Mitigating Privacy Harms from Deceptive Design in Virtual Reality

Office of the Privacy Commissioner of Canada (OPC)

2024–25 Contributions Program

RESEARCH REPORT

Submitted by

Principle Investigator/Applicant:

Dr. Leah Zhang-Kennedy
Assistant Professor
University of Waterloo

Research Team:

Hilda Hadan
Ph.D. Candidate
University of Waterloo

Co-Principle Investigator:

Dr. Lennart Nacke
Professor
University of Waterloo

Date: March 15, 2025

UNIVERSITY OF WATERLOO



TABLE OF CONTENTS

ACKNOWLEDGEMENTS 3
SUMMARY 4
CORE FINDINGS AND VR DESIGN GUIDELINES 5
Core Findings: 5
Objective 1 5
Objective 2 6
Implications and Recommendations: 7
For VR Designers and Developers 7
For Policymakers 8
For Users 9
For Researchers 10
VR DECEPTIVE DESIGN SCREENSHOTS WITH DESCRIPTION 11
An overview of the 12 VR applications selected for our analysis 12
A summary of deceptive design patterns observed by our researchers 13
Representative screenshots demonstrating the deceptive patterns in VR contexts 14
VR PRIVACY-ENHANCING DESIGN SCREENSHOTS WITH DESCRIPTION 23
A summary of privacy-enhancing design patterns observed by our researchers 24
Representative screenshots demonstrating these patterns in VR contexts 25

ACKNOWLEDGEMENTS

This project was funded by the Office of the Privacy Commissioner of Canada (OPC) 2024-25 Contributions Program. We are grateful to our funder. Thank you for your support. The views expressed in this work are those of the authors and do not necessarily reflect those of the OPC.

We thank all study participants for their time and valuable insights, which were essential to this research. We also appreciate the contributions of Dr. Reza Hadi Mogavi for his support in improving our manuscripts, Michaela Valiquette for her assistance with qualitative data analysis, and Derrick Wang for resolving technical issues during manuscript formatting.

All screenshots included in this report and our research manuscripts were captured from VR applications during our research sessions and are under the principles of fair use for research study. We have made the research materials and outcomes available at: https://osf.io/axzve/.

Please cite this publication in the following format:

Hadan, H., Nacke, L. E., & Zhang-Kennedy, L. (2025). *Mitigating Privacy Harms from Deceptive Design in Virtual Reality*. (Research Report). University of Waterloo.

This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0), with copyright retained by the author(s). These materials are for non-commercial use only.

SUMMARY

This research investigates deceptive design in Virtual Reality (VR) environments and its impact on user privacy. The research team at the University of Waterloo conducted an autoethnographic evaluation of 12 top-rated VR applications to analyze deceptive design patterns in their privacy communication and interaction mechanisms. The findings reveal **14 distinct deceptive design patterns** and demonstrate how deceptive tactics in traditional web and mobile environments are being adapted to immersive environments. While many of these patterns still heavily rely on 2D interfaces elements, **VR's spatial, immersive, and multi-sensory features amplify their impact** and increased the privacy risks for users. The VR applications' convoluted privacy policies and consent mechanisms further hinder user comprehension on the data practices. Through the evaluation, the team also identified **7 exemplary privacy-enhancing design strategies**, which can serve as a foundation for improved implementation of privacy mechanisms in VR environments.

To assess user perceptions of these deceptive design patterns, the team surveyed 424 users of the selected VR applications. The findings indicate that while **users felt the manipulative influences and expressed discomfort**, they often resign themselves to accepting privacy-invasive options and viewing such design as "typical" or "inevitable" across both VR and non-VR platforms. Their repetitive exposure to such design in mobile and web environments fostered a **false sense of normalcy**, and **eroded user resistance to manipulation**.

This research provides valuable insights for VR developers, designers, policymakers, and researchers on creating privacy-preserving VR experiences and developing clearer, more ethical privacy policies in this rapidly evolving field.

Related Publication:

Hadan, H., Valiquette, M., Nacke, L., & Zhang-Kennedy, L. (2025, October). Immersive Invaders: Privacy Threats from Deceptive Design in Virtual Reality Games and Applications. Paper to be published in the *Companion Publication of the 2025 Conference on Computer-Supported Cooperative Work and Social Computing (CSCW)*, Bergen, Norway. [Accepted paper]

CORE FINDINGS AND VR DESIGN GUIDELINES

This section presents our core research findings and VR design guidelines derived from our findings. Future VR designers, policymakers, and research can use these guidelines to create immersive experiences that not only prioritize user satisfaction and privacy at the same time.

Core Findings:

Objective 1 – Deceptive Design Evaluation on VR Applications

Finding 1: Deceptive design patterns from web and mobile platforms, such as false rights in privacy policies, bundled consent problems, privacy mazes, hidden information, bad defaults, and complex/lengthy policies, have migrated into VR environments. Most currently rely on 2D interface elements, such as checkboxes and scrolling walls of text, rather than fully leveraging VR's 3D capabilities.

Finding 2: VR's immersive features amplify the impact of some deceptive design patterns on user privacy. The occlusion of reality when wearing a headset makes it difficult for users to seek external source for verifying in-app information. The realistic rendering of virtual environments creates compelling and immersive experiences that can make users more likely to trade personal information for accessing the experience. Similarly, accessing external privacy policies requires disruptive application exits.

Finding 3: Some common deceptive patterns from 2D environments are absent in VR due to differences in modalities and interaction mechanisms. For example, problems with settings that cannot be saved are absent because privacy settings are often missing entirely, and cookie banners common on websites are noticeably missing in VR applications.

Finding 4: Some VR applications implement privacy-enhancing "bright patterns" that offer exemplary alternatives to deceptive designs, including privacy-friendly defaults, transparent communication of data practices, private privacy configuration spaces, and balanced privacy and functionality approaches.

Objective 2 – VR User Awareness, Perception, and Decision-Making

Finding 1: Users can recognize when they are being manipulated when deceptive design presents in VR applications, and this perception negatively impacts their overall user experience and reduces willingness to adopt applications, potentially damaging long-term sustainability and brand reputation.

Finding 2: Users' familiarity with similar privacy mechanisms in non-VR environments and trust in brand reputations reduce privacy concerns in VR, making them more vulnerable to manipulation despite being aware of the deceptive patterns.

Finding 3: A concerning "privacy paradox" exists in VR users' decision-making that goes beyond mere privacy resignation. Despite high privacy concerns and developing coping strategies, users often resign themselves to accepting privacy-invasive options because they perceive such mechanisms as "typical," "standard," across various digital platforms and therefore inevitable.

Finding 4: Repetitive exposure to deceptive design patterns across digital platforms creates a false sense of normalcy that erodes users' resistance to manipulation and privacy risks in VR environments. This has led to a troubling state, as being "used to being manipulated" has become an accepted norm.

Implications and Recommendations:

For VR Designers and Developers

Suggestion 1: Implement "bright patterns" as privacy-enhancing alternatives to deceptive design, such as privacy-friendly defaults, just-in-time privacy notifications, transparent data practice communication, private privacy configuration spaces, and develop more balanced approach for usability and privacy.

Suggestion 2: Create VR-specific privacy policies rather than general ones covering multiple platforms, with clear explanations of how biometric data like movement patterns or physiological responses are collected in VR and used for related purposes.

Suggestion 3: Leverage VR technology's features, design accessible privacy policies optimized for VR environments, such as interactive 3D visualizations and sound cues to make privacy information more engaging and intuitive.

Suggestion 4: Provide balanced approaches that maintain functionality while supporting privacy, such as private configuration spaces for avatar customization that give users control over their self-representation.

Suggestion 5: Recognize that users can detect manipulative design patterns, which damages user experience and brand reputation. Implement transparent and ethical design alternatives.

Suggestion 6: Avoid exploiting users' familiarity with non-VR interfaces to implement deceptive patterns, as this erodes trust in the long term.

For Policymakers

Suggestion 1: Beyond existing guidelines for 2D interfaces, current regulatory frameworks need adaptation to address VR-specific privacy design requirements to avoid the VR designs that exploit the immersive 3D features of VR to influence user privacy decisions.

Suggestion 2: Special protections for children in VR environments require clearer guidelines and enforcement mechanisms, as current child-specific privacy instructions are often buried within lengthy policies.

Suggestion 3: Standardized privacy policy design requirements should be established for immersive technologies, and privacy policy information should be made accessible both within and outside the VR environment to effectively communicate with users and support informed decision-making.

Suggestion 4: Update regulatory frameworks to govern how VR applications and companies collect and use VR-specific data to protect users against potential VR privacy challenges and hyper-personalized manipulation.

Suggestion 5: Regulations should be developed to prevent the use of deceptive design practices that span VR, mobile, web, and other digital environments, to combat the normalization of manipulation that leads users to resign themselves to privacy violations (i.e., “being used to being manipulated”).

For Users

Suggestion 1: Question the normalcy of privacy-invasive practices; just because they are common does not mean they are necessary or should be accepted without scrutiny.

Suggestion 2: Be aware that VR environments may use immersive elements to influence your privacy decisions in ways that are more subtle and powerful than in 2D environments.

Suggestion 3: Take advantage of any available private configuration spaces to manage your virtual self-representation according to your privacy concerns.

Suggestion 4: Recognize that the absence of explicit consent mechanisms in VR applications doesn't mean data isn't being collected; be proactive in seeking information about data practices.

Suggestion 5: Actively reporting concerns to developers and regulatory bodies to help challenge the current normalization of manipulative privacy mechanisms, rather than accepting them as inevitable.

For Researchers

Suggestion 1: Further comparative research is needed on how VR's spatial and immersive features specifically influence users' privacy decision-making beyond what occurs in 2D environments.

Suggestion 2: Research should expand on "bright patterns" literature to develop a standardized, accessible toolkit for VR designers to proactively adapt privacy-preserving design practices and prevent deceptive design in the design process before they harm users.

Suggestion 3: Additional investigation is needed to extend existing privacy design principles and non-VR design frameworks to incorporate VR-specific features such as unbounded displays, whole-body interaction, and motion sensing.

Suggestion 4: Future research is also needed on develop VR-specific metrics for detecting, quantifying, and assessing the impact of deceptive design on user experience.

VR DECEPTIVE DESIGN SCREENSHOTS & DESCRIPTION

Our research examined the privacy deceptive design in 12 popular VR applications. Our findings demonstrate 1) how deceptive design patterns from traditional 2D mobile and web interfaces have migrated to VR applications, and 2) how VR's unique spatial, immersive, realistic, and multi-sensory features can amplify their psychological impact and effectiveness on users.

This section includes the resources (e.g., digital photographs, countermeasure lists) that can be used for developing user educational tools to improve user awareness and literacy in managing potential impacts of deceptive designs in VR. Future researchers, educators and VR developers can also leverage these resources to empower users with practical methods to identify and mitigate privacy effects of VR deceptive design.

For a more detailed discussion of our methodology, analysis, and findings, please refer to our research papers.

An overview of the 12 VR applications selected for our analysis

This table is included in our conference paper; please refer to the preprint for details.

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

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

a. VR game acronyms are colored Blue and VR playful application acronyms are colored Pink.

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

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

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

e. We included a second adventure game—LEGO®Bricktales—due to its appeal to children and child data privacy concerns raised by the Office of the Privacy Commissioner (OPC) [98] 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 [21].

A summary of deceptive design patterns observed by our researchers

This table is included in our conference paper. It presents the deceptive design patterns observed by our researchers, including their established definitions from literature and the specific privacy mechanisms through which they manifest in VR. Please refer to the preprint for details.

Theme/Subtheme	Pattern	Description	Synthesized diary entries[a]	Mechanisms
Sneaking				
Hiding Information	Submissive Acceptance[b]	Trick users into accepting an agreement without prior access to the agreement content.	I feel tricked because agreement was assumed and I did not get to view the actual privacy policy. MOSS2 ROOM FISHER RABBIT LEGO IMRSD CHAT	Consent interactions
Obstruction				
Adding Steps	Privacy Mazes	Bury privacy controls under layers of confusing menus.	I feel irritated having to dig through various settings tabs to find data practices that affect my privacy. FISHER CLIMB	Settings & resources
Social Engineering				
Social Proof	Endorsements and Testimonials	Portray biased or fabricated testimonials as genuine to influence users' purchase decisions.	Seeing testimonials tempts me to enter my credit card for the free trial, even though I don't know if they are from genuine users or paid influencers. SN	Registration & subscription
Interface Interference				
Manipulating Choice Architecture	False Hierarchy	Prioritize certain options, make it difficult to compare choices.	I feel inclined to click on the "sign up" or "start the free trial", which grants access to my personal data, because they are higher positioned than other options. SN	Registration & subscription
	Visual Prominence	Highlight distracting elements, causing users to forget or lose focus on their initial intent.	I feel more likely to click the "sign up", "allow", and "start demo" options with bigger size and eye-catching colors, which grants access to my personal data, than other available options. ROOM CHAT TRIPP SN IMRSD	Registration & subscription, Consent interactions
Hidden Information	Hidden Information	Obscure crucial details or disguising them as unimportant.	I feel confused about why certain data are collected due to the missing privacy policy and privacy settings. MOSS2 ROOM FISHER RABBIT LEGO IMRSD	Consent interactions, Settings & resources
			I feel confused about why my media and photo library access is required since the permission was requested prior to viewing the privacy policy or using related function. CHAT	Consent interactions
Bad Defaults	Bad Defaults	Set default options that benefit the company, forcing users to manually change settings to avoid privacy risks.	I feel concerned about accidental data-sharing because the option is checked by default. ROOM CHAT HRZ	Settings & resources, Consent interactions
Emotional or Sensory Manipulation	Positive or Negative Framing	Hide or downplay critical information through visual cues.	I feel inclined to click on "accept", "agree", and "start demo" because the bright green buttons make me feel safe to do so. TRIPP SN	Registration & subscription, Consent interactions
Trick Questions	Trick Questions	Use confusing wording or double negatives to manipulate users' choices.	I feel tricked into revealing personal information because the game asked for my gender and skin color instead of asking "create your avatar." CLIMB	QoL features*
Language Inaccessibility	Complex & Lengthy Language[c]	Use hard-to-understand words and sentence structures, hindering users' informed decisions.	While the game/application has a privacy policy, it is too lengthy and hard to read. BS CLIMB CHAT HRZ TRIPP SN	Consent interactions
Forced Action				
Nagging	Nagging	Disrupt user focus with repeatedly unwanted interruptions to push actions they would rather avoid.	I feel annoyed by constant "permission error" messages because I didn't grant access to my photos and media. CHAT	Notification
Forced Registration	Forced Registration	Require account creation for tasks that shouldn't need it, potentially extracting unnecessary personal data.	I feel annoyed that nothing is accessible without registration, even after I paid for subscription. I have to sacrifice my privacy without knowing potential risks or if it's worth it. TRIPP SN	Registration & subscription
Forced Communication or Disclosure	Privacy Zuckering	Trick users into thinking it's essential for the service, leading to overshare personal data.	I feel pressured to give my credit card information to be able to see the item prices or demo session, and even after doing so I was asked for more personal details upon re-entry. BS SN	Registration & subscription, QoL features*
			I feel confused about granting media and photo library access as I do not see related functions. ROOM CHAT	Consent interactions
	Mandatory Acceptance[b]	Trick users into accepting all terms in the agreement without customization.	I feel coerced into agreeing to all data sharing practices because I cannot opt-out of those that are irrelevant to the functions. FISHER TRIPP SN	Settings & resources

Note. Themes and codes in this table follow the sequence in our deductive codebook [58]. *QoL features = Quality-of-Life features.
a. VR games and playful applications acronyms match those in Table 1. VR game acronyms are colored Blue and VR application acronyms are colored Pink.
b. New deceptive design patterns synthesized from our diary entries, and are distinct from our initial codebook from literature [58].
c. We renamed the theme to highlight the "lengthy" issue in privacy policy language, in addition to the complexity noted in the original codebook [58].

Representative screenshots demonstrating the deceptive patterns in VR contexts



Figure 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.

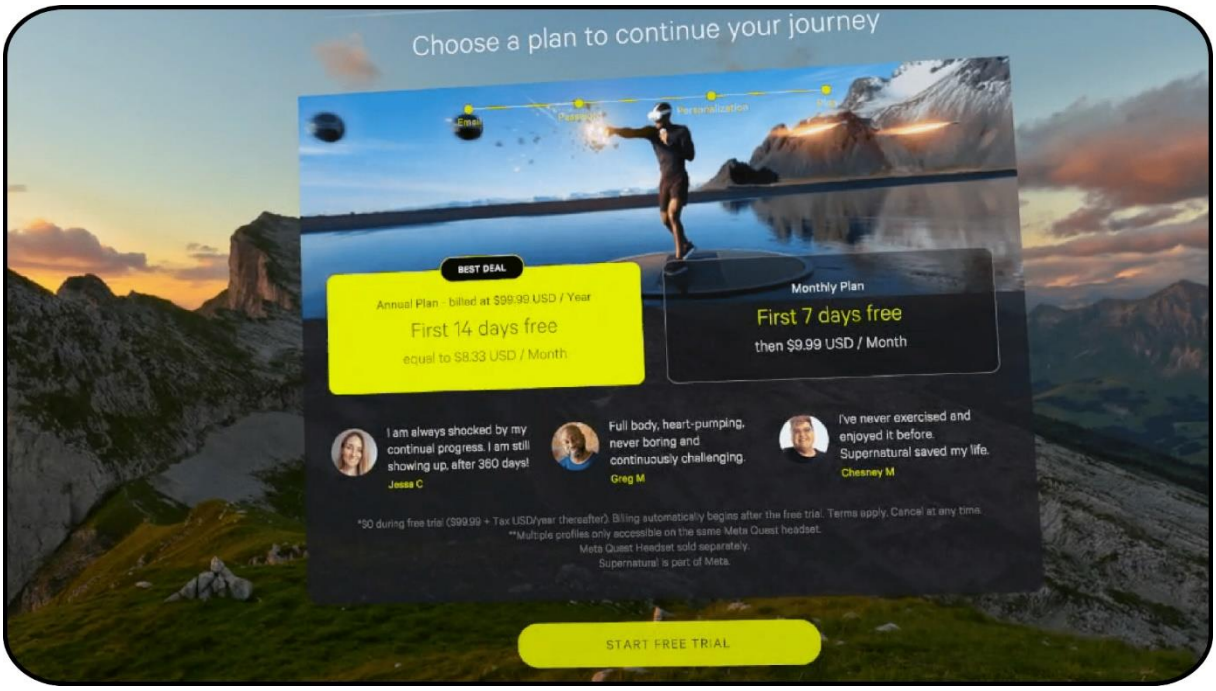


Figure 2. The subscription mechanism in Supernatural exemplifies the ***Endorsements and Testimonials*** deceptive design pattern. The mechanism features two different subscription plans alongside three testimonials that aim to persuade users to subscribe, which involves providing payment information, 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, immersive virtual environment that showcases vivid and lifelike landscapes, creates 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 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 encourages users to opt for privacy-invasive choices without fully understanding the implications of their decision.

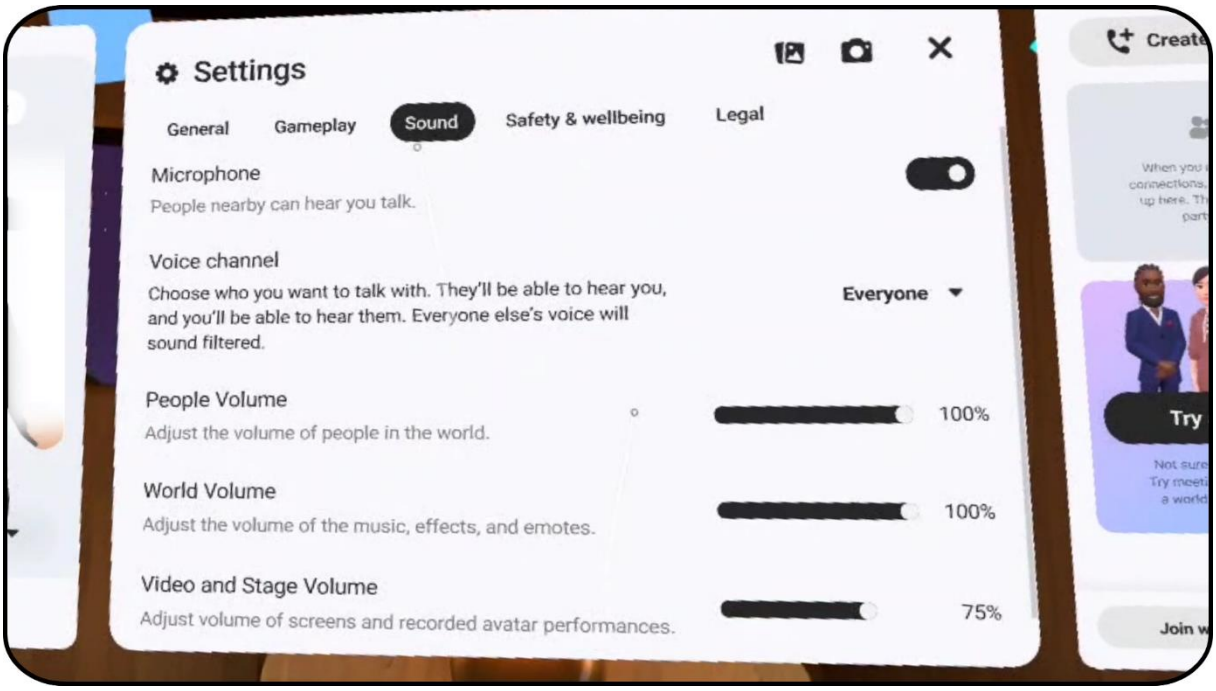


Figure 4. The consent interaction mechanism in Meta Horizon Worlds exemplifies the ***Bad Defaults*** deceptive design pattern. Within the settings menu, several privacy-invasive options are pre-enabled by default. These include automatically activating the microphone ("people nearby can hear you talk"), 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.

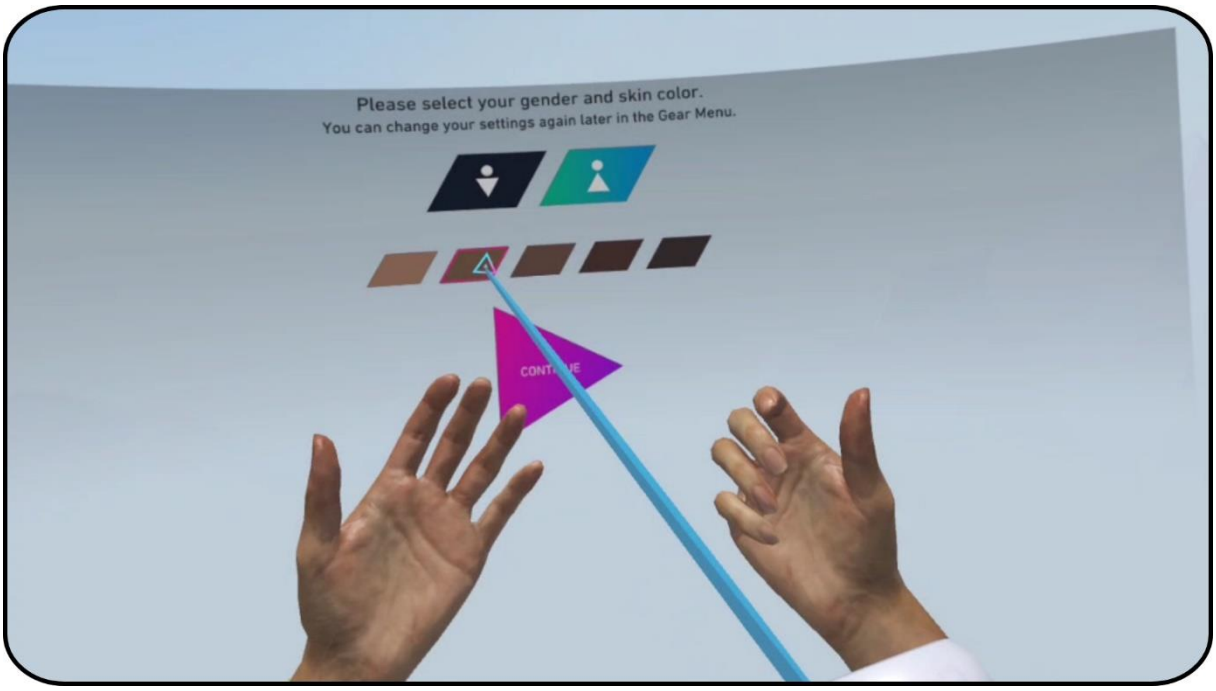


Figure 5. The quality-of-life (QoL) feature that facilitates avatar customization in The Climb 2 exemplifies the ***Trick Questions*** deceptive design pattern. In this interface, users are asked to choose their gender and skin color, phrased as "select your race and gender". Although this question was 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, data about users' avatar becomes a valuable source for inferring their personal characteristics.

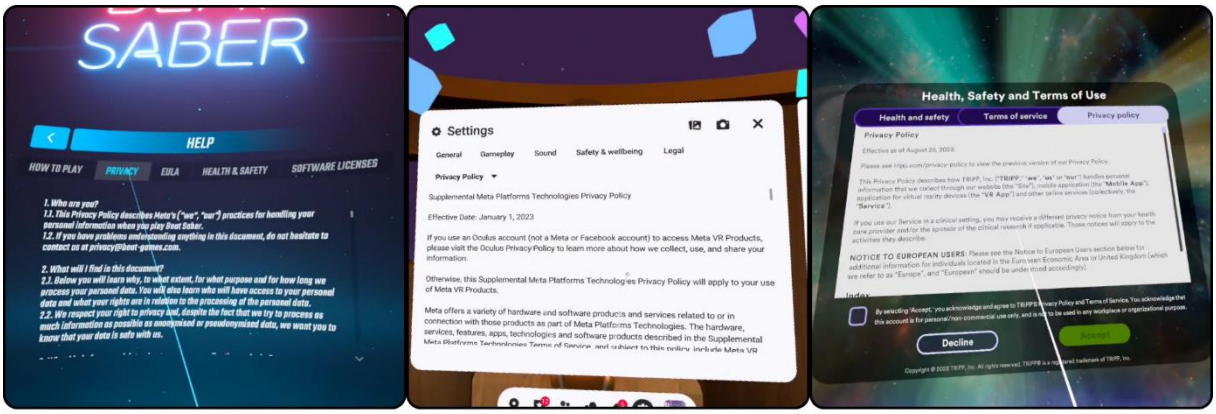


Figure 6. The in-game and in-app privacy policies in Beat Saber (see left screenshot), Meta Horizon Worlds (see center screenshot), and TRIPP (see right screenshot) exemplify ***Complex & Lengthy Language*** deceptive design pattern. Although they aim to inform users about data practices upon first entry, these documents are often lengthy and difficult to read. This complexity discourages users from fully reading the terms and hinders their comprehension of potential privacy risks. Our findings from privacy policy analysis further support this conclusion (see our research papers).



Figure 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 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 playful applications 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 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.

VR PRIVACY-ENHANCING DESIGN SCREENSHOTS & DESCRIPTION

Through our examination of privacy-related deceptive design in 12 popular VR applications, we also identified privacy-enhancing designs in VR privacy mechanisms that improve user awareness, and support more informed decision-making.

This section includes screenshots that demonstrate how these design patterns can enhance people's understanding of privacy information and facilitate them in making informed privacy decisions. These design patterns reflect commercial VR applications' efforts to enhance user privacy and offer valuable insights into how VR platforms can prioritize user privacy while maintaining engaging and immersive experiences.

A summary of privacy-enhancing design patterns observed by our researchers

This table presents a summary of privacy-enhancing design patterns (also known as "bright patterns") observed by our researchers, including their descriptions and the specific privacy mechanisms through which they manifest in VR. This table is included in our conference paper; please refer to the preprint for details.

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

Note. *QoL features = Quality-of-Life features.
a. Patterns are organized by their frequency of appearance, with the most common among all VR games and apps at the top.
b. We included acronyms for VR games and apps, matching those in Table 1, from which the diary entries originated. VR game acronyms are colored Blue and VR app acronyms are colored Pink. Entries not linked to acronyms are desired ethical design strategies from our diary entries and do not exist in the selected VR games and apps.

Representative screenshots demonstrating these patterns in VR contexts

The screenshots demonstrate visual evidence of deceptive design patterns identified during our evaluation of VR applications. Each example illustrates how privacy mechanisms are presented to users in ways that may undermine transparent understanding and informed decision-making.

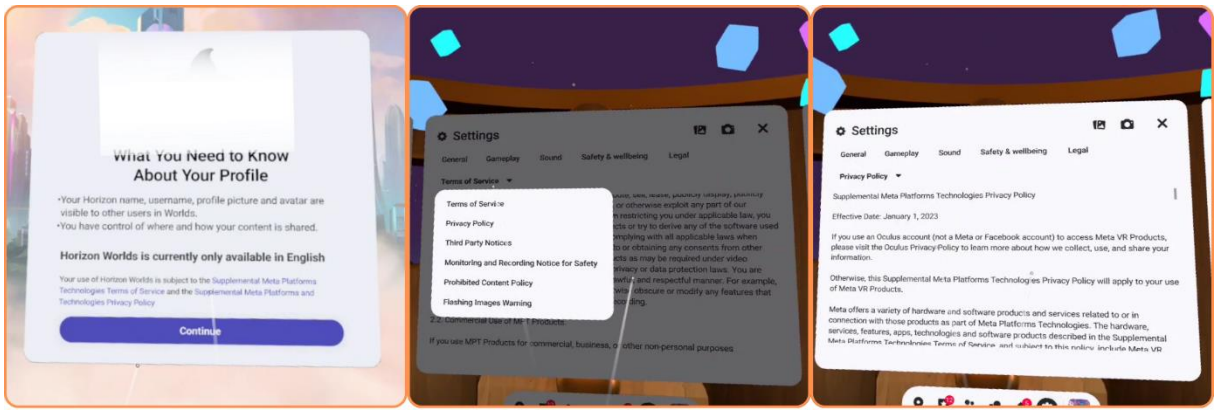


Figure 10. The in-app privacy policy in Meta Horizon Worlds exemplifies the ***Accessible privacy policy*** bright design pattern. Upon entry, the application provides users with a brief description of its data practices, along with hyperlinks to more detailed information available on external webpages (see left screenshot). This privacy information can also be accessed at any time through the settings menu (see center and right screenshots). This design ensures users can easily revisit it as needed.

Note: Our researcher's username and avatar image are concealed in the screenshot for anonymity.

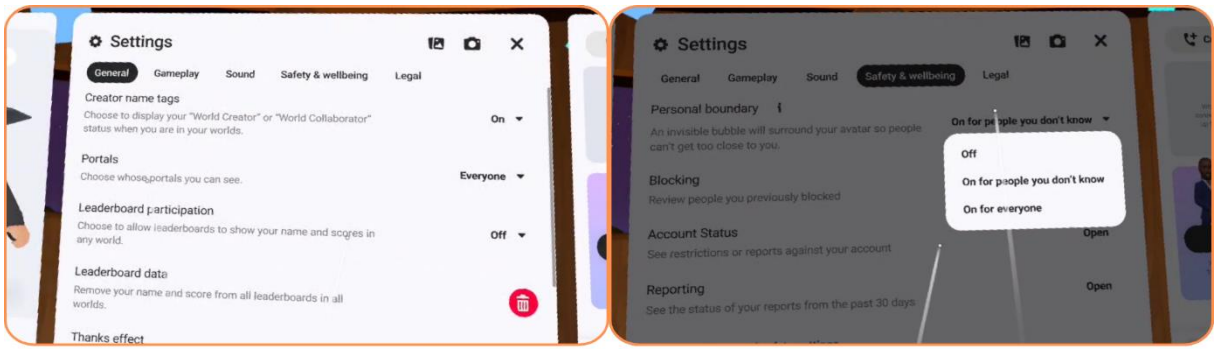


Figure 11. The settings mechanism in Meta Horizon Worlds exemplifies the ***unbiased presentation of choices*** bright design pattern. All options on the menu are in black and white, with the data deletion option distinctively highlighted in red to make it stand out (see left screenshot). Even within the drop-down menus, the options maintain a consistent color scheme, with the most privacy-preserving choice ("off") placed at the top (see right screenshot).



Figure 12. The consent interactions and settings mechanisms in VRChat (see the left and center screenshots) and the consent interactions mechanism in TRIPP (see right screenshot) exemplify the ***privacy-friendly default*** bright design pattern. These mechanisms ensure that privacy-related options are unchecked by default and require users to decide to opt-in. In VRChat, the microphone is set to "toggle" mode by default to prevent unintended listening by others. We note that although VRChat also enables auto-joining the world voice channel by default, we do not consider this a privacy-invasive bad default since the microphone remains in "toggle" mode and must be manually activated by the user.

Note: Our researcher's username is concealed in the right screenshot for anonymity



Figure 13. The quality-of-life (QoL) features, such as the private beginner spaces in VRChat (see left screenshot) and Meta Horizon Worlds (see center screenshot) and private workspace in Immersed (see right screenshot), exemplify the ***private privacy configuration space*** bright design pattern. Upon entry, these applications place users in private spaces where they can explore functionalities, adjust settings, and customize avatars before interacting in public spaces. This design allows users to familiarize themselves with privacy settings, review policy information, configure privacy preferences, and customize their avatar and username tag to conceal personal information before joining public virtual worlds.



Figure 14. The quality-of-life (QoL) feature, specifically the microphone icon in VRChat (see center screenshot), and the notification mechanisms in The Room VR (see left screenshot) and Meta Horizon Worlds (see right screenshot) exemplify ***the transparent communication of data practices*** bright design pattern. The VR Chat implemented a microphone icon on the bottom of the screen to keep users aware of their microphone status. The Room VR notifies users when their height is calibrated specifically for gameplay purposes, and Meta Horizon Worlds provides a brief description of data practices upon users' entry that clearly states what data is collected and for what purposes.



Figure 15. The privacy resource mechanisms in Meta Horizon Worlds (see left screenshot) and VR Chat (see right screenshot) exemplify the ***clear control mechanisms*** bright design pattern. Meta Horizon Worlds uses an illustrative image to show users how to access the settings menu, and VR Chat provides sign boards to guide users to ensure that privacy controls can easily be located.

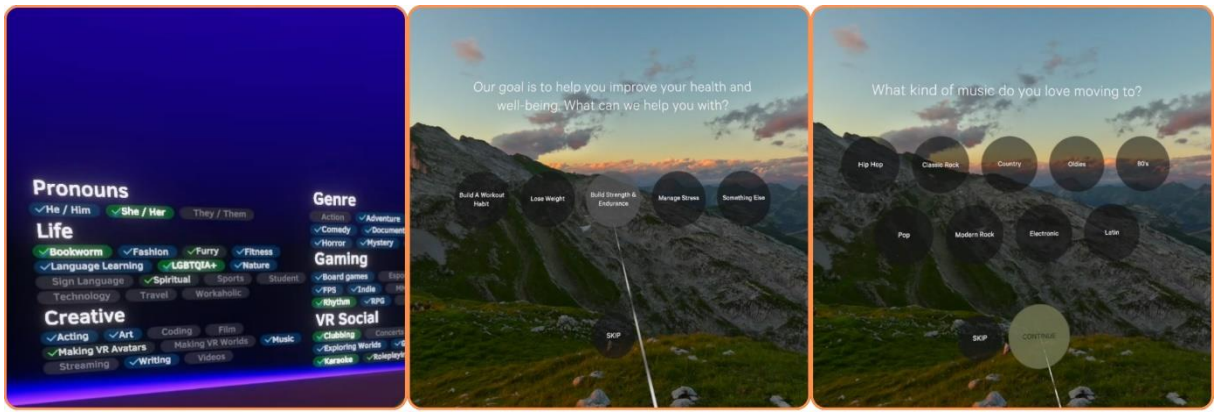


Figure 16. The quality-of-life (QoL) features in VRChat and Supernatural exemplify the ***balanced privacy and functionality*** bright design pattern. In VRChat, users are invited to provide personal details like lifestyle and social preferences to help find matching friends, but this step is optional (see left screenshot). The friend-matching can still be made without sharing this information. In Supernatural, users are asked to select their fitness goals and preferred music genre for sessions, with the option to skip these selections if preferred (see center and right screenshots).