

# Metaverse Threats & Liabilities

by Shymaa Arafat

shymaa.arafat@gmail.com, shar.academic@gmail.com

*"The World Economic Forum is committed to bringing together leading voices from the private sector, civil society, academia, and policy to define the parameters of an economically viable, accessible, and inclusive metaverse", Davos 2022*

It's no secret that the world's interest in Metaverses has grown rapidly in the last few years; Market experts expect the Metaverse economic volume to reach 5 T\$ by 2030 [1]. The 2022 Davos world economic forum held intensive discussions about Monetizing the Metaverse [2]; however, the discussions included handling the threats involved with such technology. Concerns included privacy, safety, rights protection and more with an emphasize on children using games and the internet in general [3].

*"We want to ensure that the next version of the internet and digital experiences are designed with children's well-being in mind"* Julia Goldin, Chief Product and Marketing Officer, LEGO Group.

In this article we will explore different security risks associated with Metaverses and tools to mitigate them; we will also discuss how liabilities are arranged in the Metaverse world, the regulations and some incidents of lawsuit cases. If they say a picture is worth thousand words, then this figure can give you a glimpse at what we are heading to ...

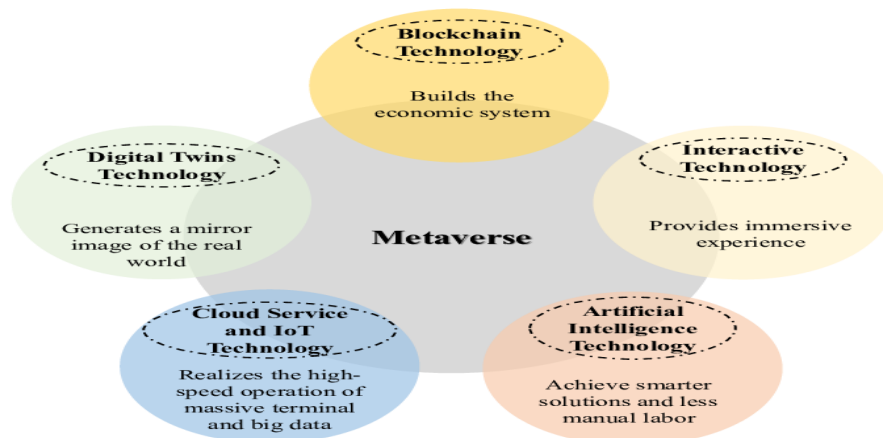


Fig1: Metaverse-related technologies and their impact on the Metaverse, taken from [9]

## Data Harvesting Attacks

It's expected that any virtual or augmented reality application will get some information about its users like the dimensions of the room they're in, their figure shape, arm length or strength,...etc because all these information is needed by the application [4] to perform its functionality; a VR experiment in [5] showed that an adversarial program had accurately inferred over 25 personal data attributes.

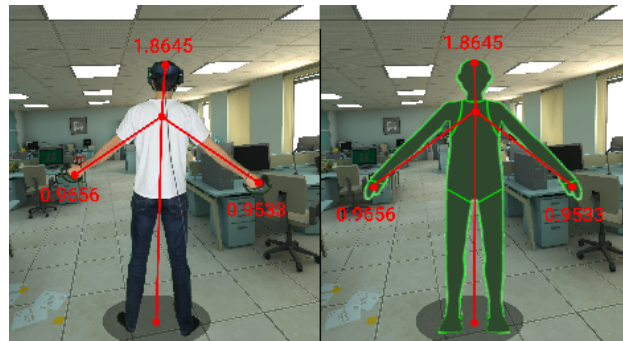


Fig 2a: VR application can deduce information about its user figure, taken from [5]

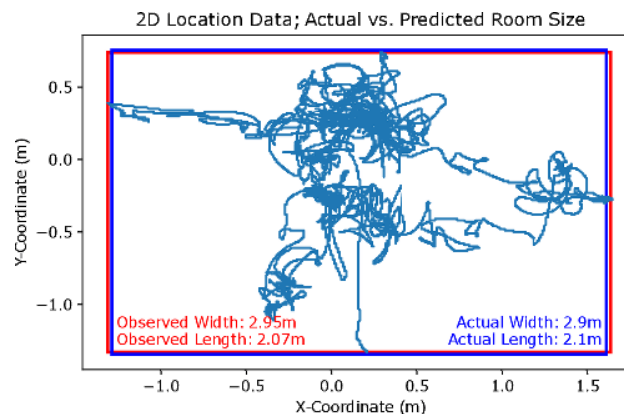


Fig 2b: VR applications can deduce information about the room size, taken from [5]

Naturally a complete Metaverse world with clothes and accessories to be worn will be able to know more about its users [6,7]. The research team by Berkeley University [8] tried to provide the first holistic framework for understanding intrusive data harvesting attacks in these emerging VR ecosystems where every thing is a digital asset and worths a money value. They introduced Meta & MetaGuard tools as a helping efforts to shape metaverse safety and privacy standards; MetaGuard is a (C#) plugin that quantify  $\epsilon$ -differential sensitivity for user data, then intelligently adding noise to maximize privacy while minimizing usability impact. You could say it is similar to the idea of mangling or obfuscation that is commonly used by some DAOs to achieve anonymity but for different reasons here, but with a careful caution of not distorting the functionality and consequently the fun or amusement (or sometimes the game competition)in

such applications.

Other research efforts in the same scientific direction does exist in the literature and there will always be room for more. The authors in [9] tried to introduce an extensive survey of all Metaverse threats, current mitigations, and future directions; while [10] discusses challenges facing developers & stake holders and presents some ideas on building a viable **Zero-Trust Architecture (ZTA)**<sup>1</sup> model for the metaverse.

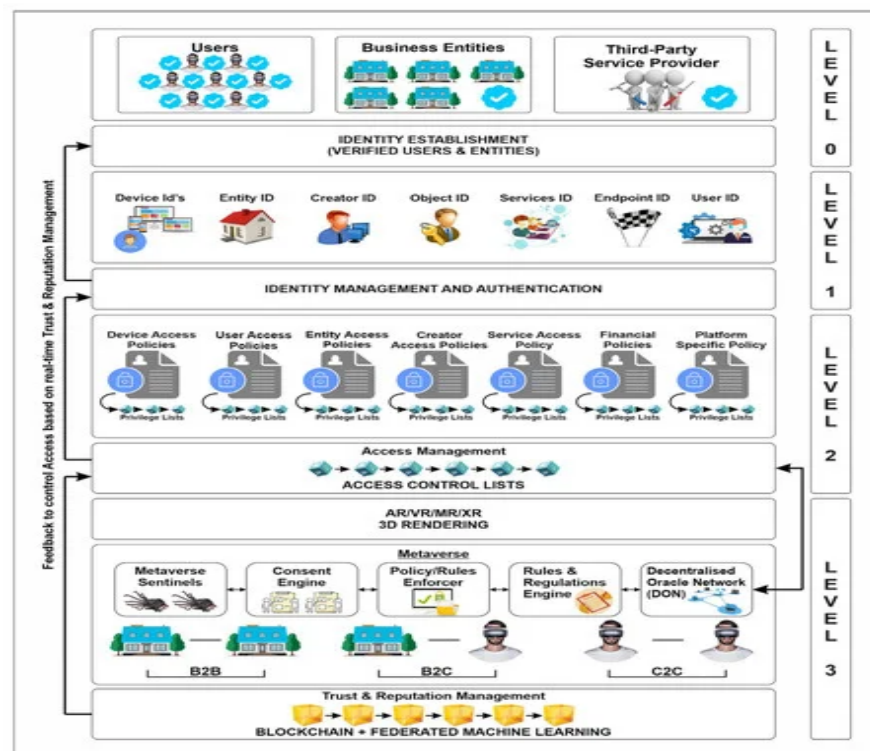


Fig 3: ZTA architectural model for the Metaverse, from [10]

## Economic Issues

Naturally plenty of uses of digital assets will evolve inside the Metaverse world; securing the identity (or you could say the “non fungibility”) of these digital assets and all financial

<sup>1</sup> It generally means a paradigm where you check and validate every TX from users (through PKI for example), from the application, from the platform,...etc; for more details visit (<https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>). However, I would informally describe it as we are normally used to in Blockchains and cryptocurrencies; authenticating users through PKIs, verifying TXs, trusted third party to map verified identity to anonymous identity as in techniques used to guarantee fair distribution of NFT free drops, the use of oracles (they call it Distributed Oracle Networks, DONs), accumulated reputation to decide when to punish or shut away malicious users (we will discuss that in what follows from [16]&[25]), providing regulations,...etc.

transactions in this new virtual world imposes the use of Blockchains and NFTs, although a Blockchain infrastructure is not exactly necessary to create a Metaverse world. In fact, there was one called "second life"<sup>2</sup> created in the year 2003 and still has 70m registered accounts till now [11]. However, there were no digital assets and financial transactions between them at that time; hence that's the way the story goes, all new Metaverses are cryptographically secured through Blockchains and all commercial activities happens through DeFi environment. Putting this in mind, we should realize that liabilities and copyright issues of NFTs will apply here too, but different countries have different DeFi regulations; for example when buying/selling/renting virtual land or property in the Metaverse, financial transactions need to be governed and regulated in an environment that lacks boundaries such as national borders. An interesting idea of a new virtual world borders The Network State is presented in [12]. Back to NFTs, we know virtual characters, clothes, accessories,...etc may have different set of rights associated with each kind; a lot of misconception, fraud, lawsuits are there regarding the rights you get when buying an NFT. A galaxy report [13] provided a glossary of examples on NFT copyright problems and some of the legal complains legal emerged around them. Examples problematic issues include whether owning a character NFT gives you the right to bring it to life as a TV show character, what happens when the company who created the NFT is sold to another company could it change the rules, how and what rights are transferred to the new owner when you sell the NFT,...etc. "Can't be Evil" [14] is a standardization attempt to encode the type, and provided rights for the NFT (as standard class types) within the creation meta data; ie, defined when minting the NFT.

## Liabilities & Regulations - Virtual Crimes

*"Regulators will have to pay attention to bullying, marginalization, and destructive stereotyping and discrimination."*, Dr. In Hyok Cha, Group Chief Digital Officer, CJ Corporation in [3]

In this new world possible harm can tackle dimensions that one couldn't possibly imagine before [15]; this includes sexual harassments, mental, pain(through the used sensor devices)<sup>3</sup>,...etc. The authors in [16] suggest that avatars in the metaverse should inherit the same arguments of artificial personality, resembling that of a robot like Sophia for example; the paper analyzed several lawsuits that we will mention in what follows and continue to newer

---

<sup>2</sup> In (<https://cointelegraph.com/news/does-the-metaverse-need-blockchain-to-ensure-widespread-adoption>) Stanford University professor Jeremy Bailenson explains why he thinks Metaverses can exist without Blockchains using a 2003 project called "Second Life" with 70m registered accounts till now; also, this 2016(before NFTs) paper (<https://www.sciencedirect.com/science/article/abs/pii/S026840121630175X>) supports his point proposing a Metaverse deployment plan with no Blockchains.

<sup>3</sup> Although did not encounter incidents in the literature, the idea as I understood from the paper, is a sensor device that for example could make you feel driving a plane with your heart beats getting higher could maybe could cause you a heart attack if controlled by an adversary, similarly a voice could go too high, a cup of tea too hot,...etc

ones. You will see that most cases end with the Metaverse company penalize and shutting away the adversary, and/or offering victims 3digits m\$ reconciliation settlement.

- The BBC article in [17] discusses a children sexual harassment that has been reported to the UK police; in 4/2022 they announced that internet sites could be fined or blocked if they failed to tackle "online harms", such as terrorist propaganda and child abuse, under government plans. However, back to the cross borders issue, the police said it had the authority to investigate criminal offences that had occurred in the UK only and those criminals were in another country. As for Roblox, the Metaverse where the incidents happened, according to BBC they shutdown the criminal's account. It's worth mentioning that it's not just UK police, the interpol and police authorities in many places [18,19] are also carving their way to handle such crimes; private organizations [20] started to provide certificates for Metaverse security Consultants (CMSC).



Fig4: John Staines and John Woodley, former police officers, from Est-E Safety Training, visit schools in UK to warn children about the worst-case scenarios in online gaming

- In the Facebook Metaverse beta version, a woman had been groped by a stranger on Horizon Worlds [22].
- A suit alleged that Facebook collected biometric information in the form of face prints, for the purpose of supporting its "face tagging" feature, in violation of the Illinois Biometric Information Privacy Act succeeded in achieving 650m\$ settlement [23].
- Also, Meta paid 725 m\$ last month for privacy leakage [24].

## Penalties & Game Reputation

Like slashing in the DeFi world, the Gaming environment often has its way to punish malicious players by shutting them away or putting some penalties on their locked digital assets. The

authors in [25] suggests, MMORPGs, a hierarchy of in-game penalties. They discuss virtual murder through a game called Kantian; i.e. when battle games allow virtual murder as a defeat, what happens if malicious players killed (virtually) their own team.

## **Virtual Interpol**

When everything is virtual in a virtual world, why not create a virtual Police?.

In October 2022, at the 90th Interpol General Assembly in New Delhi, an announcement was made, [26], that the INTERPOL Metaverse allows registered users to tour a virtual facsimile of the INTERPOL General Secretariat headquarters in Lyon, France without any geographical or physical boundaries, interact with other officers via their avatars, and even take immersive training courses in forensic investigation and other policing capabilities. The INTERPOL Metaverse is provided through the INTERPOL Secure Cloud, ensuring its neutrality.

We know also that UAE has its virtual Police Department [27].

## **Closure**

Metaverse is an emerging technology that provides enormous benefits and capabilities to its users; it is not just games and entertainment, there also educational [28] and cultural uses [29]. However, like any other technology, this comes with a lot of risks and threats which needs the collaboration of a lot of entities. Developers and scientists should work on privacy preserving solutions, police officers and law makers have to work on regulations, and also users & parents need to be cautious and aware of such risks.

## **References**

[1]<https://cointelegraph.com/news/metaverse-to-possibly-create-5t-in-value-by-2030-mckinsey-report>, last accessed 7/1/2023

[2] Stefan B. Hall and Cathi Li, World Economic Forum, <https://www.weforum.org/agenda/2022/02/metaverse-monetization-business-guide/>, accessed 12/8/2022.

[3]<https://www.weforum.org/agenda/2022/05/how-to-build-an-economically-viable-inclusive-and-safe-metaverse/>

[4] Junsu Lim, Hyeonggeun Yun, Auejin Ham, and Sunjun Kim, "Mine yourself!: A role-playing privacy tutorial in virtual reality environment", In CHI Conference on Human Factors in

Computing Systems Extended Abstracts, CHI EA '22, New York, NY, USA, 2022, Association for Computing Machinery.

[5] "MetaData, Exploring the Unprecedented Privacy Risks of the Metaverse", <https://rdi.berkeley.edu/metaverse/metadata/>, last accessed 18/6/2023

[6] Philipp Sykownik, Divine Maloney, Guo Freeman, and Maic Masuch., "Something personal from the metaverse: Goals, topics, and contextual factors of self-disclosure in commercial social vr.", In CHI Conference on Human Factors in Computing Systems, CHI'22, NY, USA, Association for Computing Machinery.

[7] <https://www.securitymagazine.com/articles/98142-9-security-threats-in-the-metaverse>, accessed 23/8/2022; the original report: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/metaverse-the-trouble-with-the-metaverse#newnavmenu-mobile>, accessed 26/8/2022.

[8] The whole "Metaverse & VR security" research thread, <https://rdi.berkeley.edu/metaverse/>

[9] [https://www.researchgate.net/publication/367455946\\_Metaverse\\_Security\\_and\\_Privacy\\_An\\_Overview](https://www.researchgate.net/publication/367455946_Metaverse_Security_and_Privacy_An_Overview), last accessed 18/6/2023

[10] "Metaverse Security: Issues, Challenges and a Viable ZTA Model" <https://www.mdpi.com/2079-9292/12/2/391>

[11] <https://cointelegraph.com/news/does-the-metaverse-need-blockchain-to-ensure-widespread-adoption>, last accessed 8/2022.

[12] <https://thenetworkstate.com/the-network-state-in-one-sentence>, last accessed 18/6/2023

[13] Andrew Hayward, <https://decrypt.co/107827/bored-apes-moonbirds-misled-buyers-nft-ip-rights-galaxy-digital>, accessed 20/8/2022.

[14] Miles Jennings and Chris Dixon, "The Can't Be Evil NFT Licenses", a16x crypto, <https://a16zcrypto.com/introducing-nft-licenses/>, accessed 1/9/2022.

[15] <https://www.pwc.com/us/en/tech-effect/cybersecurity/emerging-scams-and-phishing-risks-in-the-metaverse.html>, last accessed 17/6/2023

[16] Ben Chester Cheong, "Avatars in the metaverse: potential legal issues and remedies", International Cybersecurity Law Review 2022, <https://link.springer.com/article/10.1365/s43439-022-00056-9>

[17] <https://www.bbc.com/news/technology-48450604>, last accessed 18/6/2023

[18] Steven Fox, a police captain at the Milpitas Police Department in California,

<https://www.police1.com/investigations/articles/the-dark-side-of-the-metaverse-investigating-cryptocurrency-crimes-IFgA63O17pAXyK35/#:~:text=While%20financial%20crimes%20in%20the,sexual%20assault%20%20and%20even%20harassment.>, last accessed 17/6/2023

[19] Marc Cieslak & Tom Gerken, "Interpol working out how to police the metaverse", <https://www.bbc.com/news/technology-64501726>, last accessed 18/6/2023

[20]<https://www.thenationalnews.com/uae/2023/02/22/uae-authorities-look-at-how-to-police-dark-side-of-the-metaverse/>, accessed 18/6/2023

[21]<https://identitymanagementinstitute.org/cmssc-web3-security-certification/>, last accessed 17/6/2023

[22]<https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/>, last accessed 18/6/2023

[23]<https://www.labaton.com/cases/550-million-settlement-principle-of-biometric-privacy-lawsuit-labaton-sucharow-facebook>, last accessed 18/6/2023

[24]<https://www.xrtoday.com/virtual-reality/meta-settle-725-million-in-class-action-lawsuit/>, last accessed 17/6/2023

[25]Helen Ryland, "Getting away with murder: why virtual murder in MMORPGs can be wrong on Kantian grounds",Ethics and Information Technology 2019, <https://link.springer.com/article/10.1007/s10676-019-09498-y#:~:text=By%20exploiting%20the%20player%20controlling,be%20wrong%20on%20Kantian%20grounds>.

[26] <https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse>, last accessed 18/6/2023

[27]<https://www.thenationalnews.com/uae/2022/06/06/uae-police-set-up-metaverse-service-to-help-the-public/>, accessed 18/6/2023

[28]<https://blogs.worldbank.org/latinamerica/education-meets-metaverse-eastern-caribbean-national-colleges>,  
[https://www.researchgate.net/publication/363541574\\_Caribbean\\_Metaverse\\_Development\\_A\\_Literature\\_Review\\_Perspective](https://www.researchgate.net/publication/363541574_Caribbean_Metaverse_Development_A_Literature_Review_Perspective), accessed 19/9/2022

[29]<https://fortune.com/2022/04/28/museums-history-gamification-nfts-metaverse-tech-art-yizan-he/>, last accessed 31/8/2022