Linh To, Ana Maharjan, Phyllis Cao, Rafikiel Seyumde, Keshuo Liu, Haiyuan Zhang
Prof. Dokyun Lee
BA840 B1
01/17/2022

Executive Summary: Ethical Concerns in the Metaverse

Since Oculus launched their first virtual reality (VR) headset “Oculus Rift” in 2012 and Facebook acquired the company in 2014, we have taken some big strides into bringing the VR world closer to the physical world. On October 28th, Facebook announced the launch of their newest project of an interconnected digital world “Metaverse", a vision for the new era of the Internet where users can have real-life interactions in a virtual setting. As stated by Meta’s CEO, Mark Zuckerberg, “mobile is the platform of today…now we’re also getting ready for the platforms of tomorrow” (Meta). Undoubtedly, Data and AI technology will become a critical part of the Metaverse. While there are various benefits and opportunities presented by the development of the Metaverse, this boundless movement of data poses both a privacy and security risk for users. Algorithms are designed to improve our lives but the trade-off, in this case, includes issues regarding user privacy and security. Our project will investigate these tradeoffs by understanding the implications of the Metaverse on individual data privacy and security. We will also evaluate algorithmic security and privacy concerns through various ethical frameworks.

Issue 1: Data Profiling/Collection

User profiling and data collection are major areas of concern with the development of the Metaverse. The three main categories of user data that would be collected are demographics, behavioral and communications information. In the Metaverse, since every user and object is a product, there is a lot of profiling data that is collected about the user. For instance, on Internet 2.0, marketers will use trackable metrics such as click rates, mouse movement to understand user experiences on a website (Cresci & Pietro 5). However, with the Metaverse, the extent of data collected on the user is much broader as the platform can record audio and text recordings, body movements, physiological responses, and real or virtual interactions with the surrounding environment. This is problematic due to the realistic nature of the Metaverse technology; users are at risk of facing nudges that create over-sharing private information, which may lead to echo chamber and filter bubble issues that are prevalent in today’s social media.

Issue 2: Data Privacy/Security

Some individuals may prefer to create avatars that mimic themselves or others when collecting personal information. This may distort the image of the self/others because some decentralized systems that govern hard-coded API like Roblox could result in data theft (Mikalaukas 3). Data sharing breaches in decentralized systems to decision-makers can also pose cyber attacks. For example, Roblox uses weak hashing algorithms, putting children playing at risk (Mikalaukas 3). Therefore, malicious behaviours such as cyber-spying, cyber-stalking, and cyber-manhunt will also cause more severe mental and emotional harm (Cresci & Pietro 5). Agent-centred deontologists would agree to ensure safety for all users, with a focus on children. Furthermore, the Metaverse can exacerbate cyber-aggressions from a specific platform or community to a broader range of communities (Cresci & Pietro 5). For a consequentialist, building better communities by outweighing data risks would create safer virtual realities. Additionally, more online communications may increase the number and manners in which information could be collected and misused. Cybercrimes could be perpetrated due to more vivid but remote communication. On the one hand, corporations easily monitor online communications, implying potential data breaches while improper communication and interactions will be amplified due to immersive experiences. As Metaverse will inevitably become a new platform for educational uses, children are exposed to more unfavorable content.

Issue 3: Regulation

The Metaverse also challenges regulatory principles and control within our society (Cresci & Pietro 5). Implementing strong regulations relating to data and AI use will be difficult due to the obscurity of judicial boundaries within the Metaverse and the fast-paced nature of the current AI climate. Malpractice is more challenging to monitor in the Metaverse due to the shareability of algorithms and editable libraries. The responsible parties for evaluating security risks may require more complex skill sets and a multidisciplinary background in computer science, cyber-security, hardware, ethics, and moral philosophy. Consequentialists would weigh the options and assess if the benefits outweigh the risks and challenges mentioned above regarding security. Deontologists would have to consider users' fundamental rights with soft nudges with agent-focused virtue ethics. As observed in the current social media called “VRchat ", regulations include weak guidelines for users and focus on improving the users’ ability to self-moderate while using the platform. Users can have a say in regulation creation with the flexibility to support the individuals' needs, with various communities experimenting with government creation. Imagine “Reddit” in VR with their AI bots and volunteers as moderators.

Conclusion

In conclusion, given the potential data collection, privacy and security risks associated with the Metaverse, a few solutions have been proposed. First of all, a combination of privacy fundamental strategies can be used for users to choose their desired level of privacy, which includes creating a mannequin or multiple clones of one’s avatar to shadow one’s own activities, creating a private copy of a public space for the exclusive use of the user, or temporarily locking out other users from a public space, and allowing user teleportation, invisibility or other forms of disguise (Cresci & Pietro 7). Secondly, the implementation of AI-specific regulations may be helpful to overcome security issues through the collaboration of policymakers. For example, the GDPR and other measures have been put in place to improve AI governance. The notion of explainable AI and its implication are slowly being noticed and a consequentialist would side with these actions. In addition, more advanced technical solutions will also help to address the data-related issues that we mentioned above. For instance, Facebook is already working on new privacy-enhancing technologies (PETs) to control the use of personal data or ads through cryptography and statistical techniques (Roy, A). However, there will be various limitations for us to overcome regarding privacy and security concerns, such as exponential user growth and information storage, unpredictable software and hardware roadblocks, and difficulty to reach a union policy for the whole Metaverse. There is much more to the Metaverse that is currently unknown, and it is only with an ethical, problem-solving mindset that we can hedge all the potential challenges in the future.

References:

1. Anne Hobsona (July 2020) *Phantoms, Crashers, and Harassers: Emergent Governance of Social Spaces in Virtual Reality*. Retrieved January 17, 2022 from https://www.thecgo.org/wp-content/uploads/2020/09/Phantoms-Crashers-and-Harassers-Emergent-Governance-of-Social-Spaces-in-Virtual-Reality.pdf
2. Dick, E. (2021, November 15). *Public policy for the Metaverse: Key takeaways from the 2021 AR/VR Policy Conference*. Public Policy for the Metaverse: Key Takeaways from the 2021 AR/VR Policy Conference. Retrieved January 15, 2022, from https://itif.org/publications/2021/11/15/public-policy-Metaverse-key-takeaways-2021-arvr-policy-conference
3. Greg Kumparak (March 26, 2014). *A brief history of Oculus* - TechCrunch+ Retrieved January 17, 2022 from https://techcrunch.com/2014/03/26/a-brief-history-of-oculus/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAFekp4gP25K5i0xKcXGvkJ2O--Cg5c_2ILPj3qLyTlhv1Ewls4PYu_xfZ539FT5_1DRTR8t5Wq_mOi6LFUSxGY7jPaIn_KMdJrHgBtpwpzKk_lFeikD-zCjj9_ss3Gjdk3HPZhmR9xpfs0a1o-UEpmm25Fu76lWEl-LV3hDgzZBH
4. Meta (March 25, 2014). *Facebook to acquire Oculus* Retrieved January 17, 2022 from https://about.fb.com/news/2014/03/facebook-to-acquire-oculus/
5. Mikalaukas, Edvardus. “Is Roblox Secure? Static Analysis Reveals Subpar Security Practices on Roblox Android App.” CyberNews, 28 Sept. 2021, https://cybernews.com/security/is-roblox-secure-static-analysis-reveals-subpar-security-practices-on-roblox-android-app/.
6. Pandya, J. (2019, April 17). *Troubling trends towards Artificial Intelligence Governance*. Forbes. Retrieved January 17, 2022, from https://www.forbes.com/sites/cognitiveworld/2019/02/25/troubling-trends-towards-artificial-intelligence-governance/?sh=11c43eaf25a5
7. Pietro, R. D., & Cresci, S. (2021, December 12). *Metaverse: Security and Privacy Issues*. ResearchGate. Retrieved January 15, 2022, from https://www.researchgate.net/profile/Roberto-Pietro/publication/357116743_Metaverse_Security_and_Privacy_Issues/links/61bc38924b318a6970e8ec03/Metaverse-Security-and-Privacy-Issues.pdf
8. Roy, A. (2021, December 21). *Metaverse Data Protection and Privacy: the next big-tech dilemma?* XRtoday. https://www.xrtoday.com/virtual-reality/Metaverse-data-protection-and-privacy-the-next-big-tech-dilemma/
9. Salvador Rodriguez (December 9th 2021). *Facebook takes a step toward building the Metaverse, opens virtual world app to everyone in U.S.* Retrieved January 17, 2022 from https://www.cnbc.com/2021/12/09/facebook-opens-horizon-worlds-vr-Metaverse-app-.html