Navigating the Ethical Minefield of the Metaverse: Exploring the Privacy, Safety and Security of the Virtual World

Author: Sil Durkstra
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands

ABSTRACT

The Metaverse is a young concept in development which must still receive vast amounts of attention and research for its final realisation, but it is expected that the Metaverse will grow massively in the near future. The ethical implications of its development are of vital importance, as to create such an interactive, immersive virtual world, there must be a solid ethical foundation on which its users can feel safe. The purpose of this thesis, is first to provide policymakers of the Metaverse with possible policies and regulations to help them develop a safe and secure environment. The most important ethical implications of the Metaverse related to privacy, security and safety are the main subject of the research. This thesis contains two main research sections: A literature review and an empirical research section. First, an introduction is provided for the reader to become more familiar with the concept of the Metaverse and its ethics, and the design of the chosen research is laid out. After the research sections, the findings and recommendations are explained, and conclusions are drawn to answer the research questions. The literature review has found that current policies and regulations are unfit or lack necessary nuance to cover the ethical challenges of the Metaverse's development. The empirical research has shown that these issues can be overcome with improvements or changes in three categories: user education, effective monitoring and moderation of malicious activity, and user control over profiling.

Keywords:
Metaverse
Ethics
Privacy
Safety
Security
Policies
Regulations

PREFACE

This thesis is written as the final assignment of the IBA bachelor study programme at the University of Twente, and I have worked on the project from March 2023 to July 2023.

When I first heard about what Facebook was doing with their virtual reality programme Meta, I was initially doubtful of its practicality and realism. I had seen such ideas portrayed in fiction before, and played with Virtual Reality technology (Oculus Rift), but never really thought of this Metaverse as a concept that could or would actually be realised. It did spark my interest however, as I was now intrigued by how Facebook and other developers of similar concepts would try to develop this fantasy into reality. Also, my interest in immersive digital platforms goes much further back to my history with gaming, having loved to play immersive open-world games of all kinds during much of my time as a teenager, while also losing many precious studying hours to them as a university student. When this research field was presented as one of the possibilities as a thesis focus, I knew I had an interesting, important and most of all, fun project to do.

Also, during my time as a student at this university, my interest in ethics have grown, because of certain ethics related subjects I had followed. Therefore, Metaverse Ethics quickly rose to the top of my priority list of thesis topic choices. There are so many engaging and intriguing subjects, like the ambiguity of ethics and whether they are subjective or objective, the conflicts between self-interest and the common good, the importance of perspective and ultimately the question of "what is ethical truth?".

ACKNOWLEDGEMENTS

I would like to express many thanks to my supervisor, Robin Effing, for his guidance and critical feedback throughout the writing of this thesis. Also, I want to thank the participants of the interviews for their contributions to this research, as I really could not have done this without them. I would also like to thank my thesis circle members, who helped me by giving and receiving peer feedback and providing meaningful discussions. I would like to exceptionally thank my family and my friends for their unending and unconditional love, support and encouragement.

With that being said, my hope for this thesis is that it can provide the research field with meaningful insights on the subject, and an interesting perspective to aid the development of any future Metaverse, and lastly, I would like to thank the reader for their time. I hope that they enjoy reading about the virtual world.

Sil Durkstra

Enschede, July 2023

CONTENTS

1. INTRODUCTION

In this introductory chapter, a general explanation of the Metaverse will be supplied. The first section will cover its origins, real life examples of its various iterations, a distinction between current Metaverse iterations and the future Metaverse, and lastly a problem statement. The second section will go over the goals and objectives of this thesis' research, and formulate the research question(s).

1.1 The Metaverse

The development of the future Metaverse has been rapidly accelerating in recent years due to advancements in virtual reality technology. The concept "Metaverse" refers to a virtual world created by the convergence of physical and virtual reality (O'Brien and Chan, 2021). It is an immersive environment where people can interact with each other, access entertainment, and or conduct business. The Metaverse is still a developing concept, and there are various interpretations of what it could entail. Some envision the Metaverse as a fully immersive, three-dimensional world, while others see it as a collection of interconnected virtual spaces that users can navigate between.

The idea of the Metaverse finds its roots in science fiction literature, specifically in Neal Stephenson's 1992 novel "Snow Crash." In the book, the Metaverse is a virtual reality shared by millions of users worldwide, where people interact with each other and with digital objects in a fully immersive and interactive environment (O'Brien and Chan, 2021).

1.1.1 The Metaverse in Recent History

Stephenson's vision of the Metaverse was highly influential in shaping the development of virtual worlds as well as online gaming in the later 1990s and early 2000s (Takahashi, 2022). In 1995, the video game licensor, Lucasfilm Games, known as LucasArts between 1990 and 2021 and with Lucasfilm as its parent company, released a video game called "Habitat," which was heavily inspired by the Metaverse described in "Snow Crash." Habitat allowed users to create avatars, explore a virtual world, and interact with each other in real-time. (Morningstar and Farmer, 1990) Other influential virtual worlds that contributed to the development of the Metaverse concept include massively multiplayer online games (MMO's), such as game developer and publisher Blizzard Entertainment's "World of Warcraft" (Eugen, 2022), or films like the Matrix (NewsBTC, 2022).

In 2018, another example of the growing interest in the development of the Metaverse and the influence of Metaverse-related literary works, was released in the form of a film named "Ready Player One", directed by Steven Spielberg and inspired by a novel written by Ernest Cline of the same name. The film portrays themes and issues which reflect on possible real issues in a future Metaverse, such as "the fluidity of personal identity, the conflict between reality and illusion, and power imbalances between individuals and corporations" (Sparknotes, n.d.).

Also in recent times, there have even been artists' performances held virtually within a metaverse-like space, such as concerts by massive current pop-music stars Travis Scott, Lil Nas X, Post Malone etc. (Havens, 2022, Tassi, 2020, Kastrenakes, 2020).

More recently, advances in virtual reality technology, such as the Oculus Rift and HTC Vive, have brought the concept of the Metaverse closer to reality.

Large corporations such as Facebook, Google, and Microsoft are investing heavily in the development of virtual reality platforms and technologies, with the goal of creating a fully immersive and interactive Metaverse that can be accessed globally by millions of people (Brown, 2021, Mileva, 2023).

1.1.2 Proto-Metaverse

There is an important distinction to be made between the current practical iterations of "Metaverses" and the future Metaverse idea. With today's virtual reality technology, current "Metaverses" can be accessed, by combining virtual reality platforms and fast networks (NewsBTC, 2022). The current virtual worlds that are starting to look like the future fully immersive and interactive Metaverse, are still a part of our Web2.0. Web2.0 refers to a paradigm of a set of technologies used in today's digital world. "The second generation of the web", an article by Wilson et al. (2011) calls it, which is "user-centred, promoting social connectedness and information sharing, user-created content and collaboration". The set of virtual worlds that are present in Web2.0 however, lack the critical aspects that are required to define them as Metaverses, such as decentralised control, for example (Clubrare, 2023).

To become a fully realised Metaverse, these current platforms would need all of the aspects that make the Metaverse unique to be present in their system. This would require an implementation of technology that would cost developers a serious investment, with company "Meta", one of Facebook's initiatives, having spent over $13.7 billion in 2022 alone to realise their Metaverse vision (Boland, 2023).

The current Metaverse-like platforms with interactive and immersive aspects, but lacking the unique aspects of the Metaverse, are therefore named "Proto-Metaverses". These are the present platforms run on our web2.0 with their "virtual identities, worlds avatars, inventories" etc. (NewsBTC, 2022).

1.1.3 Problem Statement

The development of the Metaverse has raised a number of ethical issues that must be addressed, because the failure to do so could result in pressing future problems.

One of the most pressing ethical concerns associated with the Metaverse is the issue of privacy. As users engage with the virtual world, they may share personal information that can be used for targeted advertising, profiling, or illegal activities. The immersive and interactive nature of the Metaverse makes it so that users may not have the same level of privacy as they do in the physical world.

This raises important questions about the ethical use of personal information in the Metaverse and the need for clear guidelines on data protection to ensure user privacy (Dwivedi et al., 2022).

Another issue, related to the problem of privacy, is that of security. The Metaverse is a highly connected virtual environment that relies on the Internet and other networks to function. This makes it vulnerable to cybersecurity threats such as hacking, malware, and distributed denial-of-service (DDoS) attacks. This raises important questions about the security of the Metaverse and the responsibility of developers and policymakers to ensure that the virtual world is safe and secure for all its users (Huang et al., 2021).

1.2 Research Objective

The goal of this research is to analyse the ethical implications of privacy, security and safety in the Metaverse, and their ethical implementation and development. The more specific objectives of this research are listed as follows:

-To analyse the data privacy challenges in the Metaverse and propose guidelines and improved practices for data privacy protection on the platform.

-To identify the security challenges of the Metaverse and propose guidelines and improved practices for ensuring security and safety.

The objectives this research will attempt to complete, will hopefully assist policymakers, developers, or other bodies of governance with their development and implementation of the future Metaverse with fitting safety measures, which could prove beneficial for improving the Metaverse's user friendliness and its long-term sustainability. It could also help users more clearly define ethical standards for the Metaverse, providing clarity about the challenges and implications of the Metaverse's privacy, security and safety.

1.2.1 Research Question(s)

The main question this research aims to answer is the core question. In addition, to divide the question into more manageable parts, this thesis also has three sub-questions. This paper's core research question is:

What are the main ethical implications of user privacy, safety and security for the Metaverse in Europe, and how can these implications best be addressed to ensure that policymakers can develop and implement a more safe and secure environment for its users?

To answer the core question, we can formulate the sub-questions to scale down its complexity, which will help guide the thesis to answer the question in smaller steps, and gather our data and come to a meaningful conclusion. What this thesis wants to know firstly, is what the current state of the ethical implications for the metaverse are, with the aspects of user privacy, security and safety being the focus. As such, our first sub-question can be formulated followingly:

What are the current general ethical policies and regulations implemented into existing Metaverse-like platforms?

This first sub-question will be answered in the literature review of this thesis. What is important to note is that ethics are ambiguous in nature. This means that ethical implications may or may not be sufficient or even desirable, depending on the perspective of the individual. One Metaverse user may be content with an ethical standard such as the sales and purchases of user data, while another may find this unacceptable. However, it can also be argued that there is an objective baseline for ethics, not only based on the preferences of a certain perspective. Both of these statements are related to objectivism and subjectivism of ethics (Park, 2022). What this thesis will aim to accomplish, is to lay out the objective facts of the current state of ethics regarding metaverse privacy, security and safety, and then deciding whether there is room for improvement or alternatives based on subjective user interviews.

Next, the second sub-question can be defined by asking what the existing ethical challenges are with the development of the Metaverse. This means to investigate what the strengths and weaknesses of current policies are. As such, the second question has been formulated:

What are the main ethical challenges with the development of the Metaverse?

To answer this question, the literature review will assess the challenges found in relevant academic research, and what the pitfalls of current ethical policies and regulations are. The first two sub-questions will form a base of reasoning for the conclusion of the literature review. This will then help flow into the thesis's empirical research, as it will be the base to which the potential room for improvement is related.

For the last sub-question then, the goal is to merge the first two steps together and assess room for improvement in policies and regulations for the future Metaverse. It is therefore formulated as follows:

How can policymakers improve off the current regulations of privacy, security and safety regarding the Metaverse?

These sub-questions are all meant to assist the answering of the core question. In the conclusion chapter of the literature review, the first two questions will be answered, and in the conclusion of the results chapter, the third question will be answered. In the chapter "Concluding Remarks", the core question is answered with the answers to the sub-questions.

2. LITERATURE REVIEW

The introductory chapter on the Metaverse and its ethics have focused on the origins and current state of the concept and its practicalities. This chapter will go further into articles, reports and other bodies of relevant scientific literature about the metaverse and its implications related to the research question(s) and objectives. This chapter will first focus on the general implications of the Metaverse according to literature, and will then expand upon the separate research aspects of this thesis: Privacy, security and safety. It will also cover already existing regulations and policies, and briefly mention the research gap.

There is a growing body of literature on Metaverse ethics, with academics and researchers examining the various ethical issues raised by the Metaverse. However, as the Metaverse is an idea that is still in its early, inspirational stage (Kole, 2023). It is therefore relatively new research territory as well.

2.1 Research Gap

While there has been a growing interest in the ethics of the Metaverse, there are still several research gaps that need to be addressed. One of the main research gaps is related to the development of ethical policies and regulations that are specific to the Metaverse, which this research will address. While existing frameworks can provide a starting point, which the literature review will cover, the unique characteristics of the Metaverse, such as its immersive and interactive nature, require new ethical considerations that cannot be fully addressed by existing frameworks.

Overall, the research gap highlights the need for further research on the ethics of the Metaverse. By addressing the gap, we can develop a more comprehensive understanding of the ethical considerations associated with the Metaverse and develop propositions to promote a safe and secure environment, for policymakers to develop.

2.2 General Implications

First of all, an important distinction to make between the current practical instances of a "Metaverse" and the idea and plan for the real finalised Metaverse, which was also discussed in the introductory chapter, under the section of Proto-Metaverses.

2.2.1 Definition and Perspectives

In a study by Park & Kim (2022), 260 articles related to the metaverse were studied, and the study analysed their perspectives on and definitions of the Metaverse. The definition that converged all perspectives and distinct definitions into one overarching core definition, which is mentioned in the research of Mystakidis (2022), is as follows:

"The Metaverse is the post-reality universe, a perpetual and persistent multi-user environment merging physical reality with digital virtuality. It is based on the convergence of technologies that enable multisensory interactions with virtual environments, digital objects and people."

So, according to this definition, the Metaverse fuses the sensory technologies together, meaning that the human senses can be fully immersed in a user's interaction with the Metaverse and its other users. Also, it states that the physical reality and digital virtuality are merged. This means that, instead of what we see today in virtual environments, where reality is either enhanced or augmented, the Metaverse fully brings the two together.

2.2.2 A Decentralised Metaverse

Regarding the governance of the Metaverse, the current digital platforms on the internet are governed very differently, depending on the country they operate in. The future Metaverse is also expected to follow this decentralised nature of governance (Goldberg & Schär, 2023). This decentralised structure does pose very significant challenges for the Metaverse's governance, because it will function and be governed without a central body of governmental power. This lack of central oversight and governance poses the question of how exactly privacy, security and safety will be ensured for the future Metaverse's users. While the governing body of the future Metaverse may not be centralised, and instead have a distributed network in control, the current EU-centralised regulations and policies may be adhered to or if necessary improved upon, in order to shape a working set of rules for the Metaverse's safety (Rosenberg, 2022).

2.3 Existing Regulations and Policies

This section will cover the already existing regulations and policies that are currently implemented in the EU related to privacy, security and safety of current Metaverse-like digital platforms. It aims to answer the first research sub-question:

What are the current general ethical policies and regulations implemented into existing Metaverse-like platforms?

2.3.1 Difference between Regulations and Policies

Although the two terms are often used interchangeably, there are distinct differences between the two terms. While it is true that both regulations and policies exist to direct those they apply to, they usually differ in their consequences of violation, as well as serving different purposes.

A policy is "a set of ideas or a plan for action followed by a business, a government, a political party, or a group of people."

A regulation is "an official rule or the act of controlling something." (Cambridge Dictionary, 2012).

Regulations are often in effect and imposed by governmental bodies to ensure the affected people follow implemented policies. Policies act as a guide, while regulations help enforce certain aspects of the guide that are necessary to be followed (Surbhi, 2021).

Now that the difference has been made clear, the following section will cover the current policies and regulations around privacy, security and safety of virtual platforms. There are several current regulations and policies relevant to consider for the eventual regulation of a future Metaverse. These come from the European Commission within the EU (European Commission, 2023).

2.3.2 Privacy Regulation

The most relevant legislation to mention here would be the General Data Protection Regulation (GDPR), which came into effect on May 25th, 2018 (*General Data Protection Regulation (GDPR) – Official Legal Text*, 2022). The GDPR has set up a system of rules related to the collection, processing, and storage of personal data. The goal of this regulation is to provide digital platform users with greater power over their personal data, and the act has established obligations for organizations handling data. Worth noting is that the GDPR's implementation of its principles have had significant impacts on the quality of data protection in the EU.

However, some problems with data protection have not yet been overcome, such as data brokers who stockpile personal data to sell it. While the regulations do give users more power over their data, it will take changes and time for the problems that remain to be hammered out (Burgess, 2022).

2.3.3 Cybersecurity

The EU cybersecurity act is a legislative framework (regulation) that was adopted by the European commission in 2019, to give the EU agency for network and information security (ENISA) a permanent mandate, providing it with stronger resources and new tasks. It may now help handle any cybersecurity incidents when requested and can support coordination of the EU "in case of large-scale cross-border cyberattacks an crises" (The EU Cybersecurity Act, 2023). By establishing a framework for cybersecurity certification, it aims to increase the EU's digital infrastructure's strength (ENISA, 2023). This act is part of the EU cybersecurity strategy, which has been developed by the union as a result of the digital transformation of society. This transformation has been greatly "intensified by the COVID-19 crisis" (European Commission, 2022), and has led to the emergence of new challenges for cybersecurity, which have required adaptations of solutions.

The cybersecurity act and the overarching strategy implemented by the European Commission aims mainly to protect internet users' fundamental rights. However, despite the efforts of these regulations and policies, there are still gaps in capabilities as well as coordination in terms of ensuring the resilience these regulations and policies try to ensure (ENISA, 2016).

2.3.4 User Protection

Previously, concerning privacy and security, the sections discussed protection of data and users from governing bodies or illegal activities. However, this section will cover the protection of users from other users, and how the EU promotes overall user safety. In the EU, there are various safety measures in place to protect users of digital platforms from each other These measures aim to address issues such as online harassment, hate speech, harmful content or other inappropriate behaviour.

An example of one such measure is the Digital Service Act (DSA), which is the most important and ambitious regulation in the world for the protection of users' fundamental rights (The Digital Services Act (DSA), n.d.). Following the DSA, digital platforms will have to be more transparent and accountable for "their role in disseminating illegal and harmful content"

This act's implementation has received mixed reactions from the media, as for example, The Washington Post (2022) stated that "the US could learn from these rules". Criticism the act received was largely related to its rigidity and lack of clarity (Keller, 2022).

2.4 Privacy, Security and Safety: Challenges

This section discusses the challenges the Metaverse will face in its regulation of privacy, security and safety, due to its decentralised and highly interactive nature. It will aim to answer the second research sub-question:

What are the main ethical challenges with the development of the Metaverse?

2.4.1 User Privacy Challenges

Privacy is a major concern in the Metaverse, as users are often required to share personal information in order to participate in virtual environments. In a study by Zimmeck et al. (2021), the privacy practices of current virtual reality platforms were examined and the research argued that stronger privacy protections are needed to protect user data in virtual environments. Users will participate in the Metaverse through the use of virtual avatars, and use special equipment for the immersive experience, such as virtual reality devices like headsets or sensory gear (Madiega et al., 2022).

One of the challenges the Metaverse's developers will face with the case of data protection, is that the decentralised governance structure of the Metaverse will make it very difficult to determine responsibilities and liabilities. The issue that is raised here is that it is unclear what entity handles user data protection. Moreover, the Metaverse's aspect of complete immersion will make users' capacities to avoid collection of personal data even more staggered, because of the multitude of access points with consent of services (Madiega et al., 2022, Zimmeck et al., 2021).

2.4.2 Security Challenges

The challenges of Metaverse security come forth in the forms of cybersecurity risks. This has been explored in a number of studies, including a study by Huang, Li and Cai (2021), which examined the security challenges of virtual reality technologies and argued that greater attention needs to be paid to securing virtual environments against cyber threats. Because such great volumes of data will be circulating in the Metaverse, current challenges of cybersecurity will persist in the Metaverse and may likely be even more of a problem. Hacks, malware, and phishes are all examples of these challenges which will likely be particularly concerning (Shi et al., 2021).

For example, because of the Metaverse enabling devices, like the virtual reality headset, sensitive user data is needed for proper device functionality, such as voice and movement. Hacking becomes a more pressing issue here, because hacking into such a device could grant control over what the user and now victim can see and hear. (Madiega et al., 2022)

2.4.3 Social Safety Challenges

Regarding overall user safety of the Metaverse, the future is facing difficult challenges to overcome. Already, according to reports about metaverse safety written by the Centre for Countering Digital Hate (CCDH) (2021), current digital platforms struggle with harassment, racism and sexually explicit material. This ongoing issue will likely increase in severity in a future Metaverse, as it will be more interactive and immersive for its users, and therefore, not only the problems themselves will increase, but also the severity of them (Ramamoorthy, 2022).

2.5 Evaluation

Overall, the Metaverse is complex, it is young, uncertain, and even its definition depends on perspective. There are many challenges the development of the Metaverse will face, and there are some current frameworks, regulations and guidelines which can help policymakers and developers steer the Metaverse's playing rules in the right direction. However, it is clear that these policies and regulations will need to be improved or altered in order for them to cover the Metaverse's unique aspects of its interconnectivity, immersion and hyper-interactivity.

As mentioned, the privacy of the users of the Metaverse is at risk, due to extra-sensitive relevant user information, and the uncertain enforcement of privacy regulations such as the GDPR. The cybersecurity of the Metaverse faces challenges with its vast amounts of data circulation, and the uncertainty of its security against the malicious actors that the system contains, who are proficient in data breaching. The overall user safety from other users is also a difficult challenge to be overcome, as current actors that increase user safety, such as ENISA in the EU, will likely not have the same operational power in the decentralised Metaverse. Moreover, the issues of harmful interactions and content that users already face on a large scale on today's Proto-Metaverse platforms, will only likely become more pressing.

This chapter aimed to answer the research sub-questions:

What are the current general ethical policies and regulations implemented into existing Metaverse-like platforms?

And

What are the main ethical challenges with the development of the Metaverse?

What can be concluded from this literature review, is that there are policies and regulations in place to facilitate the development of a Metaverse with sufficient privacy, security and safety, but that these policies and regulations are either not fitting enough for the unique properties of the Metaverse, or that the current enforcement of them will not work in a decentralised Metaverse.

Also, the challenges that the development of the Metaverse will face, are quite difficult to overcome without proper guidelines and policies, as failure to implement these policies and regulations will likely result in a Metaverse riddled with security fallacies, concerns of privacy breaches and unsafe user's feelings about the interactive environment.

3. RESEARCH APPROACH

This research into the Metaverse means to come to understand the ethical implications and the risks of current ethical practicalities of the Metaverse. It assesses the current policies and regulations around privacy, security and safety, and decides, based on empirical research data, whether these policies and regulations are sufficient. If not, the research will propose improvements, based on the differences.

The relevant concepts of the research question can be defined as follows. Firstly, Privacy The concept of control of personal information of users and limiting its access to others in the Metaverse. The variable of the research will be how much and how well data is kept private. Secondly, security covers the measures taken to protect users' personal information from unauthorized access, use, and disclosure in the Metaverse.

The variability will concern how secure and strict these measures are and will be. Lastly, safety concerns the overall safety and insurance of user wellbeing. Its variability will be how protected users of the future Metaverse will be from other users.

Privacy and security are closely related in the sense that they both deal with protecting sensitive information from unauthorized access, use, and disclosure. Privacy refers to the ability of individuals to control the collection, use, and dissemination of their personal information. Safety is related to privacy and security, being an overarching concept for both variables, but also having its own implications, such as user health.

In other words, privacy concerns limiting access to personal information, while security is about ensuring that the access that is granted is only to authorized individuals and is done in a secure manner, and safety is the insurance of privacy, security and overall wellbeing of users.

3.1 Research Design

To answer the core question and its sub-questions, proper research methods must be used to come to an effective conclusion. Because each sub-question aims to answer different aspects of the core question (current practice; challenges; future improvement), the right methods of data collection must be applied to the corresponding research sections.

This research will be designed as follows: First, a comprehensive literature review of existing research on privacy, security, and safety in virtual worlds, online gaming, and other digital environments. This literature review will cover the first two sub-questions. The data gathered from the literature review will be quantitative: measured current policies and regulation, as well as measured challenges. This will provide a foundation of knowledge for the empirical research.

Second, the supplementary empirical research approach of this thesis will be qualitative in nature. Qualitative research will allow us to understand the variables and their implications within a real-world context through observation.

Purposive sampling will be appropriate for this research. This will ensure that participants have relevant knowledge. The sample size can be kept relatively small, because of the smaller scope of this research, as well as its feasibility.

The research will measure whether there is room for improvement from the current ethical implications for the Metaverse, which will be researched with the literature review.

To collect data for the qualitative research, interviews will be conducted with the sample group of users to explore their experiences and perspectives on the future related to the ethical implications of privacy, security, and safety in the Metaverse.

A practical limitation of this method could be the required anonymity of interviewees, but it is not realistically expected to be a problem, because personal data and direct transcripts can be kept anonymous, while collected research data will not.

To analyse the data, thematic analysis can be applied to identify key themes and patterns from the interviews, and review the themes of said emerging patterns. With these themes, the research can propose fitting solutions or improvements for the future.

3.2 Interviews

Regarding the chosen method of data collection for the empirical research, multiple aspects of the interviews must be determined and planned for effective research.

3.2.1 Profiles

The question that this empirical research aims to answer, is based off current user experience, compared to current policies and regulations, to find the difference between them and propose improvements for future policymakers. The literature review will cover the current policies and regulations, so the empirical research will collect data on user experience. Therefore, our interviewee profile will be categorised as current Proto-Metaverse users in the EU, who have experience with using and spending time on these platforms.

Respondent	Preliminary Metaverse familiarity	Average past Proto-Metaverse platforms use	Current Proto-Metaverse platform use
1	Medium-High	Moderate	Moderate
2	High	Frequent	Moderate
3	Low	Moderate	Occasional
4	Medium	Occasional	Occasional
5	Medium-High	Occasional	Moderate

Table 1: Overview of interview respondents' profiles

3.2.2 Structure

For the interviews, there are two possible structure to be used: structured or semi-structured. The structure for this thesis' interviews will be semi-structured, because it allows for more varied input of data, in case the users/interviewees wish to add any data about details that may have not been discussed otherwise. It will also allow for a more flowing interview structure, letting the interview branch off to potentially relevant topics not present in the interview questions.

3.2.3 Analysis

The analysis of the interview data will be qualitative in nature. It will focus on the content of the answers to the questions, as well as the discussion that will be held about the questions and their answers.

The inference of the qualitative analysis will be thematic, meaning that from the data and their analysis, thematic patterns of ideas and perspectives will be highlighted. To achieve an analysis of sufficient quality, continuous reflection of the developing analysis is required from the researcher (Villegas, 2023).

4. FINDINGS AND DATA ANALYSIS

Now that the literature review has established a baseline of the current state of Proto-Metaverse safety and laid out the challenges the development of the future Metaverse will likely face, the possible improvements / ideas can be discussed. The following chapter will analyse the interview data, and based on thematic analysis of the data, possible solutions in the forms of regulations or policies will be proposed. Current Proto-Metaverse users will be the participants of the interviews and be the main source of the qualitative data, as discussed in the previous section, 2.3.

To reiterate, the research sub-question this section aims to answer is the following:

How can policymakers improve off the current regulations of privacy, security and safety regarding the Metaverse?

The empirical research will try to answer this question with a set of data collected from the semi-structured interviews. The answer to this question will be given in the form of proposed solutions and or improvements in the form of potential policies or regulations.

4.1 Interview Analysis

This data analysis will compile and assess the qualitative interview data. The thematic analysis will look at patterns in the interviewee's answers and the discussions that were held about their user experiences and their ideas for solutions and or improvements. The interviews were held one-on-one online, and all interviewees were provided with an intermediate summary of this thesis for context to familiarise them with the subject, the research purpose and what the research wants from them data-wise.

4.1.1 Qualitative Data-Analysis

The interviews provided meaningful answers to the questions and interesting and insightful discussions about the problems of privacy, security and safety in current Proto-Metaverses. The selected sample group had variety in backgrounds and experiences, yet there were clear patterns emerging from all their different perspectives. To read the interview questions, please refer to Appendix A, and for a summary of the interviews, please refer to appendix B. All data represented here for analysis are referenced from the Appendices.

First of all, the familiarisation of the data has been achieved by summarising the transcripts of the interviews. This helps to gain a thorough overview of the collection of data. Secondly, the data is coded: certain parts of the text are highlighted and "coded" by assigning the highlighted phrases or words with particular descriptive codes. Then, the research can look at the codes and identifies patterns among the codes. The patterns will then be translated into themes.

4.1.2 Themes and Patterns

This section will cover the analysis of the observed themes in the data, with the main patterns being described.

The first theme that can be recognised from the patterns, is related to the interviewees' mentions of their knowledge on the Metaverse. All participants had at least some known definition of its concept, and or have had experience with using current Proto-Metaverse platforms. This means that all participants have a sufficient extent of meaningful data to provide for the analysis. While there was variance in the amount of knowledge and the forms of knowledge on the concept and its implications, all participants shared a meaningful level of experience.

Secondly, all participants have shown that they make use of more than one Proto-Metaverse platform, with most platforms used being social in nature, such as interactive social media. Also, platforms such as games were frequently mentioned to be used by participants. This gave the data a larger variety across platforms, with answers and discussions coming from multiple different perspectives, due to the platforms they were based on.

Related to the third interview question, most participants have shown that they currently use Proto-Metaverse platforms at least occasionally per week, and at most very frequently. Additionally, their past use of the platforms per year has shown to be aligned with their current weekly uses, also averaging moderate usage. The research can classify all participants as current users of Proto-Metaverse platforms, meaning that the data they provided was up to date, as well as most their data spanning over a large amount of time.

For the last section of the interview, which was meant to provide the data to actually answer the research sub-question, there was a pattern among all participants of cybersecurity related issues. They largely had problems with scams, giving up private information and unwanted online profiling. The cause for most problems was the ignorance that the participants had towards their own cybersecurity. Some of the other issues also stem from the profiling algorithms present in modern monetised digital platforms.

The last question of the interview gathered data about the participants' own ideas for solutions to their issues and improvements for the future Metaverse. Most of the answers and discussions went towards the solution of user education programmes. This solution came up often because one of the causes for their personal problems was their lack of knowledge about self defence in an online environment. The root cause of the mentioned problems is mainly malicious actors like hackers, scammers etc., and for this cause, solutions were proposed and discussed to help prevent these malicious actors from causing harm. Also, the effect of digital profiling was an emerging pattern, with ideas for solutions involving increased control over an individual's profiling, such as their cookies used by online businesses, as well as their profiling shown to other users.

4.2 Proposed Solutions

This section covers the ideas that originated from the interview themes, and the proposed solutions are nuanced and elaborated on. Since the main themes of the last interview section came down to user education, prevention of repeated malicious actions, and increased profile control, there will be three specific proposed policies to improve future situations. Any sentences or phrases in quotation marks in the following paragraphs are direct quotes or parts of direct quotes from the interviews.

4.2.1 Education and Awareness

First of all, related to the user education solution, the idea that is proposed is that of a mandatory user education programme as part of the terms and conditions of Metaverse usage. This programme "would act as a sort of tutorial at the start of any individual's use of the Metaverse". Its goal would be to "familiarise users with the Metaverse", to teach them "how to be safe and responsible with their online presence and address the risks and potential dangers of the immersive and interactive world. The programme could test and "assess the user's preliminary knowledge on the self defence of cybersecurity" to gauge the existing awareness of the user. This would adjust the programme to the user's needs.

The programme should contain at least the following aspects: first, an introduction to the Metaverse. Then, teach the user how to navigate the virtual environment, covering aspects like virtual presence, avatars, and property. Also, the users need to be taught about protecting personal information and being aware of their cybersecurity. A continuous support system should also be implemented, to have an ongoing input source for users' questions or concerns once they complete the programme.

4.2.2 Prevention of Repeated Malicious Actions

To prevent Malicious actors from being able to repeat their harmful practices, a policy could be introduced which involves the implementation of a technical system to increase security and safety. Measures taken could include, for example, strong "identification measures like multifactor authentication", or, with the cutting edge technology at hand, a biometrics scanning system, much alike to "fingerprint / face scanning access systems on mobile devices". Additionally, the system could make use of "data analytics and pattern recognition to identify and track patterns of malicious activity". Common red flags that suggest suspicious actions could be analysed, with the consequences being determined by moderators from the platform. Lastly, the system could make use of moderation and reporting practices by designating a team of moderators to handle user reports to take action against perpetrators of online incidents.

4.2.3 Profile Control

To provide users with more control over their data and online profiling, a policy could be developed to implement more granular control settings for over their private information and allowed profiling. It would be helpful to "allow users to specifically choose what data they are willing to share and with whom they share it". Examples of this include chosen profile visibility or chosen contact settings (who can contact them and who cannot).

What users would also need, is for the Metaverse's privacy "policies to be crystal clear, with well-defined boundaries of user data collection", storage and usage on the platform. It would be important to make the purpose of the privacy policy clear to users too, and state the rights that users have over their privacy.

Another important aspect of this solution is to "establish clear transparency of data management", giving users the opportunity to review their collected data, and allowing them to alter their preferences at any time.

To further increase the privacy control users will have, the policy could allow the anonymisation of data. This would let users de-identify their data to protect their privacy, while still allowing useful, beneficial profiling.

4.3 Evaluation

To conclude the findings and recommendations, this chapter qualitatively analysed the data gathered from the interview research. This was done by coding the raw data and formulating recurring themes from the codes. From the themes, a conclusion could be drawn about how to best improve the future Metaverse's privacy, security and safety compared to the current situation of Proto-Metaverse platforms.

The profiles of the interview participants were taken into account, with the purpose of the first interview section being ensuring that participants had sufficient knowledge about and experience with the subject.

The three most present themes were transformed into solutions based on policies and regulations. The purpose of these solutions were the improvement of user education and awareness, the prevention of repeated malicious actors, and the increased control users have over their profiling.

To answer the last research sub-question, policymakers of the Metaverse should consider that the three themes mentioned in this analysis are critical to be solved and improved upon by developing the given fitting policies and regulations.

5. DISCUSSION

This final chapter will summarise this thesis's core findings, and it will answer the core research question by answering the sub-questions formulated in the research question(s) section. After answering the research questions, recommendations for future research will be discussed, as well as the relevance and contribution of this thesis.

5.1 Research Questions

To review all the research questions, they will first be reiterated, then answered, with a build-up to the core question.

5.1.1 First Sub-Question

What are the current general ethical policies and regulations implemented into existing Metaverse-like platforms? With this research question, the thesis covered the present situation of governance of privacy, security and safety on Proto-Metaverse platforms. This questions would be answered with the use of a literature review. In the literature review, the research found that current policies and regulations are present to govern the rules of Proto-Metaverses, specifying three specifically applicable examples: the GDPR, the EU cybersecurity act, and the DSA. Each of these concerns privacy, security and safety respectively.

5.1.2 Second Sub-Question

What are the main ethical challenges with the development of the Metaverse? The purpose of this research question was to present the most pressing challenges that the development of the Metaverse would face. It was important to investigate the current challenges to determine whether there is room for improvement on current policies and regulations, and this would lead into the third research sub-question. This question would also be answered by the literature review. The main ethical challenges that the development of the Metaverse would face related to privacy, security and safety involve the difficulty to protect user data, the difficulty to implement effective measures to protect the user data, and the difficulty to monitor and moderate social safety. User privacy is challenged by the hyper interactive and decentralised nature of the Metaverse's environment, which will make it difficult for policies and regulations to be consistently implemented and governed. Also, the immersion and multitude of user access points will make the prevention of unwanted data collection difficult for policies to ensure.

5.1.3 Third Sub-Question

How can policymakers improve off the current regulations of privacy, security and safety regarding the Metaverse? This final sub-question aimed to compare the current ethical governance situation (current policies/regulations and challenges) to the desired future situation, and propose improvements based on the differences. The empirical research answered this sub-question by conducting interviews with experienced Proto-Metaverse users to gain insight into the desired future user experience. The specific areas that were found to require improvement and extra attention with development of the Metaverse, were user education and awareness, prevention of repeated malicious activity, and increased user control over profiling.

Possible practical policies or regulations that were proposed included mandatory starting user education programmes; security measures that authenticate users based on biometrics or multiple steps; programmes that recognise patterns in suspicious behaviour and report them to moderators; and policies that give users increased control over what personal data is shared with whom.

5.1.4 Core Research Question

What are the main ethical implications of user privacy, safety and security for the Metaverse in Europe, and how can these implications best be addressed to ensure that policymakers can develop and implement a more safe and secure environment for its users? Now that the sub-questions have been answered, the core question's answer can be comprised of the accumulation of answers to the sub-questions.

What the literature review found, is that the main ethical implications concern the protection and management of user data, the handling of cybersecurity and its challenges, and the overall safety of user's wellbeing in the Metaverse. These implications had policies and regulations implemented to support their goals, but were found to be in need of improvement or change, after the assessment of the reviewed challenges. The interview data then provided the necessary improvements and changes to successfully develop a safe Metaverse in the forms of user education, prevention of malicious action and user's profile control.

5.2 Future Research

This thesis can hopefully create a more stable base on which future research into this field can be carried out. Also, based on the conclusion of this thesis, policymakers and other researchers could consider the proposed policies and regulations. For a better understanding of the implications the results of this thesis carry, future research could attempt to discover more possible solutions and or improvements for a more safe Metaverse with this research as part of its literature review.

5.3 Relevance

As the Metaverse is still a young idea, being in its early stages of development, research into the opportunities and pitfalls of its practicalities are vital to a successful, sustainable, safe, and secure implementation. Some of the specific practical implications which are relevant to this thesis are as follows.

Feasibility of the implementation of a Metaverse: This research could aid the planning for development guidelines for the Metaverse. This could help the development process of the Metaverse, increasing the Metaverse's odds of actually becoming to exist in the modern world.

Protecting privacy: By researching Metaverse ethics, policymakers can develop the best practices for data privacy and security, which can protect users' personal information and overall safety. This could increase the probability of a sustainable user base.

Ensuring security: since the Metaverse is a complex and evolving space with its unique set of security challenges. As the Metaverse expands, security risks will also increase. By researching Metaverse ethics, developers can identify potential security vulnerabilities and develop measures to mitigate them.

Developing a safe environment: by researching the Metaverse's challenges, we can identify areas for improvement, and provide guidelines for the development and implementation of a safer environment for its users.

REFERENCES

5 Qualitative Data Analysis Methods to Reveal User Insights. (2023, March 30). https://www.hotjar.com/qualitative-data-analysis/methods/

Basumallick, C. (2022, October 10). What Is the Metaverse? Meaning, Features, and Importance. Spiceworks. https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-metaverse/

Boland, M. (2023). Meta Spends $13.7 Billion in 2022 to Build the Metaverse. Localogy. https://www.localogy.com/2023/02/meta-spends-13-7-billion-in-2022-to-build-the-metaverse/

Brown, D. (2021, October 28). What is the 'metaverse'? Facebook says it's the future of the Internet. Washington Post. https://www.washingtonpost.com/technology/2021/08/30/what-is-the-metaverse/

Burgess, M. (2022, May 23). How GDPR Is Failing. WIRED UK. https://www.wired.co.uk/article/gdpr-2022

Clubrare. (2023, March 21). Understanding the Metaverse: Comparing Web2 and Web3 Platforms. Medium. https://medium.com/clubrare-universe/understanding-the-metaverse-comparing-web2-and-web3-platforms-46828218f386

Crossley, J. (2021). The Dissertation Results/Findings Chapter (Qualitative). Grad Coach. https://gradcoach.com/qualitative-results-findings/

Digital privacy. (2022, June 7). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/digital-privacy

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B. A., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D., Gustafsson, A., Hinsch, C., Jebabli, I., . . . Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 66. https://doi.org/10.1016/j.ijinfomgt.2022.102542

ENISA. (2023, June 12). ENISA. https://www.enisa.europa.eu/

Eugen, F. (2022). Conquering the Metaverse: How Blizzard's World of Warcraft Can Show Businesses the Way. www.linkedin.com. https://www.linkedin.com/pulse/conquering-metaverse-how-blizzards-world-warcraft-can-eugen-faraj?trk=pulse-article_more-articles_related-content-card

General Data Protection Regulation (GDPR) – Official Legal Text. (2022, September 27). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

George, T. (2022a). What is a Dissertation Preface? | Definition & Examples. Scribbr. https://www.scribbr.com/dissertation/dissertation-preface-example/

George, T. (2022b). How to Write a Thesis or Dissertation Conclusion. Scribbr. https://www.scribbr.com/dissertation/write-conclusion/

Goldberg, M., & Schär, F. (2023). Metaverse governance: An empirical analysis of voting within Decentralized Autonomous Organizations. Journal of Business Research, 160, 113764. https://doi.org/10.1016/j.jbusres.2023.113764

Havens, L. (2022, June 7). Post Malone to Perform 'Twelve Carat Toothache' in a Virtual Reality Concert Hosted by Meta: Exclusive. Billboard. https://www.billboard.com/music/music-news/post-malone-twelve-carat-toothache-concert-virtual-reality-1235110887/

Huang, Y., Li, Y. J., & Cai, Z. (2023). Security and Privacy in Metaverse: A Comprehensive Survey. Big Data Mining and Analytics, 6(2), 234–247. https://doi.org/10.26599/bdma.2022.9020047

Kastrenakes, J. (2020, November 16). Lil Nas X's Roblox concert was attended 33 million times. The Verge. https://www.theverge.com/2020/11/16/21570454/lil-nas-x-roblox-concert-33-million-views

Keller, D. (2022, February 24) The DSA's Industrial Model for Content Moderation. Verfassungsblog https://verfassungsblog.de/dsa-industrial-model/

Kole, S. (2023). Metaverse Development: Building the Future of Virtual Reality. Data Science Central. https://www.datasciencecentral.com/metaverse-development-building-the-future-of-virtual-reality/

Lee, L., Braud, T., Zhou, P., & Hui, P. (2021). All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem,. . . ResearchGate. https://doi.org/10.13140/RG.2.2.11200.05124/8

Literature review. (2022, August 29). The University of Edinburgh. https://www.ed.ac.uk/institute-academic-development/study-hub/learning-resources/literature-review

Liverpool Hope University. (2021, November 4). Who is Going to Police the "Metaverse"?

https://www.hope.ac.uk/news/allnews/who-is-going-to-police-the-metaverse.html

MATT O'BRIEN AND KELVIN CHAN. (2021, OCTOBER 28). EXPLAINER: WHAT IS THE METAVERSE AND HOW WILL IT WORK? ABC NEWS. https://web.archive.org/web/20211204012219/https://abcnews.go.com/Business/wireStory/explainer-metaverse-work-80842516

MILEVA, G. (2023). 52 METAVERSE STATISTICS | MARKET SIZE & GROWTH (2023). INFLUENCER MARKETING HUB. https://influencermarketinghub.com/metaverse-stats/#toc-3

MORNINGSTAR, C., & RANDALL FARMER, F. (1991). THE LESSONS OF LUCASFILM'S HABITAT. http://www.fudco.com/chip/lessons.html

MORTENSEN, D. H. (2023, JUNE 12). HOW TO DO A THEMATIC ANALYSIS OF USER INTERVIEWS. THE INTERACTION DESIGN FOUNDATION. https://www.interaction-design.org/literature/article/how-to-do-a-thematic-analysis-of-user-interviews

NEWSBTC. (2022, NOVEMBER 21). HOW TODAY'S PROTO-METAVERSE WILL EVOLVE TO BECOME AN INTERCONNECTED VIRTUAL WORLD. NEWSBTC. https://www.newsbtc.com/news/company/how-todays-proto-metaverse-will-evolve-to-become-an-interconnected-virtual-world

NIELSEN. (2022, APRIL). NIELSEN'S STATE OF PLAY REPORT REVEALS THAT STREAMING IS THE FUTURE, BUT CONSUMERS ARE CURRENTLY OVERWHELMED BY CHOICE | NIELSEN. https://www.nielsen.com/news-center/2022/nielsens-state-of-play-report-reveals-that-streaming-is-the-future-but-consumers-are-currently-overwhelmed-by-choice/

PARK, S. (2022). MORAL SUBJECTIVISM VS MORAL OBJECTIVISM. FILOSOFIJA-SOCIOLOGIJA, 33(3). https://doi.org/10.6001/fil-soc.v33i3.4775

PARK, S. M., & KIM, Y. (2022). A METAVERSE: TAXONOMY, COMPONENTS, APPLICATIONS, AND OPEN CHALLENGES. IEEE ACCESS, 10, 4209–4251. https://doi.org/10.1109/access.2021.3140175

POLICY. (2023). https://dictionary.cambridge.org/dictionary/english/policy

PROBING REALITY AND MYTH IN THE METAVERSE. (2022, JUNE 13). MCKINSEY & COMPANY. https://www.mckinsey.com/industries/retail/our-insights/probing-reality-and-myth-in-the-metaverse'

RAMAMOORTHY, R. (2022, SEPTEMBER 26). WHY THE METAVERSE IS FILLED WITH SECURITY, PRIVACY AND SAFETY ISSUES. VENTUREBEAT. https://venturebeat.com/security/why-the-metaverse-is-filled-with-security-privacy-and-safety-issues/

RAVENSCRAFT, E. (2022, APRIL 25). WHAT IS THE METAVERSE, EXACTLY? WIRED. https://www.wired.com/story/what-is-the-metaverse/

READY PLAYER ONE: THEMES | SPARKNOTES. (N.D.). SPARKNOTES. https://www.sparknotes.com/lit/ready-player-one/themes/

RESEARCH GUIDES: ORGANIZING YOUR SOCIAL SCIENCES RESEARCH PAPER: APPENDICES. (2023, MAY 30). LIBGUIDES.USC. https://libguides.usc.edu/writingguide/appendices

ROSENBERG, L. B. (2022). REGULATION OF THE METAVERSE: A ROADMAP: THE RISKS AND REGULATORY SOLUTIONS FOR LARGESCALE CONSUMER PLATFORMS. https://doi.org/10.1145/3546607.3546611

S, S. (2021, JANUARY 21). DIFFERENCE BETWEEN RULES AND POLICIES. KEY DIFFERENCES. https://keydifferences.com/difference-between-rules-and-policies.html

SHI, C., XU, X., ZHANG, T., WALKER, P., WU, Y., LIU, J., SAXENA, N., CHEN, Y., & YU, J. (2021). FACE-MIC: INFERRING LIVE SPEECH AND SPEAKER IDENTITY VIA SUBTLE FACIAL DYNAMICS CAPTURED BY AR/VR MOTION SENSORS. https://doi.org/10.1145/3447993.3483272

STRANGE, A. (2022, AUGUST 15). PEOPLE EXPECT TO SPEND AT LEAST 4 HOURS A DAY IN THE METAVERSE. QUARTZ. https://qz.com/people-expect-to-spend-at-least-4-hours-a-day-in-the-me-1849406012

TAKAHASHI, D. (2022, JULY 8). CHIP MORNINGSTAR INTERVIEW: HOW THE METAVERSE STARTED WITH HABITAT. VENTUREBEAT. https://venturebeat.com/games/chip-morningstar-interview-how-the-metaverse-started-with-habitat/

TASSI, P. (2020, APRIL 23). FORTNITE'S TRAVIS SCOTT CONCERT WAS A STUNNING SPECTACLE AND A GLIMPSE AT THE METAVERSE. FORBES. https://www.forbes.com/sites/paultassi/2020/04/23/fortnites-travis-scott-concert-was-a-stunning-spectacle-and-a-glimpse-at-the-metaverse/?sh=564bc3cd2e1f

THE DIGITAL SERVICES ACT (DSA). (N.D.). https://www.eu-digital-services-act.com/

THE EU CYBERSECURITY ACT. (2023, MAY 25). SHAPING EUROPE'S DIGITAL FUTURE. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

VILLEGAS, F. (2023). THEMATIC ANALYSIS: WHAT IT IS AND HOW TO DO IT. QUESTIONPRO. https://www.questionpro.com/blog/thematic-analysis/

Wang, Y., Su, Z., Zhang, N., Liu, D., Xing, R., Luan, T. H., & Shen, X. (2022). A Survey on Metaverse: Fundamentals, Security, and Privacy. https://doi.org/10.36227/techrxiv.19255058.v1

Wilson, D. W., Lin, X., Longstreet, P., & Sarker, S. (2011). Web 2.0: A Definition, Literature Review, and Directions for Future Research. ResearchGate. https://www.researchgate.net/publication/220892879_Web_20_A_Definition_Literature_Review_and_Directions_for_Future_Research

Zallio, M., & Clarkson, P. J. (2022). Designing the metaverse: A study on inclusion, diversity, equity, accessibility and safety for digital immersive environments. Telematics and Informatics, 75, 101909. https://doi.org/10.1016/j.tele.2022.101909

Zimmeck, S., Goldstein, R., & Baraka, D. (2021, February). PrivacyFlash Pro: Automating Privacy Policy Generation for Mobile Apps - NDSS Symposium. NDSS Symposium. https://www.ndss-symposium.org/ndss-paper/privacyflash-pro-automating-privacy-policy-generation-for-mobile-apps/

APPENDICES

A. Interview Questions

The interview questions of this research are divided into two sections: a general profiling section to gain insight into the interviewees' profiles, and an in depth, detailed section, with the purpose of gathering the relevant information about the interviewees' experiences with current policies and regulations, and their expectations/ insights into future improvements with the development of the Metaverse.

Also, if an interviewee is previously unfamiliar with some of the relevant concepts, they will be introduced to them and provided with a brief but useful explanation.

The first general section of interview questions is as follows:

Q.1. How familiar are you with the term "Metaverse"? Please try to explain your perspective on what it is.

Q.2. Are there any current Proto-Metaverse platforms you have been active on in the past or are active on currently? Please list them (and explain if the interviewer is not familiar with any of the platforms)

Additional explanation: A Proto-Metaverse platform can be categorised by sufficiently containing one or more of the Metaverse's defining aspects present in today's version of Metaverse-like platforms: Complete immersion, high interactivity and interoperability or persistency of its existence.

Q.3.1. How much time/year have you spent on the platforms you have been active on?

Q.3.2. How much time do you spend on average per week on platforms you are active on?

For the third question, the interview will try to categorise the interviewee into one of four groups:

- frequent user: 1000+ hours/year and/ or >30 hours per week;
- moderate user: 600-1000 hours/year and/ or 20-30 hours per week;
- occasional user: 200-600 hours/year and/ or 10-20 hours per week;
- rare user: 0-200 hour/year and/ or <10 hours per week

The amount of hours that make up the three categories are based studies from McKinsey (2022) and Nielsen (2022), which found that average consumer time spent on Metaverse-like platforms, and the expected time spent in the future developed Metaverse, would equal around 4 hours per day.

From this point forward, the interviewees are grouped into three different categories: frequent users, moderate users, and occasional users.

The second section of the interview questions covers the interviewees' experiences with privacy, security and safety implications in the Metaverse-like platforms they use, and their ideas about important issues related to those implications that they would want to see resolved in the future Metaverse.

Q.4. What privacy, cybersecurity and general user safety issues do you currently experience on the platforms you use? What issues have you experienced in the past?

Q.5. Based on your personal experiences, what policies or regulations would you want to see to improve your future situations or resolve current problems you have on the used platforms?

Q.6. Do you have any other questions or remarks about the questions or the research?

The information gathered from the answers to these questions, as well as from the discussions that the interviewer and interviewee will engage in about the questions and their answer, should provide the data necessary to answer the last research sub-question, and therewith also answer the core question.

Again, these are the questions that are asked in the interviews, and the answers and discussions will be analysed thematically.

B. Respondent Profiles

Respondent	Preliminary Metaverse familiarity	Average past Proto-Metaverse platforms use	Current Proto-Metaverse platform use
1	Medium-High	Moderate	Moderate
2	High	Frequent	Moderate
3	Low	Moderate	Occasional
4	Medium	Occasional	Occasional
5	Medium-High	Occasional	Moderate

C. Summaries of the Interviews

The transcripts of the interviews are not to be made public, but a summary of the answers and discussions is provided here to supply the information used to conduct research and draw conclusions from the data.

Interview 1

Interviewee 1's understanding of the Metaverse is that the Metaverse is a virtual environment, in which people can interact seamlessly with the virtual environment and each other, and that the world is completely immersive, meaning that physical and mental reality is brought together. Users can do anything they want to in the Metaverse that they could in the real world.

The interviewee is familiar with Proto-Metaverse platforms, having experience with Proto-Metaverses such as games like World of warcraft and environments like VR-chat.

To the best of their knowledge, they have spent more than 800 hours per year (about 900) on all Proto-Metaverse platforms, categorising them into a frequent user. They state that they have been exposed to and have had experience with using these platforms on a long term basis, and have accumulated these hours over a span of multiple years.

For the second part of the third question, they answered that they currently spend around 20-30 hours per week on a Proto-Metaverse platform, making them a current moderate user as well.

The issues that they have experienced related to privacy, security or safety depend very much on the platforms, with some being far more unsafe or toxic than others. Personally, they have not had very much experience with security related issues, but an example they have named, was having their private login information leaked on a used Proto-Metaverse platform, however thankfully not causing the interviewee to lose anything like money or safety.

They say the issues are complex, and malicious actors are always adapting to the regulations and policies, and they always find a way to either overcome them or trick ignorant users into scams, giving away private information etc.

According to them, emerging security programmes like two step authentication are making good improvements, but what really must be done in their opinion is improving the education of users and increase their digital awareness.

Interview 2

How interviewee 2 sees it, the Metaverse is a virtual reality social space. An example they named is Facebook's Meta project.

They have much experience with multiple Proto-Metaverse platforms, primarily in the gaming world, with games such as ARK, Skyrim or GTA V, etc. (highly immersive platforms)

The total time active on the platforms accumulates to around 15.000 hours, across about 15 years, making the interviewee a very experienced platform user, with an average time spent /year of around 1000 hours across all used platforms. Depending on the used platform, they spent more time actively on social spaces, between 2018-2020 mostly being active on these social platforms, also mentioning the COVID pandemic's effects after discussion, causing them to spend more time online.

Per week, the interviewee says they spend 20-30 hours per week digitally, making them a moderate user of the Proto-Metaverse platforms.

The interviewee has a decent amount of experience with cybersecurity, having been on both sides of security as a user and a mock hacker, having taken a university course in Whitehat hacking. Depending on the software, they say it can be very easy to breach digital security, because some people have no knowledge on security software or any knowhow about online private security. On the other hand, the interviewee has experienced a mock malware intrusion on a university computer from one of their classmates, having experienced what it is like to have their security breached.

Related to policies, having a database where common scam techniques/ hacking techniques are collected and stored to prevent any others in the future from using similar techniques would resolve many cybersecurity issues. It would help people who have no knowledge of hacking or scams, because the database system would recognise the malicious content before it were even sent. Educating users would also drastically improve cybersecurity, helping them know what to look for in suspicious content or people.

Interview 3

The interviewee initially states that they are not quite familiar with the Metaverse. After an introduction, they gained a sense of what it entails and what it looks like currently, mainly referencing Proto-Metaverse platforms as things they are familiar with.

They say that they spend most of their digital time on Proto-Metaverse platforms like Facebook, not having used any other, more immersive platforms in the forms of gaming or business. They have strictly kept it social. They do have experience with the interactivity of these social platforms.

Per week, the interviewee states that they spend about 10-20 hours on their platforms, putting them in the category of occasional user, which matches their time per year spent, which is around 700-800 hours per year, estimated.

According to the interviewee, online advertising on these platforms are very dangerous, having no moderation on the content of the advertisements. Scams are rampant on these platforms' ads. A specific experience they name is an order they placed on a set of advertised clothing, having ordered two pairs of shorts. However, they only received a cheap pair of sunglasses. This seems to be an example of fake advertising, and scamming as a result.

Ideally, the interviewee would see that online advertising were more moderated, wanting them to be regulated by checking agents on the platforms.

Interview 4

The interviewee says that the Metaverse is an online social space. With some more explanation about the Metaverse from the interviewer, they became more familiar with the term, and said that they recognise current iterations of Metaverse-like platforms.

They state that they have experience with and use many of the social media platforms which have aspects of the Metaverse, like Facebook, Twitter, Instagram and Snapchat. These platforms are all very interactive with other users and the environment, and even have Augmented Reality aspects integrated in them that the interviewee knows about and has used.

After discussing the time spent on all platforms, the interviewee has about 200-300 hours/year spent on their used Proto-Metaverse platforms on average. This classifies them as an occasional user. This is backed up by their average weekly time spent of 16 hours per week, also putting them into the occasional user bracket.

Most of the experiences that the interviewee has had with the aspects of privacy, security and safety are related to scams and giving up private information. There are messages they received online, saying that the messenger claimed to be a family member, and tried to gain information off the interviewee that they did not see the need for. They avoided the issue with their critical thinking and experience with cybersecurity.

On how the interviewee would see improvements on future Metaverse platforms, they gave the idea of regulating I.P. bans, meaning that I.P. addresses that are frequently reported to practice malicious and or illegal cyber-activities, are banned from the further use of the platforms applicable.

Interview 5

The last interviewee says they are somewhat familiar with the Metaverse, having done research into the concept and expressing interest in its future developments. They know it is an online virtual world, completely merging physical and virtual reality. They compared it to being able to go out wherever they want with friends without actually leaving their home.

The platforms that they currently use socially are Facebook and Twitter, as well as some online games, for example online casinos, where the casino's environment is completely immersive.

The average time spent per year on these platforms, the interviewee has stated is around 300-400 hours, classifying them as an occasional user. Currently, they spend approximately 20 hours on their platforms, with most of that

time going into their social platforms. Again, this also puts them in the high end of being and occasional user.

The interviewee stated that their social presence (on Facebook) also presents their gambling profiling. This has opened them to multiple gambling related scams every week, which is quite drastic. To keep their profile more secure, the interviewee would want to be able to somewhat control the algorithm that determines their profiling. They would see the option implemented where they could somehow control who contact or view their profile and who cannot.