

Ethical Design for Data Privacy and User Privacy Awareness in the Metaverse

Ophelia Prillard^a, Costas Boletsis^b and Shukun Tokas^c

SINTEF Digital, Forskningsveien 1, 0373 Oslo, Norway

Keywords: Data Privacy, Ethics, Extended Reality, Metaverse, User Privacy.


Abstract: The significance of the metaverse has been growing rapidly within the online realm. However, several challenges remain, including privacy, ethics, and governance. Extended reality (XR) devices used to access the metaverse are equipped with high-quality sensors that can collect large amounts of sensitive user data, including biometric data and spatial data. Such considerations raise major concerns about the extent and nature of user data that this massive platform could accumulate, the data collection awareness and transparency it will provide to its users, and the ethical nature of the informed user consent it will request. This research aims to document and analyze the privacy challenges that arise from a prevalent metaverse application, align them with the related literature, and present an initial set of ethical design suggestions that can mitigate these privacy challenges. To do so, a case study shapes and informs a set of ethical design suggestions. The user onboarding of a prevalent multi-user/remote working metaverse application, Meta Horizon Workrooms, was documented and modeled through a user journey modeling language, CJML. The walkthrough revealed certain challenges regarding data privacy awareness, such as long, legally worded privacy policies, a hard-to-use user interface that can affect privacy awareness, and ambiguous wording in data-collection notices. Several best practices regarding user privacy were examined to tackle these issues, and certain ethical design solutions (e.g., informed user interface, design privacy icons, anonymization, logging, revising all consent) are suggested.


1 INTRODUCTION


Since its inception, the concept of the metaverse has been continuously evolving. It has been described in various ways, such as a second life, 3D virtual worlds, and life-logging (Wang et al., 2022; Sanchez, 2007; Dionisio et al., 2013; Bruun and Stentoft, 2019). In general, the metaverse is commonly defined as a fully immersive, hyper spatiotemporal, and self-sustaining virtual shared space that seamlessly blends elements of the physical, human, and digital realms (Wang et al., 2022; Ning et al., 2023). The metaverse is recognized as a developing paradigm in the next generation of the Internet, following the revolutions brought about by the World Wide Web and mobile Internet. Extended reality (XR) devices, such as the Microsoft HoloLens, Meta Quest, HTC Vive, and Apple Vision Pro head-mounted displays (HMDs), are gateways to the metaverse, enabling immersive digital experiences and transforming how individuals experience this next

frontier of the internet (Warin and Reinhardt, 2022; Wang et al., 2022). These devices are equipped with a collection of sensors, such as cameras, proximity sensors, gaze tracking sensors, microphones, temperature sensors, and many more, that allow tracking of users (e.g., face, hands, eye-gaze) and their surroundings (e.g., people, places, objects) (Warin and Reinhardt, 2022; Cheng et al., 2022).

In 2021, the metaverse concept swiftly gained widespread popularity, rekindling optimism about the possibility of forging an ideal virtual society characterized by strong human connections. This surge in interest prompted major corporations to pledge their commitment to metaverse development, aligning with their vision of a centralized virtual realm (Xu et al., 2023; Wang et al., 2022). Perhaps the most prominent among these companies is Meta, formerly Facebook. In September 2019, Meta unveiled Meta Horizon Worlds, a virtual reality (VR) social platform, and Meta Horizon Workrooms, a virtual office and meeting room environment, and allocated over \$10 billion toward its metaverse initiative in 2021. Notably, Meta's XR headset, the Quest 2, has achieved

^a  <https://orcid.org/0000-0003-1744-9720>

^b  <https://orcid.org/0000-0003-2741-8127>

^c  <https://orcid.org/0000-0001-9893-6613>

remarkable success, boasting sales exceeding 10 million units and securing its status as the cutting-edge, top-selling VR product globally. Furthermore, in August 2021, Nvidia introduced its plans for Omniverse, the first-ever virtual collaboration and simulation platform. In October 2022, Microsoft also made its mark by presenting Mesh, a metaverse platform designed to connect remote and hybrid workers (Cheng et al., 2022; Fernandez and Hui, 2022; Wang et al., 2022). Currently, there are a high number of metaverse-related patents filed by major corporations (Murphy, 2022; IFI Claims Patent Services, 2022), further revealing the business interest in the metaverse domain (cf. (Stahl et al., 2020; Teller, 2023)).

The growing commercialization of the metaverse, its highly centralized nature, and its multisensor-based usage have raised major concerns from well-established organizations, such as the International Association of Privacy Professionals (Weingarden and Artzt, 2022) and the World Economic Forum (World Economic Forum, 2023), as well as the academic community (Wang et al., 2022; Di Pietro and Cresci, 2021; Fernandez and Hui, 2022), about the extent and nature of the data this massive platform could accumulate, the data collection awareness and transparency it will provide to its users, and the ethical nature of the informed user consent it will request (Di Pietro and Cresci, 2021; Fernandez and Hui, 2022).

The constant surveillance from XR devices to deliver more immersive experiences in combination with the users' vulnerable, immersed cognitive state can jeopardize their privacy and safety. Biometric data, such as gaze features, gait recognition, face prints, voice prints, heart rate, and temperature, can be used to accurately profile users, analyzing their actions, reactions, and emotions as they interact with content and other users. Surveillance capitalism (Zuboff, 2019) and respective profiling practices based on sensitive biometric data are currently a significant privacy risk for the metaverse. Potential applications of these practices could be to provide highly targeted and personalized user content (e.g., advertisements) or even shape user beliefs (Fernandez and Hui, 2022; Roesner et al., 2014; Di Pietro and Cresci, 2021; Warin and Reinhardt, 2022; Dwivedi et al., 2022). That raises even more significant concerns when combined with the fact that many XR headsets and metaverse software can be used by users younger than 18. For example, Meta Quest can be used by users aged 13+¹ (Cheng et al., 2022; Choi, 2022; Lee et al., 2022). Moreover, camera record-

ings of physical surroundings, taking place through XR devices, can reveal the users' physical location with high accuracy, and business data privacy may be compromised when the metaverse is used for remote working. Hence, sensitive business data is shared in metaverse settings.

This paradigm shift in the way individuals, communities, and institutions engage offers positive avenues, such as enhanced avatar anonymity, and daunting challenges, especially concerning privacy, with the metaverse's inherent profiling, monitoring, and potential privacy invasions emphasizing the ethical dilemmas tied to sensitive data collection (European Data Protection Supervisor, 2022).

This early stage presents the first step in designing for user privacy and data privacy awareness in the metaverse from an ethical standpoint. The *goal* of this research is to document and analyze the privacy challenges that come from a prevalent metaverse application, align them with the related literature, and present an initial set of ethical design suggestions that can mitigate these privacy challenges. This work's *contribution* resides in (i) presenting an empirical, methodological approach for evaluating the privacy stages of metaverse application, (ii) describing a set of ethical design suggestions that researchers and practitioners can use in the field and inform their designs, and (iii) raising awareness on the topic of user privacy in the metaverse. The project's *vision* is to produce an ethical design framework for privacy by design in the metaverse.

2 CASE STUDY

2.1 Methodology

A case study is carried out to approach the aforementioned goal. Based on the designed methodology, the user onboarding process in a prevalent metaverse application is documented and modeled, at first, through a user interface walkthrough.

Then, the documented user onboarding is analyzed as to the potential privacy-related challenges and gaps that users may face. The main focus is to extract and analyze how users are informed about *privacy disclosures* (often termed privacy notices), how the *consent* is requested from the users, and how much control they have over their *collected data*. Identifying the potential challenges and gaps is based on the authors' heuristic evaluation of the onboarding as experts in usability, user experience, privacy, and extended reality.

Finally, based on the results of the analysis, a set

¹Meta Quest safety information for parents and preteens, <https://www.meta.com/no/en/quest/parent-info/>



Figure 1: The Meta Quest Pro headset.

of ethical design suggestions (i.e., mitigation actions) are proposed. These suggestions come from a scoping literature review on privacy-related best practices.

Overall, the methodology is designed with a mapping approach in mind, addressing the "cold start" issue that can be present early in designing the initial set of potential solutions for user privacy awareness in the metaverse. Furthermore, the visualization of the user onboarding process, as both an interface walkthrough and a journey model, allows for the combination of experiential/qualitative elements (from the walkthrough) and quantitative observations (from modeling), thus providing clearer documentation of the privacy challenges users may face.

2.2 Apparatus & Software

For the case study, the Meta Quest Pro XR headset² (Fig. 1) was used. Meta Quest Pro is an advancement over the top-selling XR headset, Meta Quest 2. Meta Quest Pro features a variety of tracking options that are expected to become commonplace very soon (e.g., with the Apple Vision Pro XR device³), such as face-, eye-, and hand-tracking, to enable an immersive experience and more natural avatar expressions and movements. More specifically, it features five cameras for room scale, two cameras for face tracking, three cameras per controller for self-tracking, and three cameras for eye tracking. As for sensors, it is equipped with an ambient light sensor, accelerometer, proximity sensor, gyrometer, barometer, and magnetometer.

Regarding the application used in the case study, the virtual office environment of Meta Horizon Workrooms (v1.15) was chosen. Horizon Workrooms is part of Meta's popular Horizon metaverse brand and has been widely used in research in the fields of edu-

²Meta Quest Pro,
<https://www.meta.com/no/en/quest/quest-pro/>

³Apple Vision Pro,
<https://www.apple.com/apple-vision-pro/>

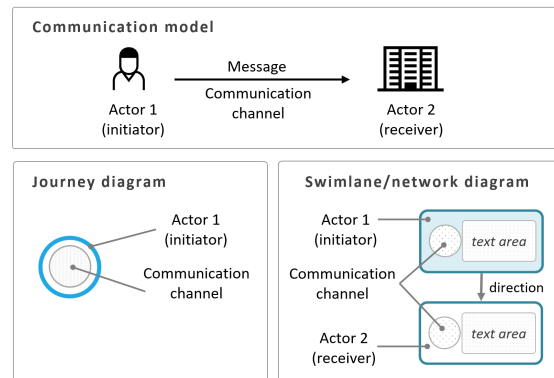


Figure 2: CJML's communication model with a sender transmitting a message to a receiver through a communication channel (upper part). The visual representation of a touchpoint in the case of a journey diagram (left) and a swimlane diagram (right) (Boletsis et al., 2021).

cation and networking, among others (Zolezzi et al., 2023; Skorupska et al., 2022; Hedrick et al., 2022; Hwang et al., 2023; Alhilal et al., 2023; Cheng et al., 2022). Horizon Workrooms has also been used in Colombia for the first court hearing in the metaverse (Bello, 2023).

2.3 User Onboarding & Modeling

The user onboarding for the Meta Horizon Workrooms application has been recorded as a user interface walkthrough, and the videos can be accessed⁴. Video 1 presents a "privacy-unaware" user journey (i.e., the user immediately consents to all data collection), while Video 2 shows a "privacy-aware" user journey, where the user opens the privacy notices and chooses not to share data. The purpose of showing both onboarding processes is to provide readers with more complete documentation of the user onboarding process. It also provides insight into how these two onboarding journeys can differ.

Then, the walkthrough was modeled using the CJML modeling language to visualize its parts clearly and quantitatively. CJML represents a visual language designed to model and illustrate service and work processes in the context of customer or user journeys. This approach is informed by a user-centric design methodology, making it accessible and intuitive to a wide range of users (Halvorsrud et al., 2021; Halvorsrud et al., 2016). In CJML, the fundamental building blocks are observable touchpoints, which can be either a "communication event" or a "non-communicative activity or action." A user's path

⁴Video recordings of user onboarding.
<https://xrlab.no/visd/videos.html>

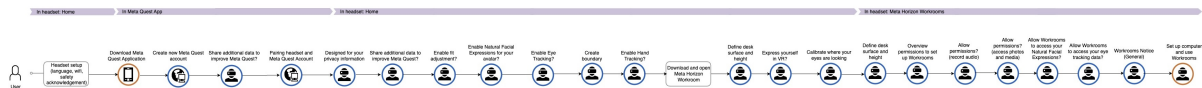


Figure 3: The CJML-created user journey model for the user onboarding process of Meta Horizon Workrooms, using the Meta Quest Pro. The blue-bordered icons are actions initiated by Meta asking for user input. A full-scale copy of the figure can be accessed at: <https://xrlab.no/visd/cjml.png>.

through these touchpoints to achieve a specific goal is referred to as a "user journey" (Halvorsrud et al., 2021; Halvorsrud et al., 2016; Halvorsrud et al., 2023). CJML offers two distinct diagram types, each serving a unique purpose (as illustrated in Figure 2). The "journey diagram" best suits journeys involving only a few actors and highlights deviations from the planned journey. On the other hand, the "swimlane diagram" is valuable for journeys that involve multiple actors, emphasizing both the initiator and the recipient of each touchpoint (Halvorsrud et al., 2021; Halvorsrud et al., 2016; Halvorsrud et al., 2023)

A journey diagram (Fig. 3) was designed for this case study. The blue touchpoints denote the communication initiated by Meta, involving requests for user input, notably through consent requests. Most of the time, user input involves reading and agreeing with some type of text, as seen in video recordings³. The modeling was carried out by the authors, who have vast experience in the use of CJML, and it was supervised by the creator of CJML, Dr. Halvorsrud.

2.4 Evaluation Results

Expert evaluation of the user onboarding process for the Meta Horizon Workrooms application using the Meta Quest Pro headset revealed challenges related to data privacy and user privacy awareness. The main theme that runs through the identified challenges is that the UI of the device and the application are not properly designed to facilitate the delivery of privacy-related information, specifically in XR settings. These challenges are described below.

Users must read quite *long texts of privacy notices* and terms before deciding on consent. For instance, to create a Meta Quest account, the user agrees to the terms that describe how they can read the "Meta Privacy Policy" and the "Supplemental Privacy Policy" to learn how their data are collected, shared, and used. The Supplemental Privacy Policy (effective 25 July 2023) consists of approximately 9,000 words. The printable version of the Meta Privacy Policy (effective 7 September 2023) contains approximately 26,800 words. In the Meta Horizon Workrooms, the extensive text of the Supplemental Privacy Policy (effective 1 January 2023) is displayed in a confined scroll area, posing readability challenges, particularly in XR set-

tings. Notably, the texts for the additional policies, such as the face tracking, eye tracking, and fit adjustments policies, are delivered as text on webpages through WebView.



Figure 4: An example of an "accept" button for sharing data that is visualized with bright blue color and a "reject" button in dark grey. There is also another link right above the two buttons (Hands Privacy Notice) that is styled like regular text (00:40 in Video 1).

The *UI design choices regarding buttons, links, scrollbars, and window sizes* make it challenging to access all the necessary information to provide informed consent. In most cases, the positive consent option that enables data sharing (e.g., tracking of natural facial expressions, eye tracking, and fit adjustments) is highlighted in bright blue. The negative option is highlighted in dark gray (Fig. 4). When users do not consent to tracking, such as hand tracking, they can only click a "Not Now" button. Upon reappearance, the "Permanent Dismiss" option is displayed as text positioned below the two other buttons, necessitating deliberate consideration before selection. The way users are prompted to enable features that come with a policy notice vary and can be inconsistent and unclear. In some cases, it is delivered as a text link in a different color, as a "Learn More" button, or even as regular, unstyled text that behaves as a link only on hover (like the Hands Privacy Notice link above the two buttons in Fig. 4). Moreover, identifying scrollable panels is challenging since some hovering action must take place to be highlighted as a scrollable area (Fig. 5). Finally, even though Horizon Workrooms deliver content in large windows, the windows become much smaller when it comes to information on privacy policies and consent (Fig. 6).

When it comes to *consent forms*, there were negative consent options that, when selected, prevented users from proceeding, as they were considered necessary for the application. For instance, to access Horizon Workrooms, the user must enable hand tracking and agree to the "Hands Tracking Notice." Permission is mandatory to enter the application. However, once inside, users seamlessly navigate and operate with the controllers. This reveals a more significant concern since it is unclear which specific data is being collected in real-time while using the application, what data is needed and requested by the software, and what is needed by the hardware. Moreover, during the onboarding process, there are several consecutive consent requests (Fig. 3) that deal with a specific subject (e.g., tracking) but are delivered in a gradual, serial way, piece-by-piece. Finally, despite the presence of privacy menus enabling users to toggle additional tracking options on/off, the privacy policies, the Meta Privacy Policy, and the Supplemental Meta Platforms Technologies Privacy Policy are non-negotiable. Declining or revising them is not an option if the user intends to use the headset or the application.

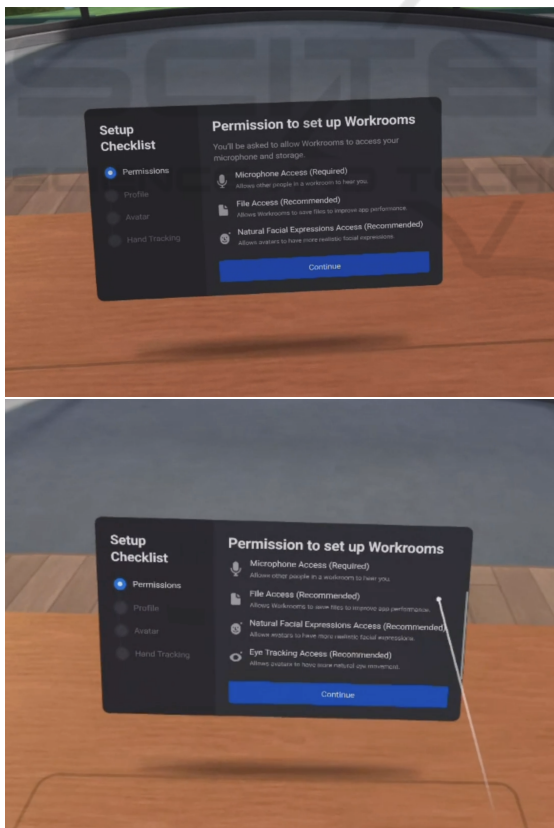


Figure 5: An example of a window with a "hidden" scrollbar that appears only on hover, revealing that the application will also request eye tracking.



Figure 6: An example of a window requesting tracking consent and its size compared to its surroundings and user's field-of-view.

3 DISCUSSION

3.1 General Observations

As stated above, the expert evaluation of the user onboarding process for the Meta Horizon Workrooms application identified several challenges regarding the UI design of the application. More specifically, it revealed how challenging it can be for users to achieve full privacy awareness in XR settings. Naturally, these challenges can be attributed to uninformed design choices. Nevertheless, literature tends to connect these challenging UI settings (especially when biometric data is shared) with "dark patterns." Dark patterns are sophisticated, manipulative, and deceptive interfaces that can deceive, steer, or manipulate users into behavior (e.g., buying products, giving consent without reading privacy notices) that is profitable for online services/platforms etc. (Gunawan et al., 2022).

Based on the literature, Meta is known for using dark patterns, leading to the coining of the term "privacy zuckering" (Gunawan et al., 2022; Bösch et al., 2016). The term was first introduced by Tim Jones in an EFF article (Jones, 2010) for "deliberately confusing jargon and user-interfaces," and it refers to the use of dark patterns (Bösch et al., 2016). It was also observed that the applications adhere to the *data protection by default* principle, as it initially disables face, eye, and hand tracking features. However, it can be pointed out that the current UX design (Fig 4, Fig 6) may inadvertently influence users toward enabling tracking features.

3.2 Privacy Notices

”Designers use dark patterns to hide, deceive, and goad users into disclosure. They confuse users by asking questions in ways non-experts cannot understand, they obfuscate by hiding interface elements that could help users protect their privacy, they require registration and associated disclosures to access functionality, and hide malicious behavior in the abyss of legalese privacy policies.” (Waldman, 2020). In this case study, the Supplemental Privacy Policy consists of approximately 9,000 words, while the printable version of the Meta Privacy Policy consists of approximately 26,800 words. It would take the average user 37 minutes and two and a half hours to read these policies alone, based on the average reading rate (238 words/minute (Brysbaert, 2019)). Realistically, expecting users to spend that much time reading privacy notices while attempting to use a metaverse application is highly unlikely, meaning they may not be fully privacy-aware when they consent to sharing data due to inherent, problematic design decisions.

3.3 User Interface

At the same time, the user has to read through and consent to several consecutive policies while having to deal with (i) hidden scrollbars, (ii) small window size, (iii) inconsistently styled buttons (shiny/blue buttons versus grey ones), and (iv) inconsistently styled hyperlinks. One might say that these design choices belong to dark patterns under the *interface interference* (Gray et al., 2023; European Data Protection Board, 2023) practice, making it hard for users to navigate the data practices and privacy controls. More specifically, points (i) and (ii), mentioned above, may fall under the *aesthetic manipulation* practice to challenge users’ access to information, point (iii) may be *stirring* (i.e., guiding users toward the ”shiny” choice), and point (iv) could utilize the *inconsistent interface* practice to challenge users’ cognitive memory and, again, challenge their access to information (Gray et al., 2023; European Data Protection Board, 2023; Waldman, 2020).

3.4 Consent

In general, dark patterns to obtain user consent raise significant concerns in light of the General Data Protection Regulation (GDPR)⁵ (Voigt and Von dem Bussche, 2017). Article 7 of the GDPR underscores the necessity for clear, distinguishable privacy notice,

⁵GDPR,
<https://gdpr-text.com/read/article-7/>

emphasizing users’ right to withdraw consent at any time. In this case study, the Meta privacy notices are fairly detailed. Nevertheless, the complex nature of data processing, storage, and sharing can be confusing for the average user. *Ambiguous wording* for sensitive data (gaze and facial tracking data) could potentially lead to misunderstandings and concerns about privacy. For example, the terms ”raw image data,” ”abstracted facial expression data,” and ”abstracted gaze data” do not explicitly list what they entail and can be difficult to understand (for experts and average users). Another example is in the event of a crash, eye calibration data might be sent to Meta servers, but the purpose and duration of its retention on the servers are unclear. Several statements, such as ”crash logs are stored on Meta servers until no longer necessary,” can be vague about the specific duration for data retention. In addition, users can, indeed, disable hand-, face-, and eye-tracking, yet to the author’s knowledge, there was no option to withdraw all consent, which may not be aligned with Article 7’s requirement. Finally, ”dark patterns also make disclosure ‘irresistible’ by connecting information sharing to in-app benefits” (Waldman, 2020), something that is the case herein (e.g., giving consent for facial tracking is advertised as a best practice to create an attractive and expressive avatar that mimics user’s facial expressions in real time).

3.5 Design Suggestions

In this work, the focus is on a single hardware device and a specific application. Naturally, any concerns regarding user privacy awareness or dark patterns cannot be proof of their existence in all XR hardware and metaverse applications. However, they can be indications and cautionary tales for any metaverse-related hardware/software. At this point, after identifying certain privacy-related challenges under specific metaverse settings and aligning them with related research, several ethical design suggestions are proposed, aiming to mitigate the aforementioned issues. To formulate the suggestions, the works of (a) Fernandez et al. (Fernandez and Hui, 2022) on privacy, governance, and ethical design in the metaverse, (b) the XRSI Privacy Framework (XR Safety Initiative, 2020) on a layered structure focused on privacy within an XR system, and (c) Abraham et al. (Abraham et al., 2022) on a useful list of recommendations for secure and private XR systems, were taken into great consideration. Finally, the review by Heurix et al. (Heurix et al., 2015) on privacy-enhancing technologies (PET) was also utilized.

Fig. 7 provides an overview of the ethical design

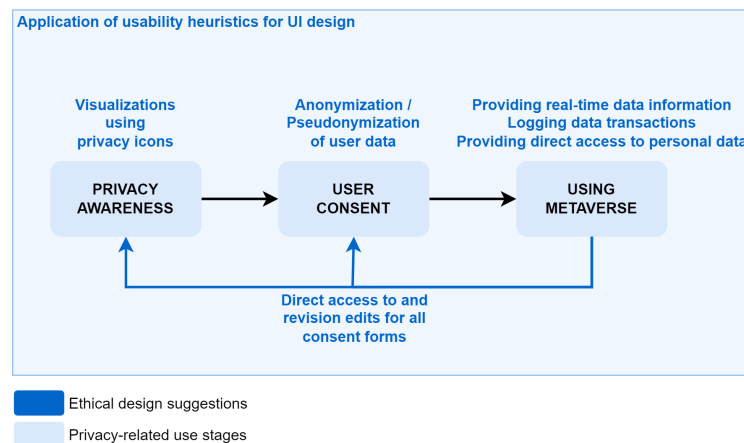


Figure 7: An overview of ethical design suggestions for data privacy and user privacy awareness in the metaverse.

suggestions based on the privacy-related use stages. In general, it is imperative that the *UI is user-friendly and easy-to-use* throughout the metaverse use. Applying usability heuristics and XR-focused UI design guidelines would ensure that users are not challenged by UI elements while attempting to achieve privacy awareness. Specific suggestions for each privacy-related use stage follow.

- Privacy Awareness.** Long privacy notices can be summarized using *privacy icons* to effectively convey privacy choices. Icons can convey information visually and succinctly (Massironi et al., 2001). Privacy icons are collections of standardized, easily understandable, and user-friendly visual symbols. These symbols represent various aspects of specific data handling practices, assessed in terms of their associated risks and accompanied by concise textual descriptions. As a result, users can better grasp potential privacy implications, leading to decreased uncertainty and enabling more informed decision-making (Efroni et al., 2019; Holtz et al., 2011).
- User Consent.** At this stage, it is important to provide users with more flexibility than merely sharing the data or being unable to use the application. De-identification, specifically, *anonymization* and *pseudonymization*, can allow users to use the applications while preserving their privacy. Anonymization can transform data in such a way that it can no longer be used to identify an individual, even when combined with other data, and pseudonymization can replace or encrypt personally identifiable information (PII) with artificial identifiers or pseudonyms (Heurix et al., 2015; Štarchoň and Pikulík, 2019). Moreover, additional flexibility is needed because users should be able to give or refuse consent to or anonymize

or pseudonymize individual data practices. Integrated consent bundled together with multiple and diverse data practices should be discouraged.

- Using Metaverse.** When using a metaverse application, it can be crucial to combat user uncertainty about privacy through transparency. Privacy-related information about exactly what data are being shared at any specific time can be provided through *discrete, real-time visualizations* (e.g., with privacy icons). At the same time, any data-sharing transaction can be stored in an easily accessible *log file* that contains a detailed account of the activity (e.g., a timestamp of the transaction and data type). *Direct access to all shared datasets and personal data* (e.g., by a single link or a menu item) is also essential (Heurix et al., 2015; Abraham et al., 2022). In the same way, direct and easy access should be provided to all consent forms that users have decided upon in the past and not to just some of the choices (e.g., tracking). That way, users can re-read all the forms and revise their consent at any time, benefiting from the application of GDPR's Article 7⁴.

These suggestions, as formulated in this work, provide the starting material toward a methodological, iterative, "evaluation-and-refinement" stage, where other metaverse applications can be evaluated as to their user privacy and data privacy awareness and, therefore, lead to the following evaluation and refinement of these design suggestions.

4 CONCLUSION

The metaverse is rapidly expanding, accompanied by the proliferation of sensor-equipped XR devices. This

growth presents a pressing concern regarding data privacy and user awareness for informed consent. Our research aimed to address this concern by developing and presenting an ethical design framework tailored to the metaverse.

The case of a prevalent application, the Meta Horizon Workrooms, was studied to achieve this goal. A detailed walkthrough of the onboarding process using the Meta Quest Pro HMD was implemented. The analysis unveiled several noteworthy issues, mainly raising concerns about the potential employment of dark pattern design choices, which could push for the acquisition of sensitive data, such as biometric information. Then, the investigation was linked to work in the field, leading to an initial set of ethical design suggestions that can be further studied and applied in future work.

It must be noted that the generalizability of the formed ethical design suggestions is limited by the focused part of the metaverse evaluation presented herein, even if all parts are grounded in literature. However, this work represents the very first step toward a complete ethical design framework for privacy by design. These suggestions are promising starting material to be used by researchers and practitioners in the field to further conduct evaluation studies of existing metaverse applications and implement them as part of new or open-source metaverse applications that will be empirically studied. It is expected that an iterative design process will take place to evaluate and refine them before solidifying them into an ethical design framework. Ultimately, this research plans to contribute to a safer and more ethically designed metaverse environment for all users.

ACKNOWLEDGEMENTS

This research was supported by the SINTEF projects "VisD: Extended Reality Visualization on Data Privacy Awareness" and "TrustworthyMetaverse", funded by the Basic Funding through the Research Council of Norway. We would like to thank Dr. Halvorsrud for her valuable contribution to the application of CJML.

REFERENCES

- Abraham, M., Saeghe, P., McGill, M., and Khamis, M. (2022). Implications of XR on privacy, security and behaviour: Insights from experts. In *Proc. of NordiCHI*, pages 1–12.
- Alhilal, A., Shatilov, K., Tyson, G., Braud, T., and Hui, P. (2023). Network Traffic in the Metaverse: The Case of Social VR. In *Proc. of ICDCSW*, pages 1–6.
- Bello, C. (2023). Euronews: Future of justice: Colombia makes history by hosting its first-ever court hearing in the metaverse. <https://www.euronews.com/next/2023/03/01/future-of-justice-colombia-makes-history-by-hosting-its-first-ever-court-hearing-in-the-me>. Accessed: 2023-09-07.
- Boletsis, C., Halvorsrud, R., Pickering, J. B., Phillips, S. C., and Surridge, M. (2021). Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment. In *Proc. of VISIGRAPP-IVAPP*, pages 266–274.
- Bösch, C., Erb, B., Kargl, F., Kopp, H., and Pfattheicher, S. (2016). Tales from the dark side: privacy dark strategies and privacy dark patterns. *Proc. Priv. Enhancing Technol.*, 2016(4):237–254.
- Bruun, A. and Stentoft, M. L. (2019). Lifelogging in the wild: Participant experiences of using lifelogging as a research tool. In *Proc. of INTERACT*, pages 431–451.
- Brysbaert, M. (2019). How many words do we read per minute? A review and meta-analysis of reading rate. *J. Mem. Lang.*, 109:104047.
- Cheng, R., Wu, N., Chen, S., and Han, B. (2022). Reality check of metaverse: A first look at commercial social virtual reality platforms. In *Proc. of IEEE VRW*, pages 141–148.
- Choi, H.-Y. (2022). Working in the metaverse: Does telework in a metaverse office have the potential to reduce population pressure in megacities? evidence from young adults in seoul, south korea. *Sustainability*, 14(6):3629.
- Di Pietro, R. and Cresci, S. (2021). Metaverse: security and privacy issues. In *Proc. of IEEE TPS-ISA*, pages 281–288.
- Dionisio, J. D. N., Iii, W. G. B., and Gilbert, R. (2013). 3d virtual worlds and the metaverse: Current status and future possibilities. *ACM Comput. Surv.*, 45(3):1–38.
- Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., et al. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *Int. J. Inf. Manag.*, 66:102542.
- Efroni, Z., Metzger, J., Mischau, L., and Schirmbeck, M. (2019). Privacy icons: A risk-based approach to visualisation of data processing. *Eur. Data Prot. L. Rev.*, 5:352.
- European Data Protection Board (2023). Guidelines 03/2022 on deceptive design patterns in social media platform interfaces. <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/>. Accessed: 2023-09-07.
- European Data Protection Supervisor (2022). Metaverse. https://edps.europa.eu/press-publications/publications/techsonar/metaverse_en. Accessed: 2023-09-07.
- Fernandez, C. B. and Hui, P. (2022). Life, the metaverse and everything: An overview of privacy, ethics, and governance in metaverse. In *Proc. of IEEE ICDCSW*, pages 272–277.

- Gray, C. M., Santos, C., and Bielova, N. (2023). Towards a preliminary ontology of dark patterns knowledge. In *Proc. of CHI EA*, pages 1–9.
- Gunawan, J., Santos, C., and Kamara, I. (2022). Redress for dark patterns privacy harms? A case study on consent interactions. In *Proc. of CSLAW*, pages 181–194.
- Halvorsrud, R., Boletsis, C., and Garcia-Ceja, E. (2021). Designing a modeling language for customer journeys: Lessons learned from user involvement. In *Proc. of ACM/IEEE MODELS*, pages 239–249.
- Halvorsrud, R., Haugstveit, I. M., and Pultier, A. (2016). Evaluation of a modelling language for customer journeys. In *Proc. of IEEE VL/HCC*, pages 40–48.
- Halvorsrud, R., Sanchez, O. R., Boletsis, C., and Skjuve, M. (2023). Involving users in the development of a modeling language for customer journeys. *Softw. Syst. Model.*, Online first. DOI: 10.1007/s10270-023-01081-w.
- Hedrick, E., Harper, M., Oliver, E., and Hatch, D. (2022). Teaching & learning in virtual reality: Metaverse classroom exploration. In *Proc. of IETC*, pages 1–5.
- Heurix, J., Zimmermann, P., Neubauer, T., and Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers & Security*, 53:1–17.
- Holtz, L.-E., Nocun, K., and Hansen, M. (2011). Towards displaying privacy information with icons. *IFIPAICT*, 352:338–348.
- Hwang, G.-J., Tu, Y.-F., and Chu, H.-C. (2023). Conceptions of the metaverse in higher education: A draw-a-picture analysis and surveys to investigate the perceptions of students with different motivation levels. *Comput. Educ.*, 203:104868.
- IFI Claims Patent Services (2022). Ifi insights: Inventing the metaverse. <https://www.ificlaims.com/news/view/briefing-metaverse.htm>. Accessed: 2023-09-07.
- Jones, T. (2010). Electronic Frontier Foundation: Facebook's "evil interfaces". <https://www EFF.org/deep links/2010/04/facebooks-evil-interfaces>. Accessed: 2023-09-07.
- Lee, J., Lee, T. S., Lee, S., Jang, J., Yoo, S., Choi, Y., Park, Y. R., et al. (2022). Development and application of a metaverse-based social skills training program for children with autism spectrum disorder to improve social interaction: Protocol for a randomized controlled trial. *JMIR Res. Protoc.*, 11(6):e35960.
- Massironi, M. et al. (2001). *The psychology of graphic images: Seeing, drawing, communicating*. Psychology Press.
- Murphy, H. (2022). Financial Times: Facebook patents reveal how it intends to cash in on metaverse. <https://www.ft.com/content/76d40aac-034e-4e0b-95eb-c5d34146f647>. Accessed: 2023-09-07.
- Ning, H., Wang, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., Ding, J., and Daneshmand, M. (2023). A survey on the metaverse: The state-of-the-art, technologies, applications, and challenges. *IEEE Internet Things J.*
- Roesner, F., Kohno, T., and Molnar, D. (2014). Security and privacy for augmented reality systems. *Commun. ACM*, 57(4):88–96.
- Sanchez, J. (2007). Second life: An interactive qualitative analysis. In *Proc. of SITE*, pages 1240–1243.
- Skorupska, K., Grzeszczuk, M., Jaskulska, A., Kornacka, M., Pochwatko, G., and Kopeć, W. (2022). A case for vr briefings: Comparing communication in daily audio and vr mission control in a simulated lunar mission. In *Proc. of MIDI*, pages 287–297.
- Stahl, J. D., Sead, N., Murrell, T., Germe, G. D. L., and Kish, S. (2020). Suggestion of content within augmented-reality environments. US Patent 10,719,989.
- Štarchoň, P. and Pikulík, T. (2019). GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices-mobile phones. *Procedia Comput. Sci.*, 151:303–312.
- Teller, E. (2023). Measurement method and system. US Patent 11,579,442.
- Voigt, P. and Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide, 1st Ed.* Springer.
- Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. *Curr. Opin. Psychol.*, 31:105–109.
- Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., and Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Commun. Surv. Tutor.*
- Warin, C. and Reinhardt, D. (2022). Vision: Usable privacy for xr in the era of the metaverse. In *Proc. of EuroUSEC*, pages 111–116.
- Weingarden, G. and Artzt, M. (2022). International association of privacy professionals: Metaverse and privacy. https://edps.europa.eu/press-publications/publications/techsonar/metaverse_en. Accessed: 2023-09-07.
- World Economic Forum (2023). Metaverse privacy and safety. <https://www.weforum.org/reports/privacy-and-safety-in-the-metaverse/>. Accessed: 2023-09-07.
- XR Safety Initiative (2020). The XRSI Privacy Framework. <https://xrsi.org/publication/the-xrsi-privacy-framework>. Accessed: 2023-09-07.
- Xu, M., Guo, Y., Hu, Q., Xiong, Z., Yu, D., and Cheng, X. (2023). A trustless architecture of blockchain-enabled metaverse. *High-Confid.*, 3(1):100088.
- Zolezzi, D., Vercelli, G. V., et al. (2023). Teaching in the Metaverse: Recreating an Italian Level A1 Course in Meta Horizon Workrooms. In *Proc. of The Future of Education*, pages 1–5.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.