photos. readwrite. https://readwrite.com/facebook_product_placement/, 2010. Last accessed on January 6, 2023.

[131] Bastian Kordyaka, Samuli Laato, Katharina Jahn, Juho Hamari, and Bjoern Niehaves. The cycle of toxicity: Exploring relationships between personality and player roles in toxic behavior in multiplayer online battle arena games. *Proceedings of the ACM on Human-Computer Interaction*, 7(CHI PLAY):611–641, 2023.

[132] Veronika Krauss. Exploring dark patterns in xr. In *Proceedings of the 1st Workshop on Novel Challenges of Safety, Security and Privacy in Extended Reality, CHI Extended Abstracts (CHIEA'22). ACM*, volume 3, page 4, 2022.

[133] Veronika Krauss, Pejman Saeghe, Alexander Boden, Mohamed Khamis, Mark McGill, Jan Gugenheimer, and Michael Nebeling. 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. Just Accepted.

[134] Veronika Krauss, Pejman Saeghe, Alexander Boden, Mohamed Khamis, Mark McGill, Jan Gugenheimer, and Michael Nebeling. What makes xr dark? examining emerging dark patterns in augmented and virtual reality through expert co-design. *ACM Transactions on Computer-Human Interaction*, 2024.

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

[136] Samuli Laato, Daniel Fernández Galeote, Ferran Altarriba Bertran, and Juho Hamari. Balancing the augmented experience: design tensions in the location-based game pikmin bloom. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 1–7, 2022.

[137] Alison Landsberg. *Prosthetic memory: The transformation of American remembrance in the age of mass culture*. Columbia University Press, 2004.

[138] Kung Wong Lau and Pui Yuen Lee. The use of virtual reality for creating unusual environmental stimulation to motivate students to explore creative ideas. *Interactive Learning Environments*, 23(1):3–18, 2015.

[139] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. Towards security and privacy for multi-user augmented reality: Foundations with end users. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 392–408. IEEE, 2018.

[140] Hosub Lee and Alfred Kobsa. Understanding user privacy in internet of things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 407–412, Reston, VA, USA, 2016. IEEE.

[141] Hyunjoo Lee, Jiyeon Lee, Daejun Kim, Suman Jana, Insik Shin, and Sooel Son. AdCube:WebVR Ad Fraud and Practical Confinement of Third-Party Ads. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 2543–2560, 2021.

[142] Pedro Giovanni Leon, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, and Lorrie Faith Cranor. What matters to users? factors that affect

users' willingness to share information with online advertisers. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, New York, NY, USA, 2013. Association for Computing Machinery.

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

[144] Clayton Lewis, Peter G Polson, Cathleen Wharton, and John Rieman. Testing a walkthrough methodology for theory-based design of walk-up-and-use interfaces. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 235–242, 1990.

[145] Jie Li, Vinoba Vinayagamoorthy, Julie Williamson, David A. Shamma, and Pablo Cesar. Social vr: A new medium for remote communication and collaboration. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI EA '21, New York, NY, USA, 2021. Association for Computing Machinery.

[146] Holin Lin and Chuen-Tsai Sun. Cash trade in free-to-play online games. *Games and Culture*, 6(3):270–287, 2011.

[147] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM conference on ubiquitous computing*, pages 501–510, New York, NY, USA, 2012. Association for Computing Machinery.

[148] Shiguang Liu and Dinesh Manocha. Sound synthesis, propagation, and rendering: a survey. *arXiv preprint arXiv:2011.05538*, 2020.

[149] Jamie Luguri and Lior Jacob Strahilevitz. Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1):43–109, 2021.

[150] Kai Lukoff, Alexis Hiniker, Colin M. Gray, Arunesh Mathur, and Shruthi Sai Chivukula. What can chi do about dark patterns? In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI EA '21, New York, NY, USA, 2021. Association for Computing Machinery.

[151] Aditi M. Bhoot, Mayuri A. Shinde, and Wricha P. Mishra. Towards the identification of dark patterns: An analysis based on end-user reactions. In *Proceedings of the 11th Indian Conference on Human-Computer Interaction*, IndiaHCI '20, page 24–33, New York, NY, USA, 2021. Association for Computing Machinery.

[152] Eryn Ma and Eleanor Birrell. Prospective consent: The effect of framing on cookie consent decisions. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI EA '22, New York, NY, USA, 2022. Association for Computing Machinery.

[153] Cayley MacArthur, Arielle Grinberg, Daniel Harley, and Mark Hancock. You're making me sick: A systematic review of how virtual reality research considers gender & cybersickness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–15, New York, NY, USA, 2021. Association for Computing Machinery.

[154] Maximilian Maier. Dark patterns–an end user perspective, 2019.

[155] Ville Mäkelä, Cayley MacArthur, Jieun Lee, and Daniel Harley. Integrating virtual reality head-mounted displays into higher education classrooms on a large scale. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, New York, NY, USA, 2025. Association for Computing Machinery.

[156] Naresh K Malhotra, Sung S Kim, and James Agarwal. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information systems research*, 15(4):336–355, 2004.

[157] Divine Maloney, Guo Freeman, and Andrew Robb. Social virtual reality: ethical considerations and future directions for an emerging research space. In *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pages 271–277, Lisbon, Portugal, 2021. IEEE.

[158] Divine Maloney, Guo Freeman, and Andrew Robb. Stay connected in an immersive world: Why teenagers engage in social virtual reality. In *Interaction Design and Children*, pages 69–79, 2021.

[159] Divine Maloney, Samaneh Zamanifard, and Guo Freeman. Anonymity vs. familiarity: Self-disclosure and privacy in social virtual reality. In *Proceedings of the 26th ACM Symposium on Virtual Reality Software and Technology*, pages 1–9, 2020.

[160] Steve Mann, Phillip V Do, Tom Furness, Yu Yuan, Jay Iorio, and Zixin Wang. Fundamentals of all the realities: Virtual, augmented, mediated, multimediated, and beyond. In *Springer Handbook of Augmented Reality*, pages 3–34. Springer, 2023.

[161] Steve Mann, Tom Furness, Yu Yuan, Jay Iorio, and Zixin Wang. All reality: Virtual, augmented, mixed (x), mediated (x, y), and multimediated reality. *arXiv preprint arXiv:1804.08386*, 2018.

[162] Arunesh Mathur, Gunes Acar, Michael J Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. Dark patterns at scale: Findings from a crawl of 11k shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–32, 2019.

[163] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 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*, pages 1–18, 2021.

[164] Tim May, Beth Perry, et al. Reflexivity and the practice of qualitative research. *The SAGE handbook of qualitative data analysis*, 109:109–122, 2014.

[165] Richard McPherson, Suman Jana, and Vitaly Shmatikov. No escape from reality: Security and privacy of augmented reality browsers. In *Proceedings of the 24th International Conference on World Wide Web*, WWW '15, page 743–753, Republic and Canton of Geneva, CHE, 2015. International World Wide Web Conferences Steering Committee.

[166] Aline Menin, Rafael Torchelsen, and Luciana Nedel. An analysis of vr technology used in immersive simulations with a serious game perspective. *IEEE Computer Graphics and Applications*, 38(2):57–73, 2018.

[167] Meta. Testing In-Headset VR Ads. Meta Quest Blog. https://www.meta.com/blog/quest/testing-in-headset-vr-ads/, June 2021. Last accessed on Feburary 15, 2023.

[168] Meta Quest Blog. First Look at the Rift, Shipping Q1 2016. Meta. https://www.meta.com/blog/quest/first-look-at-the-rift-shipping-q1-2016/, 2015. Last accessed on February 24, 2023.

[169] Abraham Hani Mhaidli and Florian Schaub. Identifying manipulative advertising techniques in xr through scenario construction. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–18, 2021.

[170] Thomas Mildner, Merle Freye, Gian-Luca Savino, Philip R. Doyle, Benjamin R. Cowan, and Rainer Malaka. Defending against the dark arts: Recognising dark patterns in social media. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*, DIS '23, page 2362–2374, New York, NY, USA, 2023. Association for Computing Machinery.

[171] Thomas Mildner, Gian-Luca Savino, Philip R. Doyle, Benjamin R. Cowan, and Rainer Malaka. 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*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[172] Paul Milgram, Haruo Takemura, Akira Utsumi, and Fumio Kishino. Augmented reality: A class of displays on the reality-virtuality continuum. In *Telemanipulator and telepresence technologies*, volume 2351, pages 282–292. Spie, 1995.

[173] Mark Roman Miller, Fernanda Herrera, Hanseul Jun, James A Landay, and Jeremy N Bailenson. Personal identifiability of user tracking data during observation of 360-degree vr video. *Scientific Reports*, 10(1):1–10, 2020.

[174] Stuart Mills. Personalized nudging. *Behavioural Public Policy*, 6(1):150–159, 2022.

[175] Stuart Mills. Deceptive choice architecture and behavioral audits: A principles-based approach. *Regulation & Governance*, 18(4):1426–1441, 2024.

[176] Thomas B. Moeslund and Erik Granum. A survey of computer vision-based human motion capture. *Computer Vision and Image Understanding*, 81(3):231–268, 2001.

[177] Alberto Monge Roffarello, Kai Lukoff, and Luigi De Russis. Defining and identifying attention capture deceptive designs in digital interfaces. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[178] Jesper Mortensen, Vinoba Vinayagamoorthy, Mel Slater, Anthony Steed, Benjamin Lok, and MC Whitton. Collaboration in tele-immersive environments. In *EGVE*, volume 2, pages 93–101, 2002.

[179] Mozilla Foundation. Privacy Not Included — Make smart choices to protect your privacy. Search for products. Read expert reviews. Get tips and tricks. https://www.mozillafoundation.org/en/privacynotincluded/, n.d. Last accessed on May 9, 2025.

[180] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an IoT world. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 399–412, 2017.

[181] Arvind Narayanan, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. Dark patterns: Past, present, and future: The evolution of tricky user interfaces. *Queue*, 18(2):67–92, 2020.

[182] Bonnie Nardi. *My life as a night elf priest: An anthropological account of World of Warcraft.* University of Michigan Press, MI, USA, 2010.

[183] Bonnie Nardi and Justin Harris. Strangers and friends: collaborative play in world of warcraft. In *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work*, CSCW '06, page 149–158, New York, NY, USA, 2006. Association for Computing Machinery.

[184] Bonnie A Nardi, Stella Ly, and Justin Harris. Learning conversations in world of warcraft. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, pages 79–79, New Jersey, United States, 2007. IEEE.

[185] Carman Neustaedter and Phoebe Sengers. Autobiographical design: what you can learn from designing for yourself. *interactions*, 19(6):28–33, 2012.

[186] Anton Nijholt, Ronald C. Arkin, Sébastien Brault, Richard Kulpa, Franck Multon, Benoit Bideau, David Traum, Hayley Hung, Eugene Santos, Deqing Li, Fei Yu, Lina Zhou, and Dongsong Zhang. Trends & Controversies. *IEEE Intelligent Systems*, 27(6):60–75, 2012.

[187] Helen Nissenbaum. Privacy as contextual integrity. *Washington Law Review*, 79:119, 2004.

[188] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. Dark patterns after the gdpr: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery.

[189] Ike Obi, Colin Gray, Shruthi Chivukula, Ja-Nae Duane, Janna Johns, Matthew Will, Ziqing Li, and Thomas Carlock. Tracing the history and evolution of dark patterns on twitter from 2010-2021. *Trans. Soc. Comput.*, 8(3–4), March 2025.

[190] Kyle O'Brien. Coca-cola embraces augmented reality with interactive experience. The Drum. https://www.thedrum.com/news/2019/09/10/coca-cola-embraces-ar-interactive-experience, September 2019. Last accessed on January 6, 2023.

[191] Oculus. Oculus Rift: Step Into the Game. `https://www.kickstarter.com/projects/1523379957/oculus-rift-step-into-the-game`, 2012. Last accessed on December 31, 2022.

[192] OECD. Dark commercial patterns. Technical Report 336, OECD Publishing, Paris, 2022.

[193] California Secretary of State 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, 2020. 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.

[194] Office of the Privacy Commissioner of Canada. 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/, March 2024. Last accessed on Apr 29, 2025.

[195] Office of the Arizona Attorney General. Attorney General Mark Brnovich achieves historic $85 million settlement with Google, October 2022. Accessed: [Insert access date here].

[196] Office of the Privacy Commissioner of Canada. OPC Sweep Report 2024: Deceptive Design Patterns. Technical report, Office of the Privacy Commissioner of Canada, Ottawa, Canada, 2024.

[197] Joseph O'Hagan, Pejman Saeghe, Jan Gugenheimer, Daniel Medeiros, Karola Marky, Mohamed Khamis, and Mark McGill. Privacy-enhancing technology and everyday augmented reality: Understanding bystanders' varying needs for awareness and consent. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 6(4):1–35, 2023.

[198] Antti Oulasvirta, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. Long-term effects of ubiquitous surveillance in the home. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pages 41–50, New York, NY, USA, 2012. Association for Computing Machinery.

[199] Sharon Oviatt. Human-centered design meets cognitive load theory: designing interfaces that help people think. In *Proceedings of the 14th ACM International Conference on Multimedia*, MM '06, page 871–880, New York, NY, USA, 2006. Association for Computing Machinery.

[200] Fiachra O'Brolcháin, Tim Jacquemard, David Monaghan, Noel O'Connor, Peter Novitzky, and Bert Gordijn. The convergence of virtual reality and social networks: threats to privacy and autonomy. *Science and engineering ethics*, 22(1):1–29, 2016.

[201] Matthew J Page, Joanne E McKenzie, Patrick M Bossuyt, Isabelle Boutron, Tammy C Hoffmann, Cynthia D Mulrow, Larissa Shamseer, Jennifer M Tetzlaff, Elie A Akl, Sue E Brennan, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Systematic reviews*, 10(1):1–11, 2021.

[202] Zhigeng Pan, Adrian David Cheok, Hongwei Yang, Jiejie Zhu, and Jiaoying Shi. Virtual reality and mixed reality for virtual learning environments. *Computers & graphics*, 30(1):20–28, 2006.

[203] Sameer Patil, Roberto Hoyle, Roman Schlegel, Apu Kapadia, and Adam J Lee. Interrupt now or inform later? comparing immediate and delayed privacy feedback. In *Proceedings of the 33rd Annual*

ACM Conference on Human Factors in Computing Systems, pages 1415–1418, New York, NY, USA, 2015. Association for Computing Machinery.

[204] Elena Petrovskaya. Ask the players! player-centric principles as guidelines for ethical microtransactions. *ACM Games*, 2(2), aug 2024.

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

[206] Ken Pfeuffer, Matthias J Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 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*, pages 1–12, 2019.

[207] Ismo Rakkolainen, Ahmed Farooq, Jari Kangas, Jaakko Hakulinen, Jussi Rantala, Markku Turunen, and Roope Raisamo. Technologies for multimodal interaction in extended reality—a scoping review. *Multimodal Technologies and Interaction*, 5(12):81, 2021.

[208] Erick Jose Ramirez, Miles Elliott, and Per-Erik Milam. What it's like to be a _: why it's (often) unethical to use VR as an empathy nudging tool. *Ethics and Information Technology*, 23(3):527–542, 2021.

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

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

[211] Amon Rapp. Autoethnography in human-computer interaction: Theory and practice. *New directions in third wave human-computer interaction: Volume 2-Methodologies*, pages 25–42, 2018.

[212] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Art. 25 GDPRData protection by design and by default, April 2016.

[213] Daniel Reinhardt, Johannes Borchard, and Jörn Hurtienne. Visual interactive privacy policy: The better choice? In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[214] Muhammad Nazhif Rizani, Mohd Nor Akmal Khalid, Hiroyuki Iida, and Reza Firsandaya Malik. Analysis of business model transition based on active user and review value. In *Proceedings of the 15th International Conference on the Foundations of Digital Games*, pages 1–4, New York, USA, 2020. ACM.

[215] Richard Rodriguez, Brian T. Sullivan, Mayra Donaji Barrera Machuca, Anil Ufuk Batmaz, Cyane Tornatzky, and Francisco R. Ortega. An artists' perspectives on natural interactions for virtual reality 3d sketching. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery.

[216] Franziska Roesner, Tadayoshi Kohno, and David Molnar. Security and privacy for augmented reality systems. *Communications of the ACM*, 57(4):88–96, 2014.

[217] Katja Rogers, Sukran Karaosmanoglu, Maximilian Altmeyer, Ally Suarez, and Lennart E Nacke. Much Realistic, Such Wow! A Systematic Literature Review of Realism in Digital Games. In *CHI Conference on Human Factors in Computing Systems*, pages 1–21, New York, NY, USA, 2022. Association for Computing Machinery.

[218] Arianna Rossi, Rachele Carli, Marietjie W Botes, Angelica Fernandez, Anastasia Sergeeva, and Lorena Sánchez Chamorro. Who is vulnerable to deceptive design patterns? a transdisciplinary perspective on the multi-dimensional nature of digital vulnerability. *Computer Law & Security Review*, 55:106031, 2024.

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

[220] Rufat Rzayev, Sven Mayer, Christian Krauter, and Niels Henze. Notification in vr: The effect of notification placement, task and environment. In *Proceedings of the Annual Symposium on Computer-Human Interaction in Play*, CHI PLAY '19, page 199–211, New York, NY, USA, 2019. Association for Computing Machinery.

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

[222] J.K. Salisbury and M.A. Srinivasan. Phantom-based haptic interaction with virtual objects. *IEEE Computer Graphics and Applications*, 17(5):6–10, 1997.

[223] Hauke Sandhaus. Promoting bright patterns. CHI '23 Workshop: Designing Technology and Policy Simultaneously, 2023.

[224] Lauri Savioja and U Peter Svensson. Overview of geometrical room acoustic modeling techniques. *The Journal of the Acoustical Society of America*, 138(2):708–730, 2015.

[225] René Schäfer, Paul Miles Preuschoff, René Röpke, Sarah Sahabi, and Jan Borchers. Fighting malicious designs: Towards visual countermeasures against dark patterns. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery.

[226] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In *Eleventh Symposium on Usable Privacy and Security (SOUPS)*, pages 1–17, Ottawa, Canada, 2015. USENIX Association.

[227] Raphael Schlembach and Nicola Clewer. 'Forced empathy': Manipulation, trauma and affect in virtual reality film. *International Journal of Cultural Studies*, 24(5):827–843, 2021.

[228] Evan Selinger and Kyle Powys Whyte. Competence and trust in choice architecture. *Knowledge, Technology & Policy*, 23(3):461–482, 2010.

[229] Daniel M Shafer, Corey P Carbonara, and Michael F Korpi. Factors affecting enjoyment of virtual reality games: a comparison involving consumer-grade virtual reality technology. *Games for health journal*, 8(1):15–23, 2019.

[230] Michael A Shapiro and Annie Lang. Making television reality: Unconscious processes in the construction of social reality. *Communication research*, 18(5):685–705, 1991.

[231] Joon-Ho Shin, Si Bog Park, and Seong Ho Jang. Effects of game-based virtual reality on health-related quality of life in chronic stroke patients: a randomized, controlled study. *Computers in biology and medicine*, 63:92–98, 2015.

[232] Ramin Shokrizade. The top f2p monetization tricks. https://www.gamedeveloper.com/business/the-top-f2p-monetization-tricks, 2013. Last accessed on July 24, 2023.

[233] Herbert Alexander Simon. *Models of bounded rationality: Empirically grounded economic reason*, volume 3. MIT press, 1997.

[234] Richard Skarbez, Missie Smith, and Mary C Whitton. Revisiting milgram and kishino's reality-virtuality continuum. *Frontiers in Virtual Reality*, 2:647997, 2021.

[235] Mel Slater. A note on presence terminology. *Presence connect*, 3(3):1–5, 2003.

[236] Mel Slater. Place illusion and plausibility can lead to realistic behaviour in immersive virtual environments. *Philosophical Transactions of the Royal Society B: Biological Sciences*, 364(1535):3549–3557, 2009.

[237] Mel Slater and Sylvia Wilbur. A framework for immersive virtual environments (five): Speculations on the role of presence in virtual environments. *Presence: Teleoperators and Virtual Environments*, 6(6):603–616, 12 1997.

[238] N Craig Smith, Daniel G Goldstein, and Eric J Johnson. Choice without awareness: Ethical and policy implications of defaults. *Journal of Public Policy & Marketing*, 32(2):159–172, 2013.

[239] Than Htut Soe, Oda Elise Nordberg, Frode Guribye, and Marija Slavkovik. 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*, pages 1–12, 2020.

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

[241] Maximilian Speicher, Brian D Hall, and Michael Nebeling. What is mixed reality? In *Proceedings of the 2019 CHI conference on human factors in computing systems*, pages 1–15, 2019.

[242] State of California. AB-2273 The California Age-Appropriate Design Code Act. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273, September 2022. Last accessed on April 29, 2025.

[243] Statista.com. Reddit - statistics & facts. statista.com. https://www.statista.com/topics/5672/reddit/#topicOverview, March 2024. Last accessed on April 2024.

[244] Frank Steinicke. *Being really virtual*. Springer, 2016.

[245] Zihao Su, Faysal Hossain Shezan, Yuan Tian, David Evans, and Seongkook Heo. 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*, 2022.

[246] Jenny Sundén. Desires at play: On closeness and epistemological uncertainty. *Games and Culture*, 7(2):164–184, 2012.

[247] Cass R Sunstein. *Why nudge?: The politics of libertarian paternalism*. Yale University Press, New Haven, Connecticut, USA, 2014.

[248] Cass R Sunstein. Fifty shades of manipulation. *1 J. Marketing Behav. 213 (2016)*, 2015.

[249] Cass R Sunstein. Sludge audits. *Behavioural Public Policy*, 6(4):654–673, 2022.

[250] Daniel Susser, Beate Roessler, and Helen Nissenbaum. Online manipulation: Hidden influences in a digital world. *Geo. L. Tech. Rev.*, 4:1, 2019.

[251] Ivan E Sutherland et al. The ultimate display. In *Proceedings of the IFIP Congress*, volume 2, pages 506–508. New York, 1965.

[252] Richard H Thaler. Nudge, not sludge, 2018.

[253] Richard H Thaler and Cass R Sunstein. Nudge: Improving decisions about health, wealth, and happiness.

[254] Richard H Thaler and Cass R Sunstein. *Nudge: Improving decisions about health, wealth, and happiness*. Penguin, London, United Kingdom, 2009.

[255] Richard H Thaler, Cass R Sunstein, and John P Balz. *Choice architecture*, volume 2013. Princeton University Press Princeton, NJ, 2013.

[256] the Consumer Council of Norway (Forbrukerrådet). Deceived by design – How tech companies use dark patterns to discourage us from exercising our rights to privacy. https://www.conpolicy.de/en/news-detail/deceived-by-design-how-tech-companies-use-dark-patterns-to-discourage-us-from/exercising-our-right, July 2018. Last accessed on January 4, 2023.

[257] The European Consumer Organisation. Monetising Play: Regulating in-game and in-app premium currencies. https://www.beuc.eu/position-papers/monetising-play-regulating-game-and-app-premium-currencies, September 2024. Last Accesed on September 12, 2024.

[258] the White House. President Obama: "Why We Must Rethink Solitary Confinement". https://obamawhitehouse.archives.gov/blog/2016/01/26/president-obama-why-we-must-rethink-solitary-confinement, January 2016. Last accessed on July, 14 2023.

[259] The XR Safety Initiative (XRSI). 1st XR Data Classification Roundtable Report. Xr safety week 2021, The XR Safety Initiative (XRSI), Deccember 2021. Last accessed on October 20th, 2022.

[260] Bruce H Thomas. A survey of visual, mixed, and augmented reality gaming. *Computers in Entertainment (CIE)*, 10(1):1–33, 2012.

[261] James Thomas and Angela Harden. Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC medical research methodology*, 8(1):1–10, 2008.

[262] Krill Tokarev. Technical and Visual Analysis of Overwatch. https://80.lv/articles/overwatch-technical-overview/, May 2016. Last accessed on August 30, 2023.

[263] Niklas Torstensson, Tarja Susi, Ulf Wilhelmsson, and Mikael Lebram. Wizard of Oz and the design of a multi-player mixed reality game. In *International Conference on Human-Computer Interaction*, pages 218–232, Berlin, Germany, 2020. Springer.

[264] Rahmadi Trimananda, Hieu Le, Hao Cui, Janice Tran Ho, Anastasia Shuba, and Athina Markopoulou. {OVRseen}: Auditing network traffic and privacy policies in oculus {VR}. In *31st USENIX security symposium (USENIX security 22)*, pages 3789–3806, 2022.

[265] Rahmadi Trimananda, Hieu Le, Hao Cui, Janice Tran Ho, Anastasia Shuba, and Athina Markopoulou. OVRseen: Auditing network traffic and privacy policies in oculus VR. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 3789–3806, Boston, MA, 8 2022. USENIX Association.

[266] Hellen Truong and Axel Dalbard. Bright patterns as an ethical approach to counteract dark patterns: A closer investigation of the ethics of persuasive design, 2022.

[267] Janice Y Tsai, Patrick Kelley, Paul Drielsma, Lorrie Faith Cranor, Jason Hong, and Norman Sadeh. Who's viewed you? the impact of feedback in a mobile location-sharing application. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2003–2012, New York, NY, USA, 2009. Association for Computing Machinery.

[268] Sarah Turner, Jason RC Nurse, and Shujun Li. "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*, pages 1–8, New York, NY, USA, 2022. ACM.

[269] Brygg Ullmer and Hiroshi Ishii. Emerging frameworks for tangible user interfaces. *IBM systems journal*, 39(3.4):915–931, 2000.

[270] United for Literacy. Adult literacy skills for success: 2022 national report. Technical report, United for Literacy, Canada, 2022.

[271] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (un)informed consent: Studying gdpr consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, page 973–990, New York, NY, USA, 2019. Association for Computing Machinery.

[272] Tetiana A Vakaliuk, Larysa D Shevchuk, Borys V Shevchuk, et al. Possibilities of using ar and vr technologies in teaching mathematics to high school students. *Universal Journal of Educational Research*, 8(11B):6280–6288, 2020.

[273] Max Van Kleek, Ilaria Liccardi, Reuben Binns, Jun Zhao, Daniel J Weitzner, and Nigel Shadbolt. Better the devil you know: Exposing the data sharing practices of smartphone apps. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 5208–5220, New York, NY, USA, 2017. Association for Computing Machinery.

[274] Scott J Vitell. Consumer ethics research: Review, synthesis and suggestions for the future. *Journal of business ethics*, 43:33–47, 2003.

[275] Scott J Vitell and James Muncy. Consumer ethics: An empirical investigation of factors influencing ethical judgments of the final consumer. *Journal of Business Ethics*, 11:585–597, 1992.

[276] Ari Ezra Waldman. Cognitive biases, dark patterns, and the 'privacy paradox'. *Current opinion in psychology*, 31:105–109, 2020.

[277] Xian Wang, Lik-Hang Lee, Carlos Bermejo Fernandez, and Pan Hui. The dark side of augmented reality: Exploring manipulative designs in ar. *International Journal of Human–Computer Interaction*, pages 1–16, 2023.

[278] Kevin D Williams. The effects of dissociation, game controllers, and 3D versus 2D on presence and enjoyment. *Computers in Human Behavior*, 38:142–150, 2014.

[279] Shane Williams. The Potential Power Of Data: Hyper-Personalization For Each And Every Client. Forbes Technology Council. https://www.forbes.com/sites/forbestechcouncil/2022/06/22/the-potential-power-of-data-hyper-personalization-for-each-and-every-client/?sh=3d162b4c5545, 2022. Last accessed on January 6, 2023.

[280] Maximiliane Windl, Anna-Marie Ortloff, Niels Henze, and Valentin Schwind. Privacy at a glance: A process to learn modular privacy icons during web browsing. In *Proceedings of the 2022 Conference on Human Information Interaction and Retrieval*, CHIIR '22, page 102–112, New York, NY, USA, 2022. Association for Computing Machinery.

[281] Richmond Y. Wong, Andrew Chong, and R. Cooper Aspegren. Privacy legislation as business risks: How gdpr and ccpa are represented in technology companies' investment risk disclosures. *Proc. ACM Hum.-Comput. Interact.*, 7(CSCW1), April 2023.

[282] Robert F Woolson. Wilcoxon signed-rank test. *Encyclopedia of Biostatistics*, 8, 2005.

[283] Robert F Woolson. Wilcoxon signed-rank test, 2007.

[284] XR Safety Initiative (XRSI). The XRSI Definition of Extended Reality (XR). XR Safety Initiative Standard Publication XR 001, The XR Safety Initiative (XRSI), March 2020. Last accessed on October 16th, 2022.

[285] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 chi conference on human factors in computing systems*, pages 1–12, New York, NY, USA, 2019. Association for Computing Machinery.

[286] Johannes Zachrisson, Gøril Storrø, and Casper Boks. Using a guide to select design strategies for behaviour change; theory vs. practice. In Mitsutaka Matsumoto, Yasushi Umeda, Keijiro Masui, and Shinichi Fukushige, editors, *Design for Innovative Value Towards a Sustainable Society*, pages 362–367, Dordrecht, 2012. Springer Netherlands.

[287] José P Zagal, Staffan Björk, and Chris Lewis. Dark patterns in the design of games. In *Foundations of Digital Games 2013*, 2013.

[288] André Zenner, Marco Speicher, Sören Klingner, Donald Degraen, Florian Daiber, and Antonio Krüger. Immersive notification framework: Adaptive & plausible notifications in virtual reality. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI EA '18, page 1–6, New York, NY, USA, 2018. Association for Computing Machinery.

[289] Leah Zhang-Kennedy, Maxwell Keleher, and Michaela Valiquette. Navigating the gray: Design practitioners' perceptions toward the implementation of privacy dark patterns. *Proc. ACM Hum.-Comput. Interact.*, 8(CSCW1), April 2024.

[290] Leah Zhang-Kennedy, Michaela Valiquette, An Bella Chen, Hilda Hadan, and Sangho Suh. Folk tales of iot: Understanding the impact of stories on users' positive and negative perceptions of smart home iot devices. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, pages 1–18, 2025.

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

APPENDICES

Appendix A

Reflexivity Statement

To ensure the rigor of the qualitative research in this thesis, we follow literature's recommendations [164, 221] and provide a *Reflexivity Statement*. This statement acknowledges the potential biases that may influence qualitative data coding and theme development process due to H. Hadan's cultural background, educational training, and experience with computer and VR games and non-game applications. The thematic analyses in Chapter 3, Chapter 4, Chapter 6, Chapter 5, and Chapter 7 were led by H. Hadan, who has a strong research background in deceptive design, with prior publications on this topic in both Extended Reality environments (including VR) and traditional PC-based games [100, 103, 102, 11]. H. Hadan also has several years of experience researching privacy and security issues from a user-centered perspective [101, 105, 290]. This interdisciplinary background and experience align well with the goal of this thesis, as identifying the manifestation and impact of deceptive designs require consideration of both design mechanisms and user perspectives.

The autoethnography methodology in Chapter 6 and Chapter 7 puts H. Hadan into a first-hand user perspective. While H. Hadan's expertise and extensive experience in deceptive design ensured a rich identification of these patterns in the applications, we still note that her personality might have influenced the focus and the interpretation of autoethnographic data. Hadan, as a user, identified herself as empathetic and sensitive and tend to be caring and compassionate. This personality allowed for picking up on subtle emotional manipulation and patterns that exploit users' attachment to in-game characters.

In addition, H. Hadan has a strong focus on observable facts and more straightforward outcomes based on concrete evidence. While this personality might have limited H. Hadan's interpretation of hypothetical future consequences of deceptive design, her expertise enabled a thorough understanding of user manipulation currently in the games and applications.

We also note that H. Hadan's personal experience with the computer and VR games and non-game applications has influenced this research. Introduced to video games at a young age, H. Hadan has engaged with a diverse array of North American and Asian titles across multiple genres, primarily on PC and PlayStation platforms. In 2017, she began playing *Overwatch*, a game that became a medium for reconnecting with her family members during the COVID-19 pandemic, until the game's servers were shut down in China in 2023 [118]. To date, H. Hadan has played *Overwatch* (both *OW1* and *OW2*) for about 7 years, over 3,000 hours of gameplay in different game modes and characters. Her personal experience of before and after the integration of deceptive design into the game enhanced her understanding of how manipulative tactics can negatively impact users. In 2023, H. Hadan began exploring user privacy perceptions and concerns in immersive technology and conducted studies on platforms such as the Meta Quest[1] and SteamVR[2]. These explorations further enhanced her understanding of the privacy risks associated with immersive technologies and the presence of deceptive design, and the limited awareness many users have of such threats. Since then, H. Hadan has led multiple studies examining deceptive design and privacy concerns in both traditional and VR gaming environments, and has gained valuable insights into user experiences and design challenges across these mediums.

Our research team, including collaborating researchers and supervisors, brings together diverse expertise in interaction design, user experience, English literature, privacy and cybersecurity, and games user research. This collective expertise enabled more nuanced interpretation of qualitative data and enhanced the overall validity and depth of our research outcomes.

In summary, H. Hadan's background presents a valuable resource to our research, as

[1]Meta Quest VR Store. https://www.meta.com/experiences/
[2]Steam VR. https://store.steampowered.com/app/250820/SteamVR/

it allows us to have a nuanced documentation and analysis of potential deceptive design elements. While we acknowledge that H. Hadan's personality and personal experience with OW2 and VR games and applications may influence our research findings, we see this as a strength. This deep familiarity equips H. Hadan with a nuanced understanding of its strengths and weaknesses, which enabled a more comprehensive analysis.

Appendix B

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

In accordance with ACM Publications Policy[1] and literature suggestion [104], we acknowledge our use of the ChatGPT (GPT-4o and o3 models) AI writing assistant in the preparation of this thesis. This tool was used to correct grammatical errors and, in a few instances, to improve sentence structure and suggest more suitable word choices using prompts:

- *"fix any grammar errors in the following sentence and ensure a smooth flow [our human-written sentence]."*
- *"give me 10 possible words/phrases that can more concisely and precisely reflect the idea in [our human-written phrase/sentence]."*

[1]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

Our decision to use AI tools was guided by the aim of achieving concise and clear academic writing while preserving the "human-touch" in our expression [104]. We did not use AI for any part of data collection, analysis, or image generation. All analyses were conducted manually by H. Hadan and collaborating researchers using non-AI-supported versions of Covidence[2] and Dovetail[3]. Figures presented in this thesis were created using Microsoft Excel or pre-built templates available on Canva[4]. Screenshots from computer and VR games and applications were captured using the Snipping Tool on a Windows PC and the screenshot function on the Meta Quest 3 headset, then annotated using Miro[5]. All manuscripts included in this thesis were manually reviewed, verified, and copy-edited by the research team to ensure accuracy and clarity.

[2]Covidence - Better systematic review management. https://www.covidence.org/
[3]Dovetail - Thematic analysis software. https://dovetail.com/
[4]Canva: Visual Suite for Everyone. https://www.canva.com/
[5]Miro — The Innovation Workspace. https://miro.com/

Appendix C

Materials from Study "Understanding User Awareness and Concerns..."

C.1 Survey Questions

C.1.1 User Awareness of XR Data Operation

Q1: You mentioned that you have experience using XR devices. What data do you think are being observed by the device?

- Identifying in-app/in-world assets (e.g., personal virtual objects, personal avatars)
- Physical appearance (e.g., body dimensions)
- Environment information and dimensions (e.g., users' surroundings, room layout, device/user position in relation to environment, user position in relation to device)
- Physical movements and characteristics (e.g., head/hand/body/eye motion, orientation, position, gestures, posture, fitness information)
- Physiological data (e.g., pupil and cornea reflections, brainwaves, skin signals)

- Visual attention (e.g., eye gaze, area of interest, fixation, heatmaps, time to first fixation, time spent on a certain point, fixation sequences)
- Mannerisms (e.g., gait, habitual movements)
- Cognitive, emotional, personality estimates (e.g., cognitive load, stress, depression, excitement, identity traits, etc.)
- Non-identifying virtual assets (e.g., in-app achievements)

C.1.2 Scenarios and Questions

Sample Scenario:

> *You are at home / personal room, and your XR device (e.g., smart headset, touch controller, 3D projects) is keeping track of your* ***Physical appearance (e.g., body dimensions)*** *when* ***you use the device****.*

Questions below are repeated with each Scenario.

Q2: "I think the Scenario like this (will) happen..." (each answered on 5-point Likert scales from "1-extremely unlikely" to "5-extremely likely")

- Today
- Within 2 years
- Within 10 years

Q3: How comfortable are you about the data collection described in the Scenario? (answered on a 5-point Likert scale from "1-very uncomfortable" to "5-very comfortable")

Q4: Please indicate how sensitive you consider the data being collected in the Scenario. **Sensitive Information** is any information which could cause serious mental, physical, or financial harm if it's lost, misused, or shared without permission. (answered on a 5-point Likert scale from "1-not sensitive" to "5-very sensitive")

Q5: (if "1-very uncomfortable" or "2-uncomfortable" in Q3) If you had no choice on data collection, what would you do (if any) to mitigate the discomfort raised? [open-ended question]

C.2 Codebook

Table C.1: This codebook presents the themes and codes we developed from participants' mitigation strategies responded to open-ended responses to Q5.

Theme	**Frequent codes**	**Example responses**
Away from device	Avoid at all cost	"It can be very dangerous. Avoid at all cost."
	Cease using equipment	"Most likely the only way to reduce data collection would be to not use the device."
	Get rid of device	"I would get rid of device." "I'd sell the VR headset."
	Wouldn't buy the device	"I'd not purchase device which is capable of this kind of data collection."
Benefit vs. Privacy	Accept the data collection if its beneficial to me	"If them obtaining that data benefited me in some way, improved my health for example."
	Evaluate if the device worth the value	"ask myself is it worth it.If the reasons are strong enough I [will] convince myself to only focus on the price."
	I should be paid if they use my data	"at least reward people for their own data." "[I should] getting paid for the collection and use of my data."
Company and System Trust	Bring concern to the company	"I'd try to raise concerns to such companies."
	Choose the device/brands I trust	"choose the devices/brands I feel most comfortable sharing my data with."
	Must comply with user privacy settings	"allow users to set privacy settings and actually comply with them."
	Trust the system	"I'd trust a good system, so in the end I'd be comfortable sharing my data."
Consent and Permission	Be able to opt out	"I'd like to be able to opt out."
	Data collection should with my permission	"Informing that it is doing this and when it is collecting data, how it is being used, and viewing it if necessary." "I'd not partake at all if sensitive data was collected from me without my explicit permission."
	Access and control data usage post-collection	"Having access on how and from whom my personal data are used for."
Comprehend and control what happen to my data	Ensure data is used only for my interests	"show the users that data is only used for their interests and not with second intentions." "data is not used for malicious actions."
	Search option from the Internet	"search for third-party ways to cheat that device so it would process wrong data [not my personal data]."
	Seek privacy protection regulations	"I'd check the data privacy laws surrounding the product." "make sure to have some sort of data collection protection contract."
	Understand data operation	"try research at maximum about the data collection to prevent discomfort."

Table C.1 Continued. This codebook presents the themes and codes we developed from participants' mitigation strategies responded to open-ended responses to Q5.

Theme	**Frequent codes**	**Example responses**
Ignore and Give up	Don't mind data collection but can't be 24/7	"I don't mind the data it collects, but every waking moment in my day would be uncomfortable."
	Everyone's being monitored	"everyone is being monitored anyway. I'm not special." "Technology will overcome us." "We have no privacy."
	I can mitigate the discomfort	"I believe I have the ability to mitigate the discomfort."
	Keep using device and ignore the data collection	"just not think about the data being collected." "ignore the discomfort."
	None	"None." "Nothing can be done."
Limit the collection	Disconnect / turnoff /uninstall when not use	"unplug the device when I'm not using it." "disconnect the device from the Internet."
	Have separate devices for different activities	"having a separate device for activities that wouldn't mix with my main personal computer or devices."
	Limit the device usage only when necessary	"Use the device a lot less." "only use it for certain things and games."
	Not register personal info	"I can lie about my digital self and not have a very personal experience." "Not register the personal avatar on the device."
	Physically block device sensors	"obscure the view of the sensor that the device is using to operate." "cover the device when not in use."
	Physically contain the tracking ability	"find a way to totally block any data that is sent." "put the device in a room that is less personal."
	Seek data protection apps	"I'd download some apps to stop it [data collection]."
	Seek data protection configuration options	"find if there's a setting that disables data collection for commercial purposes." "there should be options to reduce/control the amount and type of data being collected."
	Self-censor privacy disclosure	"avoid my usual mannerism so that the machine can't learn them." "try to not demonstrate my feelings to that device."
Privacy above anything	Be careful and not support it	"have more attention when i use it." "I'd refuse to support it [data collection] in any way." "I'd not agree for this kind of monitoring."
	Concerned about impersonation	"it would be real easy to impersonate someone if those details were to be gathered."
	Personalized advertisements and manipulation	"it will be used to sell me something in the future." "it can be used for manipulate my behavior through the shopping, voting and important life decisions habits."
	Ensure that I can't be identified from my data	"assure me somehow data is anoymized." "something like a VPN would exist for those circumstances in the future, where my data is collected by third parties are unable to connect that data to your identity."
	Switch to alternatives that respect privacy	"I'd try other companies who doing device who respect privacy." "I'd search for alternative headsets without data collection."

C.3 Participant Demographic Information

Table C.2: Overview of Participants' demographics ($N = 464$)

Gender	n (% of total)
Man	230 (50%)
Woman	222 (48%)
Non-binary / third gender	11 (2%)
Prefer not to say	1 (< 1%)
Age	
18-19	12 (3%)
20-29	313 (68%)
30-39	88 (19%)
40-49	39 (8%)
50-56	12 (3%)
Mean (SD)	27.78 (7.95)
Education level	
Less than a high school diploma	4 (< 1%)
High school degree or equivalent	173 (37%)
Associate's degree (e.g., AA, AS)	30 (7%)
Bachelor's degree (e.g., BA, BS)	162 (35%)
Graduate or professional degree (e.g., MA, MD, Ph.D.)	94 (20%)
Prefer not to say	1 (< 1%)
Income	
Less than $25,000	182 (39%)
$25,000-$49,999	151 (33%)
$50,000-$99,999	86 (19%)
$100,000-$199,999	19 (4%)
More than $200,000	5 (1%)
Prefer not to say	21 (5%)

Table B.2 Continued. Overview of Participants' demographics ($N = 464$)

Country of residence	
Belgium	5 (1%)
Canada	5 (1%)
Czech Republic	8 (2%)
Greece	25 (5%)
Hungary	20 (4%)
Italy	43 (9%)
Netherlands	5 (1%)
Poland	66 (14%)
Portugal	123 (27%)
Slovenia	7 (2%)
Spain	28 (6%)
United Kingdom of Great Britain and Northern Ireland	57 (12%)
United States of America	52 (11%)
Other (9 countries)*	20 (4%)
Frequency of use (`EXPERIENCE_FREQUENCY`)	
At least once a day	23 (5%)
At least once a week	117 (25%)
At least once a month	121 (26%)
At least once every three months	69 (15%)
At least once every six months	60 (13%)
Once a year	74 (16%)
Purpose of use (`EXPERIENCE_PURPOSE`)	
Arts (e.g., virtual gallery, design & prototyping, virtual graffiti)	79 (17%)
Education or training (e.g., students, sports, military, medical procedures)	80 (17%)
Entertainment (e.g., gaming, socializing)	437 (94%)
Healthcare (e.g., mental health diagnoses and treatment)	11 (2%)
Workplace requirement (e.g., remote work, staff connection, workplace functionality)	31 (7%)
Other (i.e., research, curiosity, getting directions, fitness)	10 (2%)

*Note. * "Other" includes 9 countries, each containing fewer than 5 participants: Austria, Estonia, Finland, France, Germany, Ireland, Lativa, Norway, Sweden.*

Table B.2 Continued. Overview of Participants' demographics ($N = 464$)

Internet Users' Information Privacy Concerns (IUIPC)	
Control factor (IUIPC_AWARENESS)	
Range (Min - Max)	(3 - 7)
Mean (SD)	5.78 (0.92)
Awareness factor (IUIPC_CONTROL)	
Range (Min - Max)	(3 - 7)
Mean (SD)	6.29 (0.74)
Collection factor (IUIPC_COLLECTION)	
Range (Min - Max)	(1.25 - 7)
Mean (SD)	5.69 (1.14)
Experience with XR devices (EXPERIENCE_YEARS)	
Less than 6 months	185 (40%)
6 months to 1 year	103 (22%)
1 year to 5 years	165 (36%)
5 to 10 years	9 (2%)
More than 10 years	2 (< 1%)
Type of devices used (EXPERIENCE_DEVICE)	
Smart headsets, smart glasses	396 (85%)
Touch controllers, wired gloves, 3D mouse	121 (26%)
Handheld or Mobile devices (e.g., handheld viewers, mobile phone, tablet)	268 (58%)
Projectors and display walls	51 (11%)

C.4 Wilcoxon Signed Rank Test

Table C.3: Wilcoxon Signed-Rank Tests with Bonferroni adjustment [34] on participants' comfort level and perceived data sensitivity across data types. A same pair of scenarios is presented to $n \approx 64$ participants.

	Descriptive Stats		Wilcoxon-signed rank test								
data_type	**Mdn (SD)**	**Min-Max**	Physical appearance	Identifying in-app/in-world assets	Environment information and dimensions	Physical movements and characteristics	Physiological data	Visual attention	Mannerisms	Cognitive, emotional, and personality estimates	
comfort_level											
Physical appearance	3 (1.10)	(1 - 5)									
Identifying in-app/in-world assets	3 (1.10)	(1 - 5)	*W=248.5* *P=.002*** *r=-0.39*								
Environment information and dimensions	3 (1.06)	(1 - 5)	*W=323.5* *P <.15* *r=-0.17*	*W=804.5* *P=.001**** *r=-0.46*							
Physical movements and characteristics	3 (1.14)	(1 - 5)	*W=320.0,* *P=.02** *r=-0.28*	*W=502* *P=.11* *r=-0.20*	*P=.65* *P=.65* *r=-0.06*						
Physiological data	2 (1.03)	(1 - 5)	*W=612.5* *P=.81* *r=-0.03*	*W=1473.5* *P <.001**** *r=-0.48*	*W=738.5* *P=.003*** *r=-0.37*	*W=838.5* *P <.001**** *r=-0.46*					
Visual attention	3 (1.12)	(1 - 5)	*W=395.5* *P=.64* *r=-0.06*	*W=410.5* *P=.048** *r=-0.25*	*W=465* *P=.46* *r=-0.10*	*W=367* *P=.40* *r=-0.10*	*W=181.5* *P=.04** *r=-0.28*				
Mannerisms	3 (1.07)	(1 - 5)	*W=345.0* *P=.62* *r=-0.07*	*W=827* *P <.001**** *r=-0.49*	*W=539.5* *P=.25* *r=-0.14*	*W=574.5* *P=.12* *r=-0.18*	*W=231.5* *P=.06* *r=-0.24*	*W=584.5* *P=.29* *r=-0.13*			
Cognitive, emotional, and personality estimates	2 (1.14)	(1 - 5)	*W=1052.5* *P <.001**** *r=-0.59*	*W=1031.5* *P <.001**** *r=-0.61*	*W=751* *P <.001**** *r=-0.61*	*W=1002* *P <.001**** *r=-0.50*	*W=317* *P=.007*** *r=-0.39*	*W=988* *P=.002*** *r=-0.39*	*W=567.5* *P=.001*** *r=-0.42*		
Non-identifying virtual assets	4 (1.01)	(1 - 5)	*W=143.5* *P <.001**** *r=-0.58*	*W=189* *P=.001*** *r=-0.40*	*W=285* *P <.001**** *r=-0.53*	*W=252* *P=.005*** *r=-0.35*	*W=0* *P <.001**** *r=-0.80*	*W=181* *P <.001**** *r=-0.57*	*W=146.5* *P <.001**** *r=-0.62*	*W=27.5* *P <.001**** *r=-0.78*	

*Note. Mdn=Median, W=Test Statistic, r=Effect size, Significance are displayed as: *** P < .001, ** P < .01, * P < .05.* *Table continued on next page.*

Table C.3 Continued. Wilcoxon Signed-Rank Tests with Bonferroni adjustment [34] on participants' comfort level and perceived data sensitivity across data types. A same pair of scenarios is presented to $n \approx 64$ participants.

	Descriptive Stats		Wilcoxon-signed rank test								
data_type	**Mdn (SD)**	**Min-Max**	Physical appearance	Identifying in-app/in-world assets	Environment information and dimensions	Physical movements and characteristics	Physiological data	Visual attention	Mannerisms	Cognitive, emotional, and personality estimates	
data_sensitivity											
Physical appearance	4 (1.28)	(1 - 5)									
Identifying in-app/in-world assets	2 (1.24)	(1 - 5)	*W=782.5* *P=.008*** *r=-0.34*								
Environment information and dimensions	3 (1.20)	(1 - 5)	*W=469* *P=.42* *r=-0.10*	*W=164.5* *P <.001**** *r=-0.49*							
Physical movements and characteristics	3 (1.26)	(1 - 5)	*W=594* *P=.23* *r=-0.15*	*W=181* *P <.001**** *r=-0.49*	*W=322* *P=.67* *r=-0.06*						
Physiological data	4 (1.16)	(1 - 5)	*W=503.5* *P=.68* *r=-0.05*	*W=234* *P <.001**** *r=-0.58*	*W=327.5* *P=.006*** *r=-0.34*	*W=151* *P <.001**** *r=-0.46*					
Visual attention	3 (1.22)	(1 - 5)	*W=547.5* *P=.12* *r=-0.20*	*W=276.5* *P=.07* *r=-0.24*	*W=369* *P=.57* *r=-0.07*	*W=526.5* *P=.006*** *r=-0.34*	*W=406* *P=.002*** *r=-0.44*				
Mannerisms	3 (1.20)	(1 - 5)	*W=411* *P=.56* *r=-0.08*	*W=262* *P=.002*** *r=-0.38*	*W=695.5* *P=.40* *r=-0.10*	*W=286* *P=.09* *r=-0.20*	*W=742.5* *P <.001**** *r=-0.48*	*W=290* *P=.16* *r=-0.18*			
Cognitive, emotional, and personality estimates	4 (1.00)	(1 - 5)	*W=17* *P <.001**** *r=-0.73*	*W=113* *P <.001**** *r=-0.67*	*W=88* *P <.001**** *r=-0.61*	*W=75* *P <.001**** *r=-0.71*	*W=53* *P <.001**** *r=-0.61*	*W=74.5* *P <.001**** *r=-0.69*	*W=104* *P <.001**** *r=-0.58*		
Non-identifying virtual assets	2 (1.28)	(1 - 5)	*W=1109* *P <.001**** *r=-0.62*	*W=525.5* *P <.001**** *r=-0.49*	*W=1723.5* *P <.001**** *r=-0.56*	*W=1012.5* *P <.001**** *r=-0.61*	*W=1469.5* *P <.001**** *r=-0.79*	*W=831* *P <.001**** *r=-0.64*	*W=934.5* *P <.001**** *r=-0.52*	*W=1263* *P <.001**** *r=-0.81*	

*Note. Mdn=Median, W=Test Statistic, r=Effect size, Significance are displayed as: *** P < .001, ** P < .01, * P < .05. Table continued on next page.*

Table C.3 Continued. Wilcoxon Signed-Rank Tests with Bonferroni adjustment [34] on participants' comfort level and perceived data sensitivity across data types. A same pair of scenarios is presented to $n \approx 64$ participants.

	Descriptive Stats		Wilcoxon-signed rank test							
data_type	**Mdn (SD)**	**Min-Max**	Physical appearance	Identifying in-app/in-world assets	Environment information and dimensions	Physical movements and characteristics	Physiological data	Visual attention	Mannerisms	Cognitive, emotional, and personality estimates
likely_today										
Physical appearance	3 (1.27)	(1 - 5)								
Identifying in-app/in-world assets	4 (1.28)	(1 - 5)	*W=226.5* *P <.001**** *r=-0.46*							
Environment information and dimensions	4 (1.26)	(1 - 5)	*W=217* *P=.009*** *r=-0.31*	*W=598* *P=.06* *r=-0.23*						
Physical movements and characteristics	4 (1.23)	(1 - 5)	*W=339.5* *P=.002*** *r=-0.37*	*W=683* *P=.11* *r=-0.20*	*W=217* *P=.37* *r=-0.12*					
Physiological data	2 (1.17)	(1 - 5)	*W=520.5* *P=.24* *r=-0.14*	*W=1402* *P <.001**** *r=-0.66*	*W=846.5* *P <.001**** *r=-0.57*	*W=797* *P <.001**** *r=-0.54*				
Visual attention	3 (1.25)	(1 - 5)	*W=226* *P=.03** *r=-0.28*	*W=471* *P=.14* *r=-0.19*	*W=690.5* *P=.02** *r=-0.30*	*W=361* *P=.27* *r=-0.14*	*W=62* *P <.001**** *r=-0.51*			
Mannerisms	3 (1.20)	(1 - 5)	*W=372* *P=.35* *r=-0.12*	*W=985.5* *P <.001**** *r=-0.56*	*W=637* *P=.007*** *r=-0.33*	*W=656* *P=.001*** *r=-0.40*	*W=97.5* *P <.001**** *r=-0.54*	*W=487* *P=.46* *r=-0.09*		
Cognitive, emotional, and personality estimates	2 (1.08)	(1 - 5)	*W=1016.5* *P <.001**** *r=-0.59*	*W=1387* *P <.001**** *r=-0.67*	*W=982.5* *P <.001**** *r=-0.70*	*W=968* *P <.001**** *r=-0.70*	*W=259* *P=.09* *r=-0.24*	*W=1006* *P <.001**** *r=-0.54*	*W=811* *P <.001**** *r=-0.53*	
Non-identifying virtual assets	4 (1.30)	(1 - 5)	*W=108* *P <.001**** *r=-0.64*	*W=225* *P=.09* *r=-0.21*	*W=485.5* *P=.03** *r=-0.25*	*W=195.5* *P=.02** *r=-0.30*	*W=10* *P <.001**** *r=-0.77*	*W=212* *P=.001*** *r=-0.42*	*W=111.5* *P <.001**** *r=-0.57*	*W=61* *P <.001**** *r=-0.74*

*Note. Mdn=Median, W=Test Statistic, r=Effect size, Significance are displayed as: *** P < .001, ** P < .01, * P < .05.*

Table C.4: Wilcoxon Signed-Rank Tests on participants' comfort level across device statues ($N = 464$).

device_status	**Descriptive Stats**		
	Mdn (SD)	**Min-Max**	**Wilcoxon Signed-Rank Test**
comfort_level			In-use
In-use	3 (1.10)	(1 - 5)	
Running in the background	3 (1.20)	(1 - 5)	*W=38588, P < .001***, r=-0.23*
data_sensitivity			In-use
In-use	3 (1.12)	(1 - 5)	
Running in the background	3 (1.10)	(1 - 5)	*W=24216, P=.005**, r=-0.14*
likely_today			In-use
In-use	3 (1.14)	(1 - 5)	
Running in the background	3 (1.11)	(1 - 5)	*W=38028, P < .001***, r=-0.24*

*Note. Mdn=Median, W=Test Statistic, r=Effect size, Significance are displayed as:*** $P < .001$, ** $P < .01$, * $P < .05$.*

Appendix D

Materials from Study "A Preliminary Exploration on..."

D.1 Example of Our Game Mechanics Analysis Process

Here, we present an example of our game mechanics analysis on OW2 Battle Pass in Figure D.1 and Figure D.2. In this process, we started with the core Battle Pass interface (top screenshot) and expanded on our discussion to other related interfaces that players could encounter during their interaction.

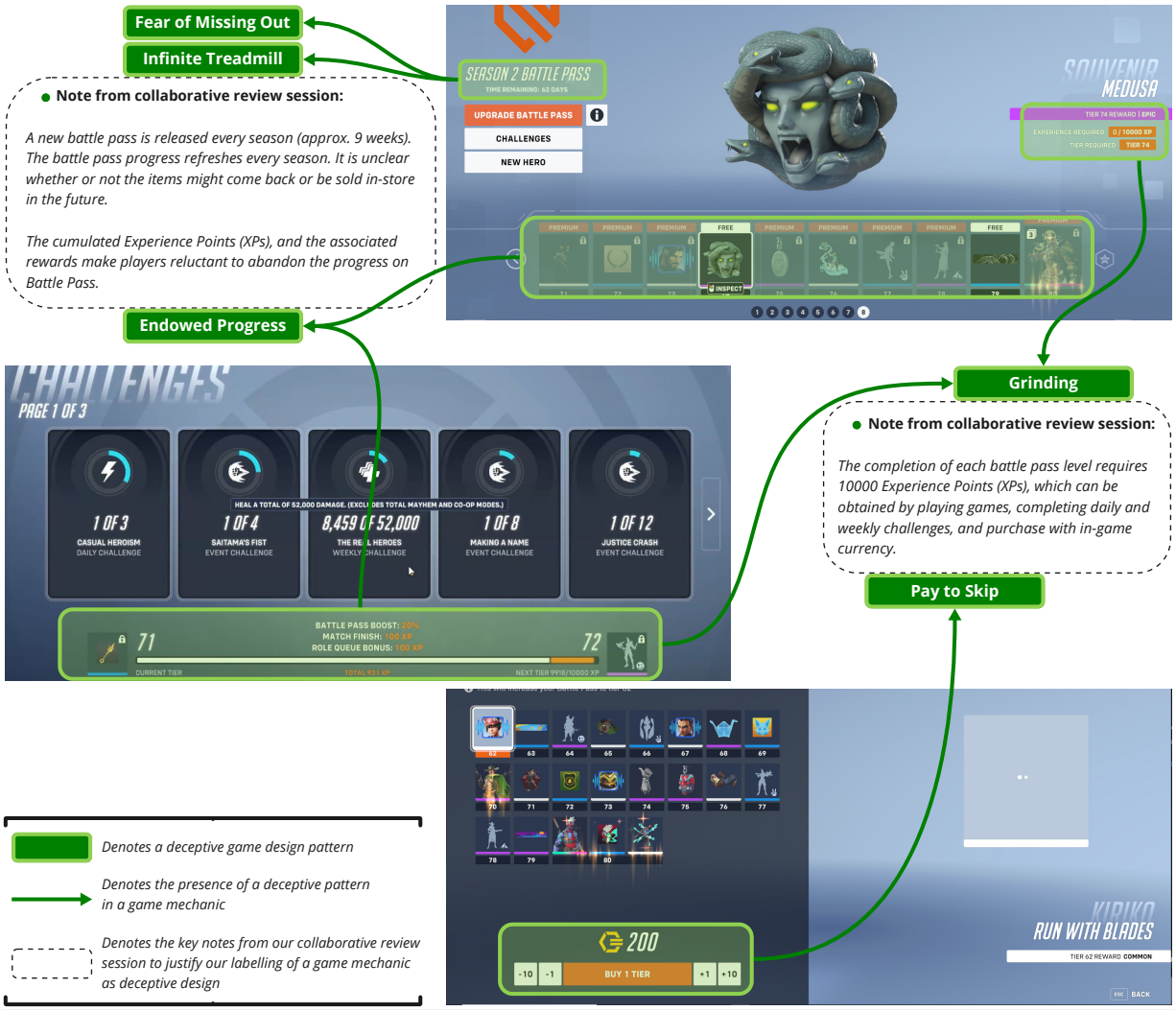


Figure D.1: Example of our game mechanics labeling process on screenshots of OW2 Battle Pass. Only key screenshots are included in this example. From top to bottom: (1) core Battle Pass interface demonstrating rewards, XP requirements, and duration; (2) XP earning breakdown illustrating XP earning sources; (3) Battle Pass level purchase interface with prices in OW coins that are purchasable with real money. Green labels denotes specific deceptive game design patterns from our *Assessment Guide*. Green arrows and highlighted areas denote the presence of these deceptive game design in the game mechanics. In the deductive labeling process, we wrote down the "Notes" from our researchers during the collaborative review session to support labeling decisions.

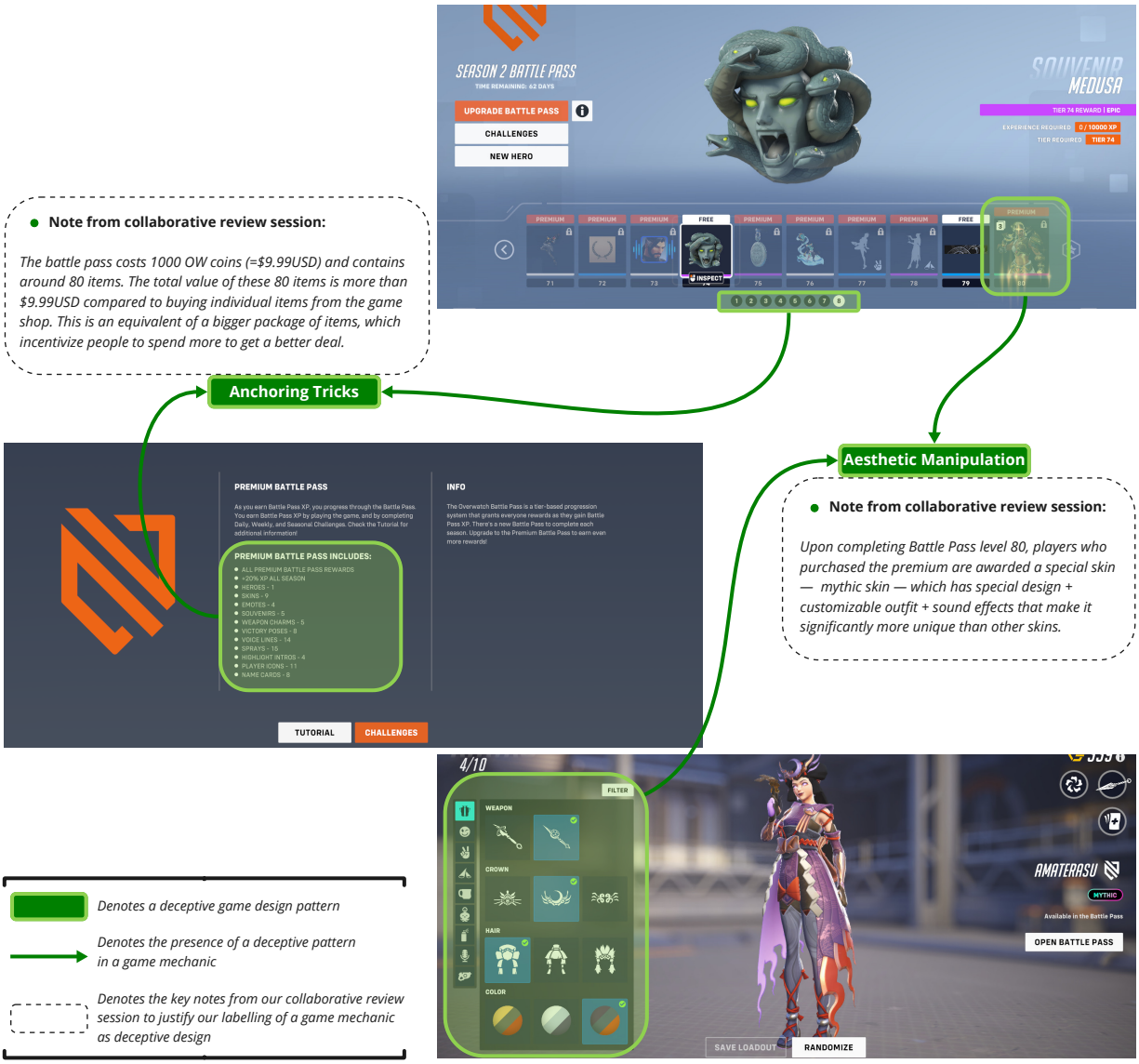


Figure D.2: Example of our game mechanics labeling process on screenshots of OW2 Battle Pass. Only key screenshots are included in this example. From top to bottom: (1) core Battle Pass interface demonstrating rewards, XP requirements, and duration; (2) Battle Pass information page detailing rewards and premium benefits; (3) mythic skin interface highlighting it's unique and customizable design. Green labels denotes specific deceptive game design patterns from our *Assessment Guide*. Green arrows and highlighted areas denote the presence of these deceptive game design in the game mechanics. In the deductive labelling process, we wrote down the "Notes" from our researchers during the collaborative review session to support labeling decisions.

D.2 Reddit Search Keywords

- 42 deceptive design keywords: [‘deceptive’, ‘deceive’, ‘manipulative’, ‘coercive’, ‘malicious’, ‘misleading’, ‘obnoxious’, ‘seductive’, ‘steering’, ‘trickery’, ‘attack’, ‘monetization’, ‘money’, ‘monetizing’, ‘confuse’, ‘exploit’, ‘manipulate’, ‘mislead’, ‘subvert’, ‘intent’, ‘preference’, ‘trick’, ‘autonomy’, ‘undermine’, ‘consent’, ‘abuse’, ‘harm’,’deceiving’, ‘manipulating’, ‘subverting’, ‘tricking’, ‘abusing’, ‘harming’, ‘undermining’, ‘attacking’, ‘confusing’, ‘scummy’, ‘scam’, ‘scammy’, ‘respect’, ‘respectful’, ‘respective’];
- 21 game mechanics keywords: [‘battle’, ‘battlepass’, ‘pass’, ‘daily’, ‘dailies’, ‘challenge’, ‘challenges’, ‘weekly’, ‘weeklies’, ‘double’, ‘event’, ‘seasonal’, ‘season’, ‘coins’, ‘cosmetics’, ‘skin’, ‘hero’, ‘kiriko’, ‘lifeweaver’, ‘flowerman’, ‘ramattra’].

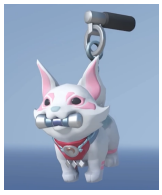
D.3 OW2 In-Game Items Glossary

Table D.1: Overwatch 2 In-Game Obtainable Items Glossary

Item*	Example	Description
Player Icons		Player icons are avatars which are displayed to a player's friends and group.
Name Cards		Name cards are on the background of a player's profile.
Skins		Skins modify the appearance and voice clips of heroes.
Emotes		Emotes make the hero strike a pose or perform an action while in-game.

Note. Items such as *player title* and *golden weapon* that cannot be obtained from the Battle Pass and the Game Shop are omitted. *Item information is based on Overwatch Wiki. https://overwatch.fandom.com/wiki/Cosmetics

Table D.1 Continued. Overwatch 2 In-Game Obtainable Items Glossary

Item*	Example	Description
Souvenirs		Souvenirs are objects displayed with emotes.
Weapon Charms		Weapon charms can be hung on a hero's weapon.
Victory Poses		Victory poses modify how a hero stands on the victory screen.
Voice Lines		Voice lines make other players around the hero hear them say a phrase.
Sprays		Sprays can be put on surfaces in game by pressing the bound key or button.
Highlight Intros		Highlight intros customize the animation that is shown when the game ends.

Note. Items such as *player title* and *golden weapon* that cannot be obtained from the Battle Pass and the Game Shop are omitted. *Item information is based on Overwatch Wiki. https://overwatch.fandom.com/wiki/Cosmetics

D.4 Sample Diary Entry Structure

Table D.2: Structural outline of a sample diary entry from a *Moss2* gameplay session on February 1, 2024. The diary was documented in Miro given its feasibility in linking videos, screenshots, and diary texts. From left to right: (1) description of the lead researcher's experience, reactions, thoughts, and feelings complemented by corresponding screenshots of game design elements, and (2) post-gameplay reflection on possible presence of deceptive game design and its context.

Date: February 1, 2024	
Estimated Time: ∼3.5 hours including diary writing	
[Imported Video Recording]	
[*Diary*]	**[Reflection Note:]**
Today's session with Moss Book II produced a strong emotional moment that further made me more emotionally invested in Quill, the brave mouse protagonist. She had to fight a scary owl (a winged tyrant) that threw her and her uncle off a cliff. I was on the edge of my seat as Quill went after her uncle. The game then showed a really touching scene where Quill found her uncle Argus died. The moment that she holds Argus' body and looks at my direction for help made me feel like I was right there with Quill on her suffering.	I really love how Quill interacts with me directly - it makes the game so much more engaging. Her reactions to my moves are spot on and she reacts to my every move and gives me a high-five when I do something right. Even when I mess up, she's still there showing she cares about me and bears with me while I try to solve the puzzles. It's like she's a real character to me, not just some avatar. This feeling motivates me to keep going and solve all the puzzles and guide her through the story.
[Screenshots]	
As I and Sahima found Quill under the cliff, she surprised me with a hug. While the limitations of VR technology prevented a fully tactile experience, the animation of "hugging" my controller pointers with her whole body effectively conveyed the warmth and gratitude in her embrace. This simple gesture touched deeply and reminded me of the bond we had built throughout our shared adventure. It was no longer just about guiding Quill through puzzles anymore; it was about protecting a close friend.	The emotional weight of the hug was further amplified when we found what happened to Quill's uncle. His death made the story of Moss even more meaningful and gave me a stronger sense of purpose. I became even more determined to keep Quill safe and avenge her uncle's loss because I knew she was counting only on me now.
[Screenshots]	**[Next Session:]**
The way the game implemented it for Quill's hug was cool, but imagine if we could feel every detail – like the warmth of her fur or the gentle squeeze of her tiny paws. That would be so immersive and emotional. I bet it would change the way we feel about the characters we're playing with.	In my next session, I'll be looking for other methods that the game uses to enhance player immersion and emotional connection. It will be interesting to see how Moss Book II continues to use storytelling and VR technology to create a truly impactful experience.

D.5 Deceptive Game Design Patterns Identified from Overwatch2 and VR Applications

Table D.3: Deceptive designs identified in OW2 using our *Assessment Guide* (see Chapter 5), which formed the foundation for our qualitative analysis of user perceptions on Reddit.

***Theme*/Subtheme**	**Code**	**OW2 Game Mechanics**	**Expert Discussion Notes**[a]
Theme 1: Sneaking			
Hiding Information	Reference Pricing	In-Game Shop	Discounted/cheaper items appeared to be better deals, comparing to full-priced/expensive ones displayed alongside.
Theme 2: Obstruction			
Creating Barriers	Intermediate Currencies	OW Coins	The use of five distinct in-game currencies, each with different exchange rates and purchase restrictions, creates confusion and makes it difficult for users to assess the true cost of items.
Theme 3: Social Engineering			
Urgency	Countdown Timers	Battle Pass	The countdown timers pressured users into completing the Battle Pass before time runs out.
		Daily/Weekly/Seasonal Challenges	Time-limited challenges refresh daily, weekly, and seasonally pressured users into completing them.
		In-Game Shop	I feel pressured to buy bundles and discounted items as they refresh weekly, indicated by a countdown timer.
	Fear of Missing Out (FOMO)	Battle Pass	The time-limited rewards create a strong loss aversion effect, where users may feel compelled to complete the Battle Pass to avoid losing premium content they have already invested in.
		Daily/Weekly/Seasonal Challenges	The time-sensitive nature of challenge rewards may foster a sense of urgency and make users feel they must engage regularly to maximize their earnings.
		New Character	Restricting new characters to a limited-time Battle Pass tier may create a fear of missing out, as it means missing the easiest path and quick access.
Personalization	Social Obligation	New Character	The team-based gameplay dynamics create implicit pressure to unlock the new characters quickly, as users may feel responsible for contributing effectively to their team.

Note. a. Contents in quotes are descriptions directly from OW2 design mechanisms.

Patterns not obvious in design mechanisms analysis but were brought up by users in Reddit analysis.

denotes deceptive designs mentioned in the game-related literature [287, 129].

denotes deceptive designs mentioned in VR-related literature [100].

Table D.3 Continued. Deceptive designs identified in OW2 using our *Assessment Guide* (see Chapter 5), which formed the foundation for our qualitative analysis of user perceptions on Reddit.

***Theme*/Subtheme**	**Code**	**OW2 Game Mechanics**	**Expert Discussion Notes**[a]
Theme 4: Interface Interference			
Manipulating Choice Architecture	Visual Prominence	Battle Pass	Nearly all desirable content locked (grayed out) behind the premium tier, which may make users feel purchasing the premium Battle Pass essential.
	Bundling	Battle Pass	Packaging over 80 rewards into a single purchase creates a perception of greater value compared to individual purchases, even when users may not want all included items.
		In-Game Shop	Discounted bundles reinforce the idea of a better deal, and encourage purchases even when users may not have originally intended to buy all included items.
Emotional or Sensory Manipulation	Adorable design	Battle Pass	Unique mythic skins with custom sound and visual effects are positioned at the final level, which uses aesthetic appeal to drive purchases.
		In-Game Shop	Cute or visually appealing items may increases the temptation to make users purchase and use them in gameplay.
Theme 6: Forced Action			
Gamification	Pay-to-Play	Battle Pass	The recurring premium fee each season creates an ongoing financial commitment for users who want access to rewards.
			The option to buy XP levels instead of grinding introduces pressure to spend money when users have limited playtime.
		New character	Gating new characters behind the premium Battle Pass drives user purchases for immediate access rather than delayed unlocks.
	Grinding	Daily/Weekly/Seasonal Challenges	The requirement to complete repetitive tasks pressure users to play daily.
		Battle Pass	High XP requirements per level push users to continually engage in gameplay and complete challenges to progress.
		New Character	Unlocking new characters through extensive grinding incentivizes immediate purchase to avoid prolonged future challenges.
	Playing by Appointment	Double XP Weekend	Time-limited XP boost events create urgency, and compel users to participate during specific windows to maximize progression.

Note. a. Contents in quotes are descriptions directly from OW2 design mechanisms.

Patterns not obvious in design mechanisms analysis but were brought up by users in Reddit analysis.

denotes deceptive designs mentioned in the game-related literature [287, 129].

denotes deceptive designs mentioned in VR-related literature [100].

Table D.3 Continued. Deceptive designs identified in OW2 using our *Assessment Guide* (see Chapter 5), which formed the foundation for our qualitative analysis of user perceptions on Reddit.

***Theme*/Subtheme**	**Code**	**OW2 Game Mechanics**	**Expert Discussion Notes**[a]
Theme 6: Forced Action			
Sunk Cost Fallacy	Endowed Progress	Battle Pass	Users who have already progressed in the Battle Pass may find it difficult to abandon incomplete levels.
		Daily/Weekly/Seasonal Challenges	Once users have partially completed challenges, they may feel compelled to finish them to avoid wasted effort.
	Waste Aversion	In-Game Shop	Remaining in-game currency from past purchases may incentivize users to buy additional currency packs to avoid "wasting" unused coins.
Theme 7: Facilitation			
Infinite Treadmill	-	Battle Pass	The recurring nature of seasonal Battle Passes creates an ongoing cycle where users may feel pressured to complete each new pass.
		Daily/Weekly/Seasonal Challenges	Constantly refreshing challenge cycles may encourage users' continuous participation and reinforce their habitual gameplay.

Note. a. Contents in quotes are descriptions directly from OW2 design mechanisms.

Patterns not obvious in design mechanisms analysis but were brought up by users in Reddit analysis.

denotes deceptive designs mentioned in the game-related literature [287, 129].

denotes deceptive designs mentioned in VR-related literature [100].

Table D.4: Based on our *VR Deceptive Game Design Assessment Guide* in Table 5.1, this table presents deceptive design patterns we identified within *Moss2* and *Beat Saber*.

***Theme*/Subtheme**	**Code**	**VR Game Mechanics**[a]	**Synthesized Diary Entries**[b]
Theme 1: Sneaking			
	-	-	-
Theme 2: Obstruction			
Creating Barriers	Price Comparison Prevention	Beat Saber: Song Purchase System	I feel frustrated because comparing individual song and song pack prices in-game is impossible, as no clear prices provided in game.
Theme 3: Social Engineering			
Social Proof	Parasocial Pressure	Beat Saber: Song Gallery	I feel attracted to songs and music packs from my favorite singers, games, or anime.
Urgency	Limited Time Messages	Beat Saber: Song Purchase System	I feel tempted to buy songs and music packs during the time-limited sale.
Personalization	Competition	Beat Saber: Leaderboard	While my skills may not compete with global or local players and my friends, I feel pressured to perform better to beat my old scores to avoid losing gained skills.
Theme 4: Interface Interference			
Manipulating Choice Architecture	False Hierarchy	Beat Saber: Main Menu	I feel tempted to tap on the music pack beside game mode options on the main menu because it seems special compared to those within each game mode.
	Visual Prominence	Beat Saber: Song Purchase System	I feel distracted by the notification that purchasing the entire music pack is cheaper, and the visually prominent "buy music pack" option on top of the "buy level (song)" option that I intend to select.
	Bundling	Beat Saber: Song Purchase System	I feel buying whole music packs because an in-game notification claims they are cheaper, despite no clear prices listed for individual songs or packs.
Theme 4: Interface Interference			
Emotional/Sensory Manipulation	Adorable design	Beat Saber: Song Gallery	I feel attracted to play the game repeatedly because of its beautiful and visually striking block and lightsaber designs. I feel attracted to the BTS music pack[c] because each song has the singers' avatars dancing with me in the game. I feel attracted to songs and music packs with cute covers. I feel attracted to songs with strong beats as they help me catch the rhythm and perform better in the game.
		Moss: Book II: Character Design	I feel attracted to play the game by the cute character designs, and colorful and vibrant map environments. I feel attracted to interact with the characters because she actively "talk" to me using sign language.

Note. a. Mechanics from a same game are grouped by color. We used pink for game mechanics from *Moss2* and blue for those from *Beat Saber*.

b. Contents in quotes are descriptions directly from the game.

c. BTS Music Pack. Beat Saber Wiki. https://beatsaber.fandom.com/wiki/BTS_Music_Pack. Last accessed on May 4, 2024.

denotes deceptive designs mentioned in the game-related literature [287, 129].

denotes deceptive designs mentioned in VR-related literature [100].

Table D.4 Continued. Based on our *VR Deceptive Game Design Assessment Guide* in Table 5.1, this table presents deceptive design patterns we identified within *Moss2* and *Beat Saber*.

***Theme*/Subtheme**	**Code**	**VR Game Mechanics**[a]	**Synthesized Diary Entries**[b]
Theme 4: Interface Interference			
Emotional/Sensory Manipulation	NPC/Narrative Manipulation	Moss: Book II: Game Narrative	I lose track of time spent in game due to deep connection to the story and characters from the unexpected twists in the storyline.
		Moss: Book II: 3D Interaction and Immersion	I lose track of time spent in game as I feel being part of the story because of the interactive 3D feedback that allow me to flip pages of the story book, move objects in the environment, and "pet," "hug," and "high-five" with the characters.
Trick Questions	-	Beat Saber: Song Purchase System	I feel confused by the option for purchasing individual songs (" buy level") as it might refer to purchasing a difficulty level rather than a song. Whereas the "buy music pack" option is more straightforward.
Theme 4: Interface Interference			
Hidden Information	-	Beat Saber: 3D Interaction and Immersion	I lose track of time due to deep engagement of gameplay and the absence of an in-game clock.
		Moss: Book II: 3D Interaction and Immersion	I lose track of time due to deep engagement of gameplay and the absence of an in-game clock.
		Beat Saber: Gameplay	I feel frustrated by the lack of an option or progress bar to mark specific parts of a song where I struggle. As a result, when I fail a game, I must repeatedly practice the entire song.
		Moss: Book II: Progress Indicator	I feel confused about my storyline progress because the progress indicator is too subtle and blends into the library environment seamlessly.
Theme 6: Forced Action			
Forced Communication/Disclosure	Privacy Zuckering	Beat Saber: Song Purchase System	I feel vulnerable because purchasing songs or music packs requires entering payment information before seeing clear prices.
Gamification	Pay-to-Play	Beat Saber: Song Purchase System	I feel annoyed by the fact that even though I bought the game I have to consistently buy new songs and music packs.
			I lose track of money spent on songs and music packs since each costs only around $2 to $4 USD.
	Power Creep	Beat Saber: Gameplay	Over time, I feel bored by playing the same songs repeatedly, which drives me to buy new ones.
	Can't Pause or Save	Moss: Book II: Saving Options	I feel pressured to play continuously and stop less, as the game solely on automatic saves. I cannot save my progress manually even when my battery is dying.

Note. a. Mechanics from a same game are grouped by color. We used pink for game mechanics from *Moss2* and blue for those from *Beat Saber*.

b. Contents in quotes are descriptions directly from the game.

c. BTS Music Pack. Beat Saber Wiki. https://beatsaber.fandom.com/wiki/BTS_Music_Pack. Last accessed on May 4, 2024.

denotes deceptive designs mentioned in the game-related literature [287, 129].

denotes deceptive designs mentioned in VR-related literature [100].

Table D.4 Continued. Based on our *VR Deceptive Game Design Assessment Guide* in Table 5.1, this table presents deceptive design patterns we identified within *Moss2* and *Beat Saber*.

***Theme*/Subtheme**	**Code**	**VR Game Mechanics**[a]	**Synthesized Diary Entries**[b]
Theme 6: Forced Action			
Sunk Cost Fallacy	Endowed Value	Beat Saber: Gameplay	I feel pressured to play daily to maintain my gained skills and song mastery.
Theme 8: Other			
Complete the Collection	-	Beat Saber: Song Gallery	I feel the urge to own all songs in a music pack due to my positive experiences with some songs.
		Moss: Book II: Scrolls and Armors	I feel the urge to collect all scrolls and armors, even revisiting maps, though they don't affect the storyline.

Note. a. Mechanics from a same game are grouped by color. We used pink for game mechanics from *Moss2* and blue for those from *Beat Saber*.

b. Contents in quotes are descriptions directly from the game.

c. BTS Music Pack. Beat Saber Wiki. https://beatsaber.fandom.com/wiki/BTS_Music_Pack. Last accessed on May 4, 2024.

denotes deceptive designs mentioned in the game-related literature [287, 129].

denotes deceptive designs mentioned in VR-related literature [100].

D.6 Thematic Analysis Codebook of Reddit Posts

Table D.5: Codebook of players experiences and perceptions toward the candidate deceptive design and OW's business model transition, found in the Overwatch community discussions.

Theme	Code	Player Statement (paraphrased*)
Time Sinking Experiences	Insane amount of grind	Years of grind for a single skin seem insurmountable for casual players like me.
	New character locked behind grind	Locking the new character in the battle pass assists grinds, nobody knows if they would be able to unlock her in the future
	Forced to play	I feel being forced to play instead of enjoying a quality game. I have purchased content but still have to grind to receive rewards slowly.
	Huge gap between earnings and costs	Earning 60 coins per week seems pathetic considering a legendary skin costs 1900 coins.
	No attainable OW coins	I cannot earn enough coins for the next battle pass like in most games.
	Hard to complete	Challenges force you to play in 4 different game modes is annoying, un-fun, and difficult.
Money Sinking Experiences	No progression outside of premium	I cannot get progression, good rewards, accomplishments, recognition without premium.
	Removed excitement towards events	I'm no longer excited for yearly event or holiday skins as nothing is earnable for playing.
	Unfair Item Pricing	Cosmetics are overpriced.
	Disrespectful to my effort	Charging or making players grind for old unlockable items is ridiculous, while giving away a shop bundle for free through Twitch drops is disrespectful.
	FOMO sales	I'm pressured to buy now or lose only lifetime chance for preferred skin that may never. appear in shop again
	Accidental purchase	The swapped placement of Ok and Cancel led to my accidental purchase of a $20 USD skin.
Social Consequences	social obligation	My team needs me to unlock a character to combat the enemy team.
	Players are underappreciated	The minimal rewards from the battle pass and challenges create an unrewarding and disrespectful gaming experience.
Psychological Impacts	Lackluster Items	The rewards are lackluster, skin designs are underwhelming, and there is nothing worth grinding for.
	Item-value limited by the game genre	Grinding the battle pass for the mythic skin for a character I don't play is useless.
	No realistic way to complete collection	The game expects me to grind 17,000 weeks or spend $10,226 USD to get all OW2 items.
Predatory Marketing Strategies	Price skimming	Intentionally overpriced contents create a false sense of value for players. A cheaper system will be introduced to feign concern for and acknowledge community feedback.
	Fake bundles & discounts	Items put on sale without being sold at full price to begin with.
	Being vague about OW1 coins	Intentionally vague about OW1 currency to encourage spending before OW2, incentivizing real-money purchases on OW2 contents.
	Limited utility of OW1 coins	OW1 coins are now useless, limited to default legendary skins only, and can't be used to purchase older skins that were available for years.

Note. *For ethical considerations, we paraphrased all direct quotes in such a way that the original post and the creator are not easily traceable. See Section 6.2.4.

Table D.5 Continued. Codebook of players experiences and perceptions toward the candidate deceptive design and OW's business model transition, found in the Overwatch community discussions.

Theme	**Code**	**Player Statement (paraphrased*)**
Disappointment Surpassed	Better gameplay in OW2	I was really impressed with the core gameplay of OW2 and I enjoyed new graphics and game modes.
Enjoyment	Lost the sense of rewarding	Everything in the game feels empty and pointless without spending money.
	Lost interest in items	I can feel myself just completely disconnecting with caring about cosmetics.
	Free players have no incentives to play	I don't want to burst the free-to-play bubble, but don't expect to get cool items without spending some cash
	Unsustainable in the long-term	The current system seriously injures the game's growth and lifespan. It only caters to whales who spend big but will quickly move on to the next trendy game.
Detrimental Business Practices	Evasive response to player feedback	The game publisher acts like they listen to their players but don't actually care.
	Value profit more than gameplay	Giving out (old) skins in Twitch drops instead of in gameplay says a lot about their values and focus.

Note. *For ethical considerations, we paraphrased all direct quotes in such a way that the original post and the creator are not easily traceable.

See Section 6.2.4.

Appendix E

Materials from "A Structured Investigation of..."

E.1 Example Diary Entry

Table E.1: 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.

E.2 Example Screenshots Deceptive Design Patterns from VR Games and Playful Applications



Figure E.1: 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.*

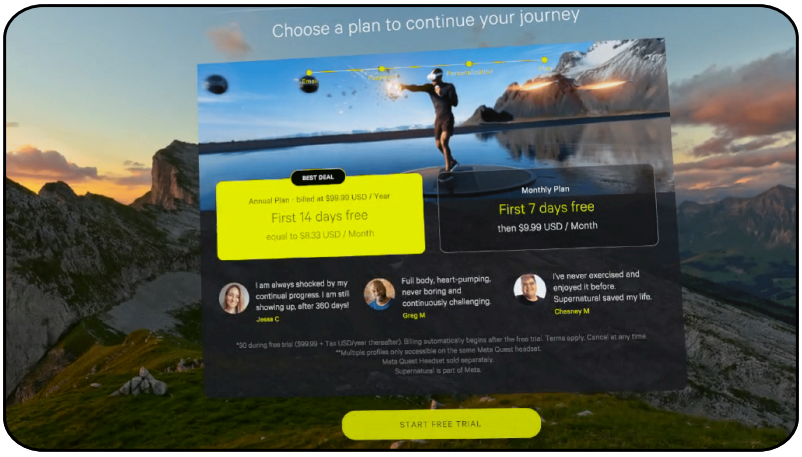


Figure E.2: The subscription mechanism in *Supernatural* exemplifies the `Endorsements and Testimonials` deceptive design pattern. The mechanism includes two different subscription plans alongside three testimonials that aim to persuade users to subscribe, which involves providing payment information, 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 photorealistic 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.

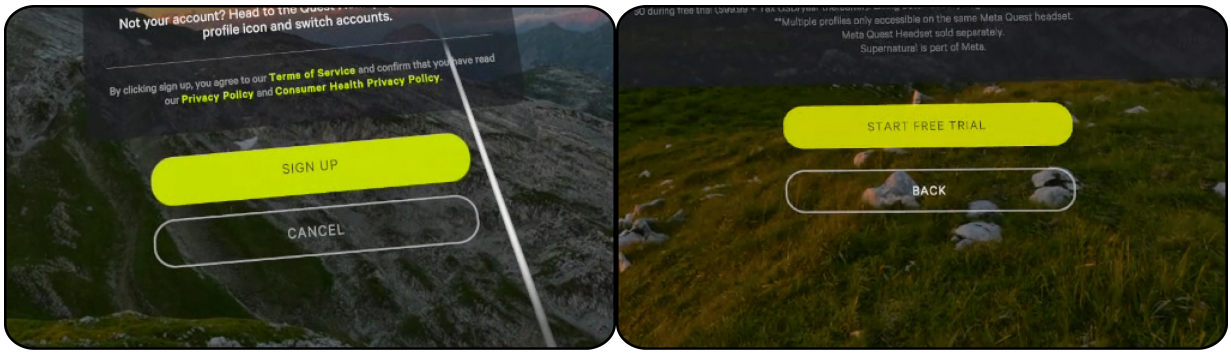


Figure E.3: The registration and subscription mechanisms in *Supernatural* (see left and right screenshots, respectively) exemplify the `False Hierarchy`, `Visual Prominence`, and `Positive or Negative Framing` deceptive design patterns. Options that involve acceptance are brightly colored, visually 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.

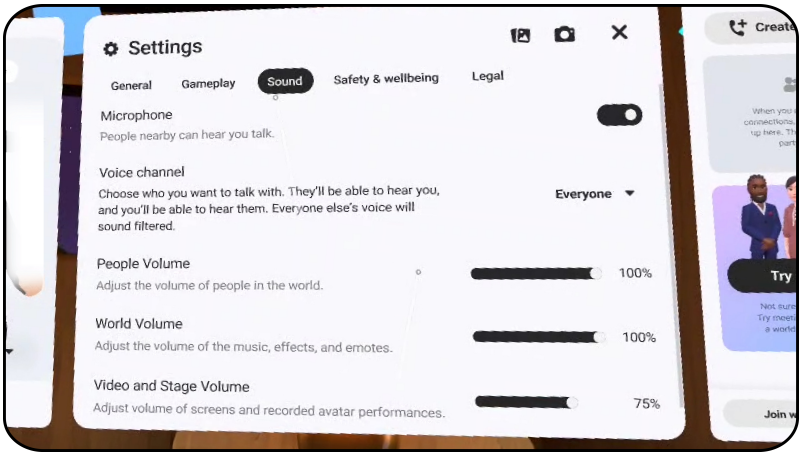


Figure E.4: The consent interaction mechanism in *Meta Horizon Worlds* exemplifies the `Bad Defaults` deceptive design pattern. Within the settings menu, several privacy-invasive options are pre-enabled by default. These include automatically activating the microphone ("people nearby can hear you talk"), 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.*

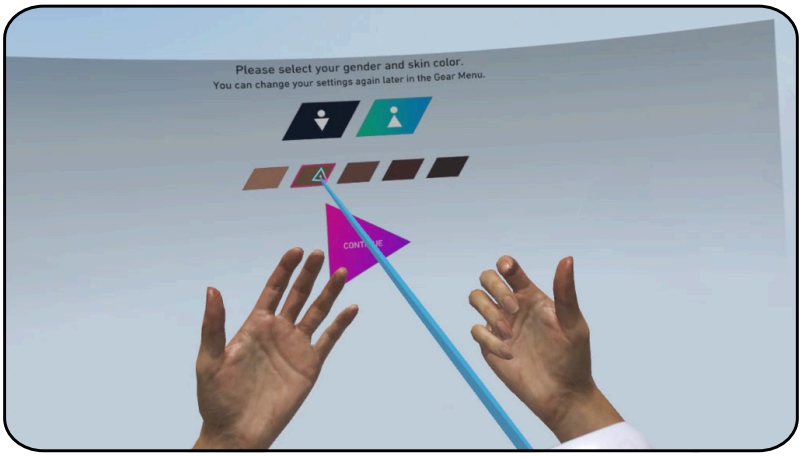


Figure E.5: The quality-of-life (QoL) feature that facilitates avatar customization in *The Climb 2* exemplifies the `Trick Questions` deceptive design pattern. In this interface, users are asked to choose their gender and skin color, phrased as "select your race and gender". Although this question was intended for avatar customization, the wording exemplifies the misleading nature of Trick Questions. As users see the photorealistic 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.

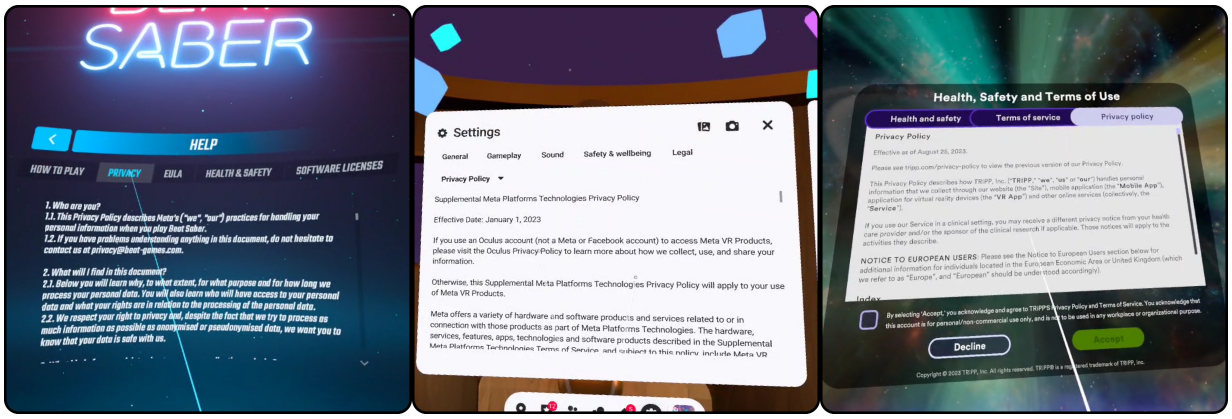


Figure E.6: The in-game and in-app privacy policies in *Beat Saber* (see left screenshot), *Meta Horizon Worlds* (see center screenshot), and *TRIPP* (see right screenshot) exemplify `Complex & Lengthy Language` deceptive design pattern. Although they are aimed to inform users about data practices upon 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 Chapter 7 and Section E.3).



Figure E.7: 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.

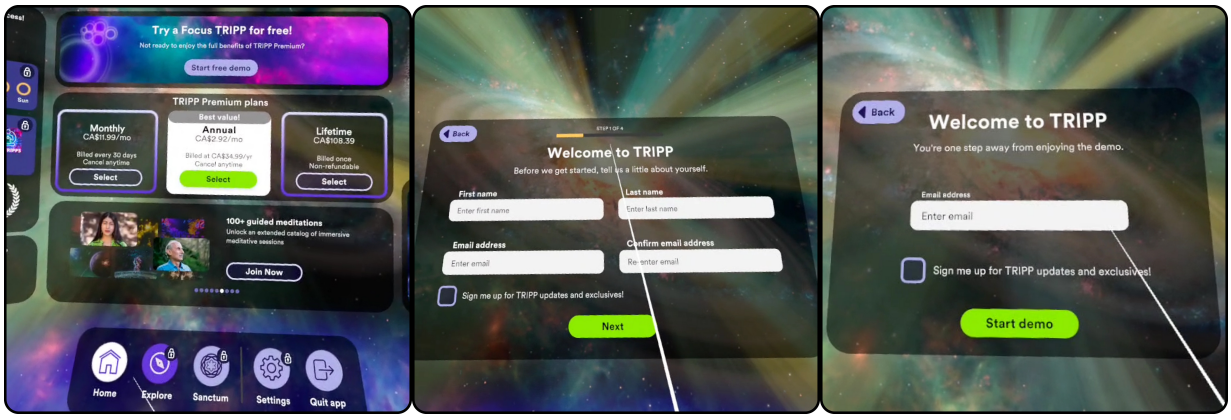


Figure E.8: The registration and subscription mechanism in *TRIPP* exemplifies the `Forced Registration` deceptive design pattern. No functions are usable or accessible without registration (see left screenshot). Users are required to provide their email address to even start a demo session (see center 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.



Figure E.9: 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.



Figure E.10: 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 [177], as users' focus is naturally drawn to the visually striking VR game and application previews, and leave critical privacy information overlooked.

E.3 Privacy Policy Readability Assessment

Following GPEN's approach [82], we assessed the readability of the 13 selected privacy policies using the Flesch Reading Ease Score in Microsoft 365.[1] 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 E.2 presents the results, where lower scores indicate more difficult contents requiring a higher education level to understand.

Table E.2: 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

[1] 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

E.4 Detailed Demographics

Table E.3: Overview of Participants' demographics (n=182)

Scenario(S)	**S1 (n=62)**	**S2 (n=59)**	**S3 (n=61)**
Gender			
Female	27 (43.5%)	26 (44.1%)	33 (54.1%)
Male	34 (54.8%)	32 (54.2%)	28 (45.9%)
Non-binary / third gender	1 (1.6%)	1 (1.7%)	0 (0%)
Prefer not to say	0 (0%)	0 (0%)	0 (0%)
Age			
Range (Min-Max)	18-64	19-59	18-64
Mean (SD)	34.27 (11.15)	34.61 (10.9)	36.34 (11.02)
Education Level			
High school diploma, GED, or less	13 (21.0%)	10 (16.9%)	8 (13.1%)
Associates or technical degree	6 (9.7%)	3 (5.1%)	11 (18.0%)
Bachelor's degree or equivalent	35 (56.5%)	34 (57.6%)	33 (54.1%)
Graduate or professional degree (MA, MS, MBA, PhD, JD, MD, DDS etc.)	8 (12.9%)	12 (20.3%)	9 (14.8%)
Country of Origin			
Canada	5 (8.1%)	29 (49.2%)	8 (13.1%)
United States of America	57 (91.9%)	30 (50.8%)	53 (86.9%)
Experience in Professional VR Roles			
VR Developer/Engineer	1 (1.6%)	1 (1.7%)	5 (8.2%)
VR Researcher	3 (4.8%)	1 (1.7%)	8 (13.1%)
VR Designer (e.g., UI, UX)	2 (3.2%)	3 (5.1%)	4 (6.6%)
VR Product Manager	4 (6.5%)	3 (5.1%)	8 (13.1%)
VR Data Analyst	3 (4.8%)	2 (3.4%)	6 (9.8%)
Never	53 (85.5%)	50 (84.7%)	47 (77.0%)
Other	-	1 (1.7%)	1 (1.6%)

Table E.3 Continued. Overview of Participants' demographics (n=182)

Scenario(S)	**S1 (n=62)**	**S2 (n=59)**	**S3 (n=61)**
IUIPC			
Control			
Range (Min-Max)	2-7	2-7	1-7
Mean (SD)	5.76 (0.96)	5.53 (1.01)	5.52 (1.09)
Awareness			
Range (Min-Max)	1-7	1-7	1-7
Mean (SD)	6.12 (1.02)	6.2 (0.85)	6.01 (1.06)
Collection			
Range (Min-Max)	1-7	1-7	1-7
Mean (SD)	5.38 (1.43)	5.22 (1.61)	5.26 (1.35)
Awareness and Concern about Deceptive Design [19]			
Others			
Mean (SD)	3.25 (0.98)	2.78 (0.91)	2.89 (0.96)
Median	4	3	3
Mode	4	2	4
Personal			
Mean (SD)	2.97 (0.95)	2.79 (0.99)	2.88 (0.87)
Median	3	3	3
Mode	4	2	3
General Experience with VR Devices			
Less than 6 months	7 (11.3%)	4 (6.8%)	5 (8.2%)
6 months to 1 year	8 (12.9%)	8 (13.6%)	11 (18.0%)
1 to 2 years	17 (27.4%)	18 (30.5%)	20 (32.8%)
2 to 5 years	22 (35.5%)	24 (40.7%)	22 (36.1%)
More than 5 years	8 (12.9%)	5 (8.5%)	3 (4.9%)

Table E.3 Continued. Overview of Participants' demographics (n=182)

Scenario(S)	**S1 (n=62)**	**S2 (n=59)**	**S3 (n=61)**
Reason of VR Device Use			
Entertainments (e.g., gaming, socializing)	60 (96.8%)	56 (94.9%)	55 (90.2%)
Healthcare (e.g., mental health diagnoses and treatment)	7 (11.3%)	10 (16.9%)	18 (29.5%)
Education or training (e.g., students, sports, military, medical procedures)	16 (25.8%)	13 (22.0%)	18 (29.5%)
Workplace requirement (e.g., remote work, staff connection, workplace functionality)	9 (14.5%)	4 (6.8%)	11 (18.0%)
Arts (e.g., virtual gallery, design & prototyping, virtual graffiti)	21 (33.9%)	20 (33.9%)	13 (21.3%)
Other	2 (3.2%)	4 (6.8%)	6 (9.8%)
Experience with the VR App			
Less than 1 month	3 (4.8%)	9 (15.3%)	8 (13.1%)
1 to 6 months	12 (19.4%)	27 (45.8%)	19 (31.1%)
6 months to 1 year	12 (19.4%)	11 (18.6%)	15 (24.6%)
1 to 2 years	21 (33.9%)	9 (15.3%)	16 (26.2%)
More than 2 years	14 (22.6%)	3 (5.1%)	3 (4.9%)
Frequency of VR App Use			
Everyday	5 (8.1%)	4 (6.8%)	5 (8.2%)
A few times a week	23 (37.1%)	30 (50.8%)	35 (57.4%)
Once a week	10 (16.1%)	6 (10.2%)	5 (8.2%)
A few times a month	19 (30.6%)	14 (23.7%)	15 (24.6%)
Once a month or less	5 (8.1%)	5 (8.5%)	1 (1.6%)
Personal Rating of VR App Experience			
1 Star	-	1 (1.7%)	1 (1.6%)
2 Star	3 (4.8%)	4 (6.8%)	2 (3.3%)
3 Star	11 (17.7%)	10 (16.9%)	11 (18.0%)
4 Star	31 (50.0%)	30 (50.8%)	27 (44.3%)
5 Star	16 (25.8%)	14 (23.7%)	20 (32.8%)
no response	1 (1.6%)	-	-

E.5 Kendall correlation matrix of participants' awareness and concerns about VR deceptive design and privacy, and demographics

Table E.4: Kendall's τ correlation matrix [68] of participants' awareness and concerns about VR deceptive design, online privacy, and demographics ($N = 182$). Only significant correlations ($P < .05$) are displayed. Low correlations ($\tau < 0.3$) have a white background; moderate correlations ($0.3 \leq \tau < 0.7$) have a light pink background.

	Age	Education Level	Professional VR job	VR experience	Influence awareness	Harm awareness	Manipulation concern	IUIPC_Control	IUIPC_Awareness
Education Level	τ=0.132								
Professional Job		τ=0.305							
VR experience	τ=0.08								
Influence awareness									
Harm awareness					τ=0.357				
Manipulation concern			τ=0.107	τ=-0.081	τ=0.365	τ=0.476			
IUIPC_Control					τ=0.13	τ=0.111	τ=0.084		
IUIPC_Awarnees			τ=-0.131		τ=0.117	τ=0.092		τ=0.480	
IUIPC_Collection					τ=0.09	τ=0.158	τ=0.178	τ=0.336	τ=0.361

E.6 Scenarios

Table E.5: Scenario description, corresponding VR application, design mechanism, and incorporated privacy deceptive design patterns.

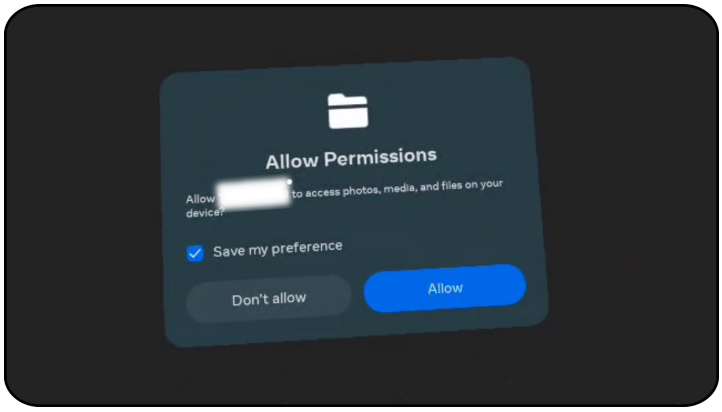
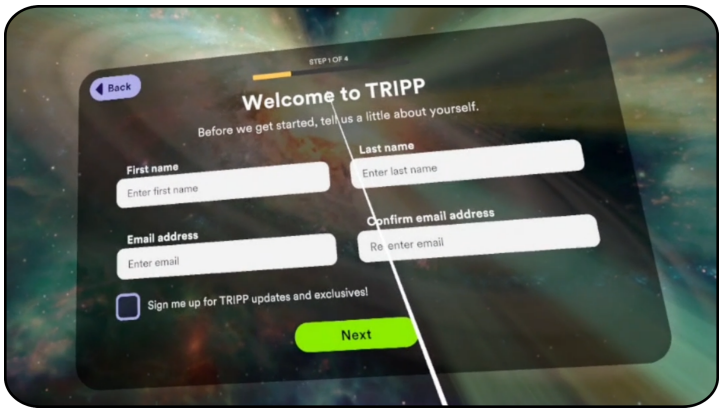
ID	Scenarios
S1	 *Description:* Imagine you are about to use **VRChat**, a social VR application. Upon entering the application, you are immediately presented with a **Permission Request** asking whether to grant permissions for accessing your photos, media, and files. You must decide whether to approve or deny these permissions before proceeding further into the application. • False Hierarchy/Visual Prominence: Highlight the "Allow" option that is invasive to user privacy. • Bad Default: Set default options that benefit the company but risky for users' privacy. • Privacy Zuckering: Trick users into thinking this permission is essential for the service. • Hidden Information: Obscure crucial details of the purpose of data collection.

Table E.5 Continued. Scenario description, corresponding VR application, design mechanism, and incorporated privacy deceptive design patterns.

ID	Scenarios
S2	

Description: Imagine you are about to use **TRIPP**, a VR wellness application. As you begin, you are presented with a **Registration Form**. Before accessing any functions, you are required to either enter your email address or register an account by providing your firstname and lastname to unlock all features.

- Forced Registration: Require account creation for tasks that should not need it, potentially extracting unnecessary personal data
- Privacy Zuckering: Trick users into thinking this permission is essential for the service.

Table E.5 Continued. Scenario description, corresponding VR application, design mechanism, and incorporated privacy deceptive design patterns.

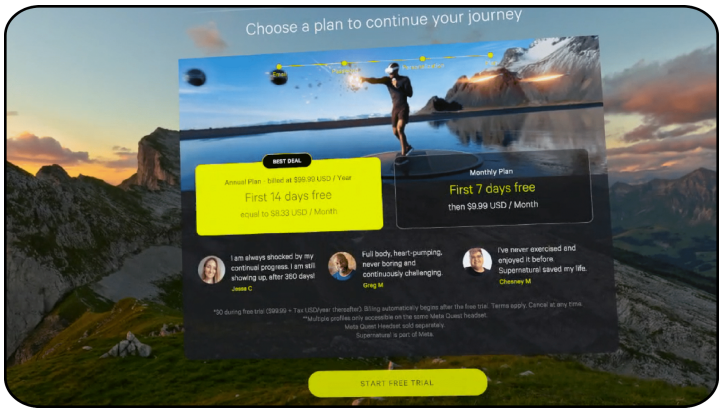
ID	Scenarios
S3	 *Description:* Imagine you are about to use **Supernatural**, a VR fitness application that offers a subscription-based experience set in a photorealistic, immersive virtual landscape. As you start, you are presented with **Subscription Form** with two subscription plans and showcasing three testimonials. Before accessing any features, you are required to select and pay for a subscription. • Endorsements and Testimonials: Use fabricated testimonials to influence users' purchase decisions. • False Hierarchy/Visual Prominence: Highlight the acceptance option that transmits user data. • Positive or Negative Framing: Use vibrant green to communicate emotional safety on options that transmit user data.

Table E.5 Continued. Scenario description, corresponding VR application, design mechanism, and incorporated privacy deceptive design patterns.

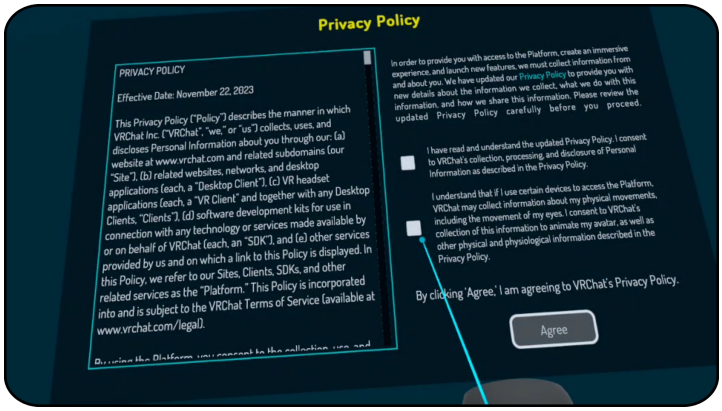
ID	Scenarios
S4	 *Description:* Imagine you are using **The Climb 2**, a single-player VR game, and you are seeking to read its privacy policy. The main **Settings Menu** offers six distinct buttons, each leading to a different sub-menu. To look for the privacy policy, you must navigate to the "options" sub-menu, where you will see two buttons on the right and various application settings in the center. To access the privacy policy, you will need to select the "privacy" option on the right side. • Privacy Maze: Bury privacy controls under layers of confusing menus.
S5	 *Description:* Imagine you are about to use **VRChat**, a social VR application. This application requires you to review and consent to its privacy policy upon first entry. As you begin, you are presented with a **Consent Form** with a detailed privacy policy document that explains the application's data practices. You can scroll through the document to view the full content before checking the required boxes and clicking "Agree." Consent must be given before you can access the main application. • Complex & Lengthy Language: Use hard-to-understand words and sentence structures to hinder users' understanding of privacy information.

Table E.5 Continued. Scenario description, corresponding VR application, design mechanism, and incorporated privacy deceptive design patterns.

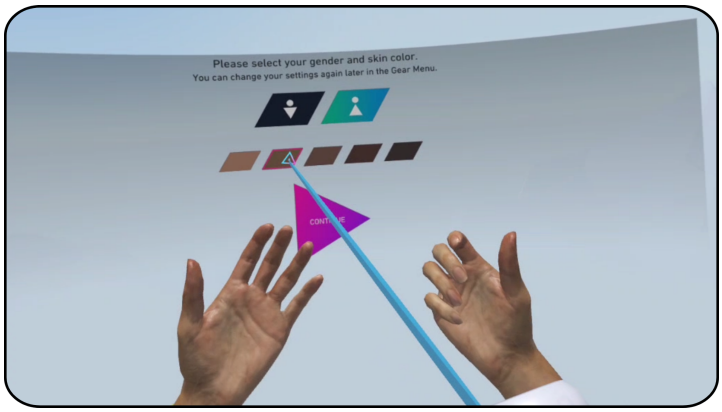
ID	Scenarios
S6	 *Description:* Imagine you are about to use **The Climb 2**, a single-player VR game. As you start, you are prompted to customize your avatar. The **Avatar Creation Interface** asks you to select your gender and skin color, and you can see a photorealistic rendering of your avatar's hands from a first-person perspective. These choices will define how your avatar appears in the game world. • Trick Questions: Use confusing wording to manipulate users' choices and lead them to provide real gender and skin color.

Table E.5 Continued. Scenario description, corresponding VR application, design mechanism, and incorporated privacy deceptive design patterns.

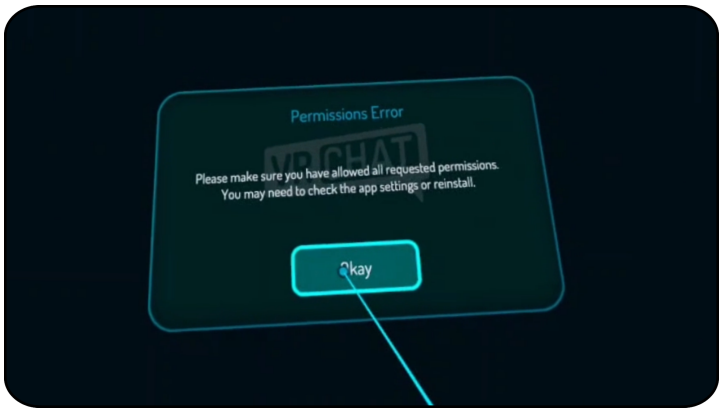
ID	Scenarios
S7	 *Description:* Imagine you are about to use **VRChat**, a social VR application. Upon entry, you deny the application's request for access to your photos, media, and files. However, as you continue interacting with the application—completing the privacy policy consent, logging into your account, or trying to transfer to different virtual worlds—you are repeatedly interrupted by a "permissions error" **Notification** message. Each time, you must press "okay" to proceed. This Notification persists throughout your experience with VRChat. • Nagging: Disrupt user workflow with repeatedly unwanted interruptions to push actions they would rather avoid.

Table E.6: This table presents the two screenshots used in each scenario, with 1 clean screenshot and 1 screenshot with all VR design elements labeled to facilitate participants' selection.

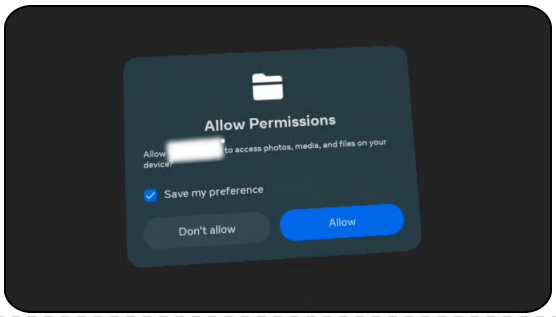
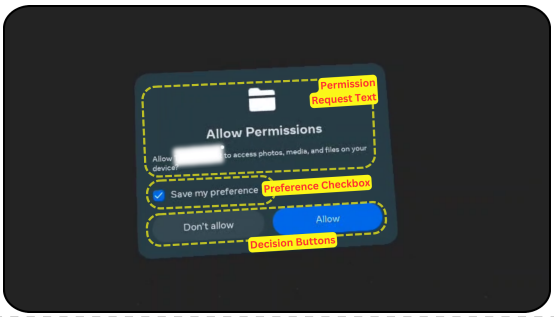
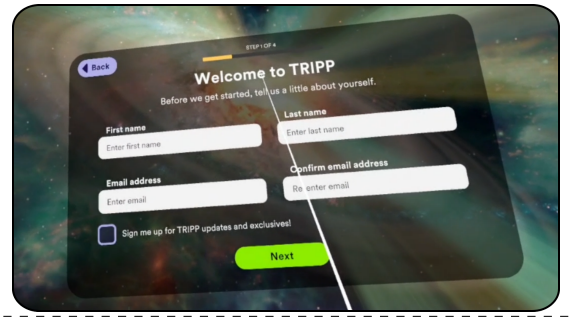
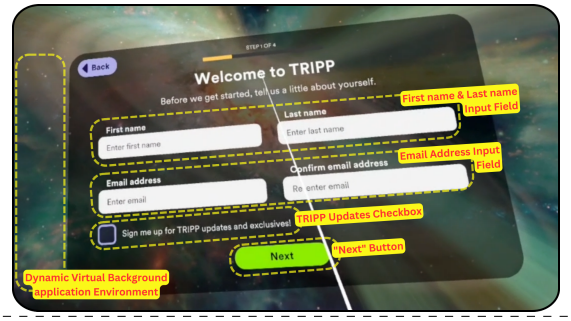
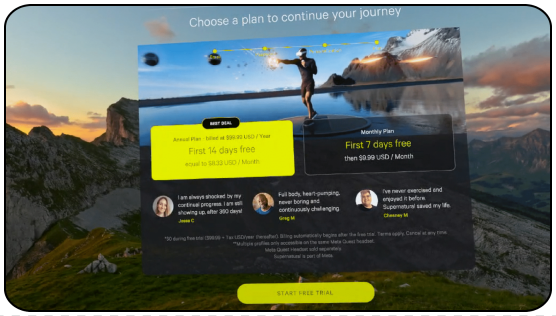
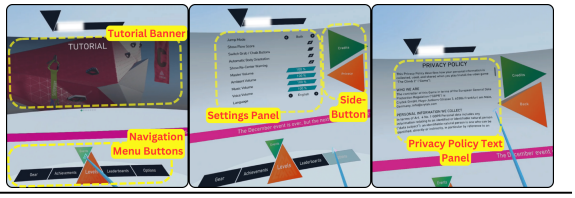
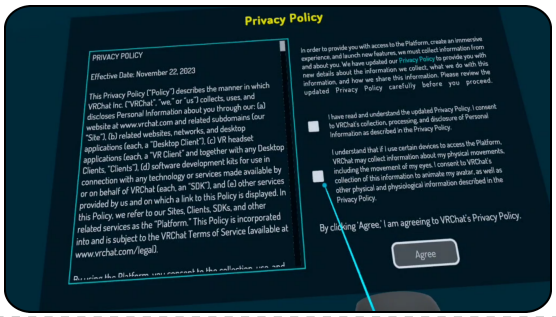
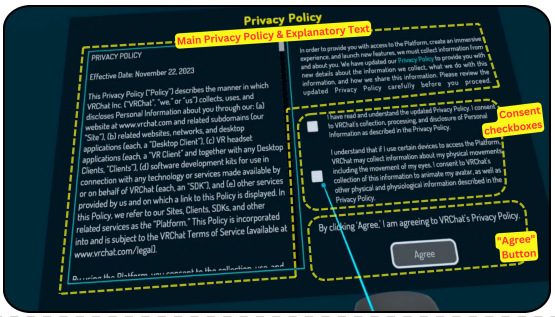
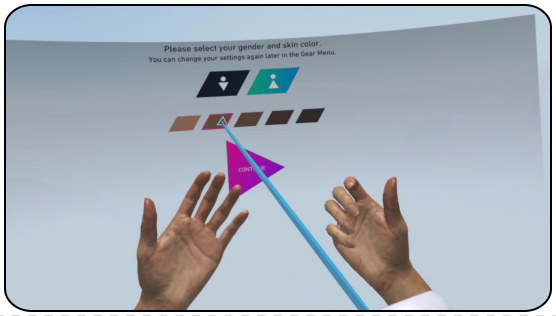
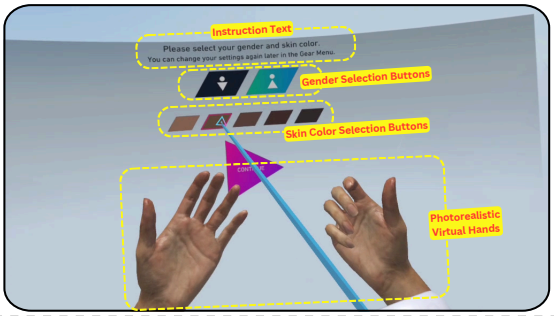
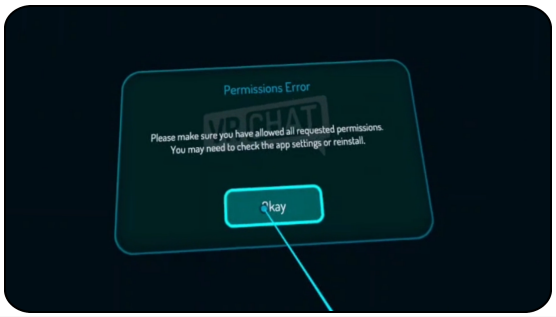
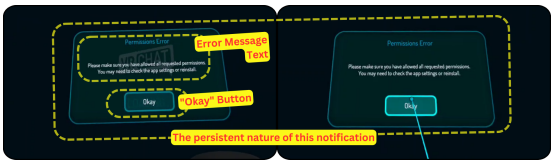
ID	Screenshot (clean)	Screenshot (labeled)
S1		
S2		
S3		
S4		

Table E.6 Continued. This table presents the two screenshots used in each scenario, with 1 clean screenshot and 1 screenshot with all VR design elements labeled to facilitate participants' selection.

ID	Screenshot (clean)	Screenshot (labeled)
S5		
S6		
S7		

E.7 Survey Questionnaire

E.7.1 General Experience with VR Technology and Selected Applications

Q1: How long have you been using the VR equipment or applications?

- Less than 1 month
- 1 month to 6 months
- 6 months to 1 year
- 1 to 2 years
- More than 2 years

Q2: What is the main reason that encouraged you to use VR devices and applications? *(select all that apply)*

- Entertainments (e.g., gaming, socializing)
- Healthcare (e.g., mental health diagnoses and treatment)
- Education or training (e.g., students, sports, military, medical procedures)
- Workplace requirement (e.g., remote work, staff connection, workplace functionality)
- Arts (e.g., virtual gallery, design & prototyping, virtual graffiti)
- Other, please specify:

Q3: Have you ever worked in a professional role related to VR design, research, or development? *(select all that apply)*

- VR Developer/Engineer
- VR Researcher

- VR User Experience (UX) or User Interface (UI) Designer
- VR Game Designer
- VR Product Manager
- VR Data Analyst
- Other, please specify:
- I have never worked in VR-related professional role.

Q4: You indicated in the screening questionnaire that you have experience using [the VR application]. How long did/have you been using this VR application?

- Less than 1 month
- 1 month to 6 months
- 6 months to 1 year
- 1 to 2 years
- More than 2 years

Q5: In general, how often do/did you use this VR application?

- Everyday
- More than once a week
- Once a week
- More than once a month
- Once a month
- More than once a year
- Once a year

Q6: Overall, how would you rate your experience with this application? (5 stars = excellent experience)

Q7: Please elaborate on specific aspects or features of this VR application that contribute to your star rating. (open-ended response)

Q8: Please list the brand and model of the VR device you used to play this VR application. (open-ended response)

E.7.2 Perception and Experience with Privacy Deceptive Design Patterns

Instruction: *Next, we will show you a short video clip that demonstrates a VR design feature you may have encountered in The Climb 2.*

An Example Scenario: *Imagine you are about to use **The Climb 2**, a single-player VR game. As you start, you are prompted to customize your avatar. The **Avatar Creation Interface** asks you to select your gender and skin color, and you can see a photorealistic rendering of your avatar's hands from a first-person perspective. These choices will define how your avatar appears in the game world.*

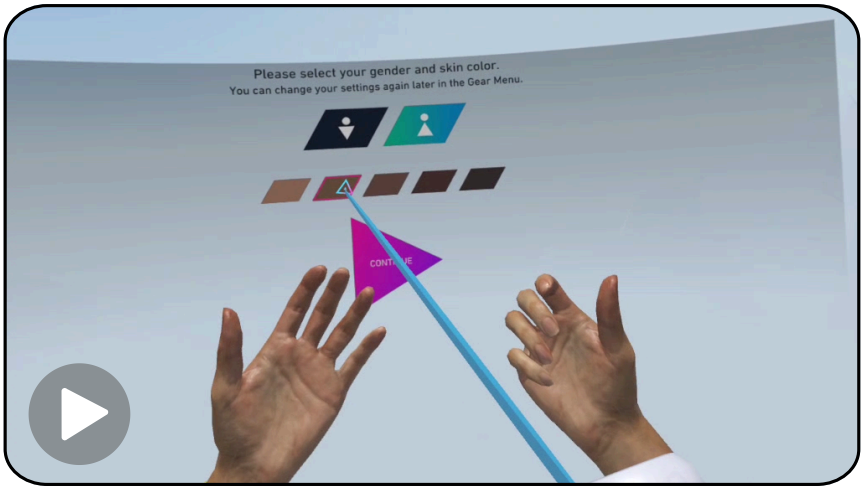


Figure E.11: An example screenshot of the video clip.

Instruction: *Please answer the questions based on your personal experience with this avatar creation interface while using The Climb 2.*

Q9: Drawing from your previous experience using The Climb 2, what would be your thoughts and actions if you encountered this avatar creation interface? (open-ended response)

Q10: Please briefly explain the reasons behind your thoughts and actions to this avatar creation interface. (open-ended response)

Q11: When using this avatar creation interface, do you remember making any of the following decisions? *(select all that apply)*

- I granted the application permission to access content (e.g., photos, media, files) stored on my VR device.
- I opted to remember my settings for future use of the application.
- I entered my personal details (e.g., name, email) into the application.
- I provided my payment information to subscribe to the application.
- I looked for and read through the application's data usage and protection policies.
- I do not remember making any decisions.
- I did not make any decisions.
- Other, please specify: [open space]

Q12: To what extent do you think your decision(s) might have impacted your personal privacy? (answered on 5-point scale(s) from 1-not at all to 5-significantly)

- Display the selected items in Q11.

Q13: In which way do you think this decision might impact your privacy? (open-ended response)

- Display items in Q12 with a score ≥ 3.

Instruction: *The avatar creation interface you viewed includes* ***User Interface (UI) elements*** *that can facilitate your decision-making in your interaction.*

UI elements are the components of an interface that users interact with directly. Examples of UI elements include buttons, drop-down menus, sliders, text fields, checkboxes, toggles, and VR-specific properties like realistic virtual objects or dynamic 3D environments.

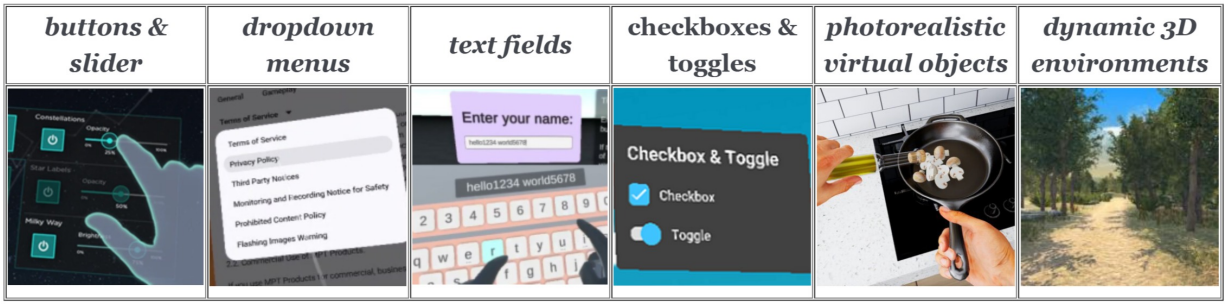


Figure E.12: Example UI elements we used to support participants' understanding.

Q14: Looking at the video again, did any specific design elements influence your decision-making process during your experience with this feature? If yes, please click and highlight the element(s). If design elements from other feature of this VR application influenced your decision-making with this avatar creation interface but are not shown in this screenshot, please select "other" and specify. (present a screenshot with design elements circled and labeled with corresponding names, options are customized for each scenario).

- Instruction Text
- Gender selection buttons
- Skin color selection buttons
- Photorealistic virtual hands
- Other, please specify:

The following questions are repeated with each selected design element in Q14.

Q15: Please explain how this design element affected your decision during your own experience with this avatar creation interface. (open-ended response)

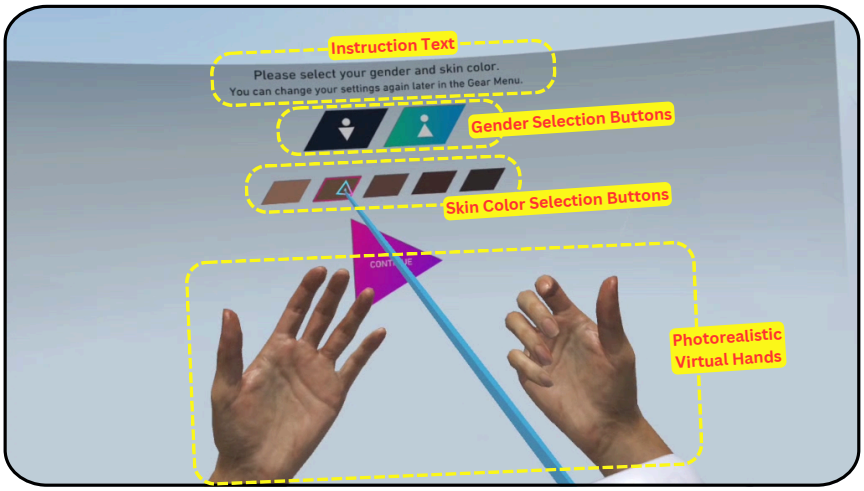


Figure E.13: An example screenshot of the video clip.

Q16: Please indicate your level of agreements with the following statements (answered on 5-point Likert scales, from "1-strongly disagree" to "5-strongly agree"): *The decision or action I made as a result of interacting with this design element is...*

- Beneficial to me.
- Beneficial to the application's developer/publisher.
- Beneficial to the third-party stakeholders (e.g., marketing, legal services, analytical vendors).

After repeating all the design elements, conclude this part of our study with Q17.

Q17: What is the intention of this [VR design feature] and its design elements? And why? (open-ended response)

E.7.3 General Concerns of Influence of Online Design and Privacy

Q18: Please indicate your level of agreements with the following statements (answered on 5-point Likert scales, from 1-strongly disagree to 5-strongly agree) (adapted from [19]):

- The design of VR applications can influence [people's/my] choices and behaviors on managing and sharing their personal information.
- VR applications that are designed to influence users can cause harm to [people's/my] personal information.
- I am worried about the influence of VR applications' design on [people's/my] choices and behaviors when it comes to managing and sharing their personal information.

Q19: Internet Users' Information Privacy Concerns (IUIPC) scale [156].