TATA CONSULTANCY SERVICES

Building on belief

User Privacy Protection in the Emerging World of Metaverse

Abstract

Web 3.0 has kickstarted a new era of innovation. Organizations have been quick to unveil their many capabilities, such as social connectivity and automation. The next evolution in the online experience is the metaverse–an immersive cyberspace, providing real-time virtual experience of social engagements via interoperable platforms. However, despite its potential, the metaverse is rapidly turning into a privacy nightmare for many stakeholders, including metaverse platform developers, hardware, software, crypto service providers, regulatory bodies, and end-users themselves.

Privacy is an area that will need to be managed with extreme caution ab initio. This paper provides insights on why privacy is important in the metaverse; the challenges surrounding potential technologies used to build metaverse; data that can be collected from potential sources; laws or regulations that are likely to control such issues, and best practices that organizations should follow to mitigate potential privacy risks.

Exploring the metaverse

The metaverse may be viewed as a “digital universe” where users interact, play, socialize, create, explore, and engage with each other through their digital avatars. Activities in the real world can be carried out in the metaverse by leveraging technologies like augmented reality (AR) and virtual reality (VR), blockchain, and more.

Despite its obvious advantages, however, privacy-related risks are likely to plague the metaverse.

The complexity of privacy challenges in the metaverse comprises, for example, regulation of data generated via avatars, identity breach, data transfer, and more. One aspect of the metaverse that presents privacy concerns is the large amount of personal data collected from users. Unlike typical social engagement platforms, metaverse systems may follow individuals far more closely.

Real-time tracking of physiological responses, biometric data like facial expressions, vocal inflections, and vital signs is possible in the metaverse. To further complicate matters, such data may fall under ‘sensitive’ category requiring strict controls, because, if such data remains unprotected, it may violate privacy via social engineering or other cyber-attacks if it is unprotected. It may also be misused for untargeted advertising by unregulated organizations or intermediaries, for example, for promoting health policies. Thus, while the technology is promising, it is fraught with privacy challenges, unless adequate regulations are developed on consent, collection, and transfer of data.

Data regulation and privacy paranoia

Transparency is critical for data privacy protection, and this would mean identifying the data to be collected accurately. Since metaverse data is likely to originate from a range of sources, being able to pinpoint the source of each data element is also essential. As mentioned previously, AR/VR technologies capture users' biometric data, facial gestures, etc., or from the metaverse itself and these must be adequately protected. Figure 1 depicts the architecture of data flow and regulation. The data (raw or processed) may be regulated via technical means like anonymization or legal regulations like General Data Protection Regulation (GDPR).

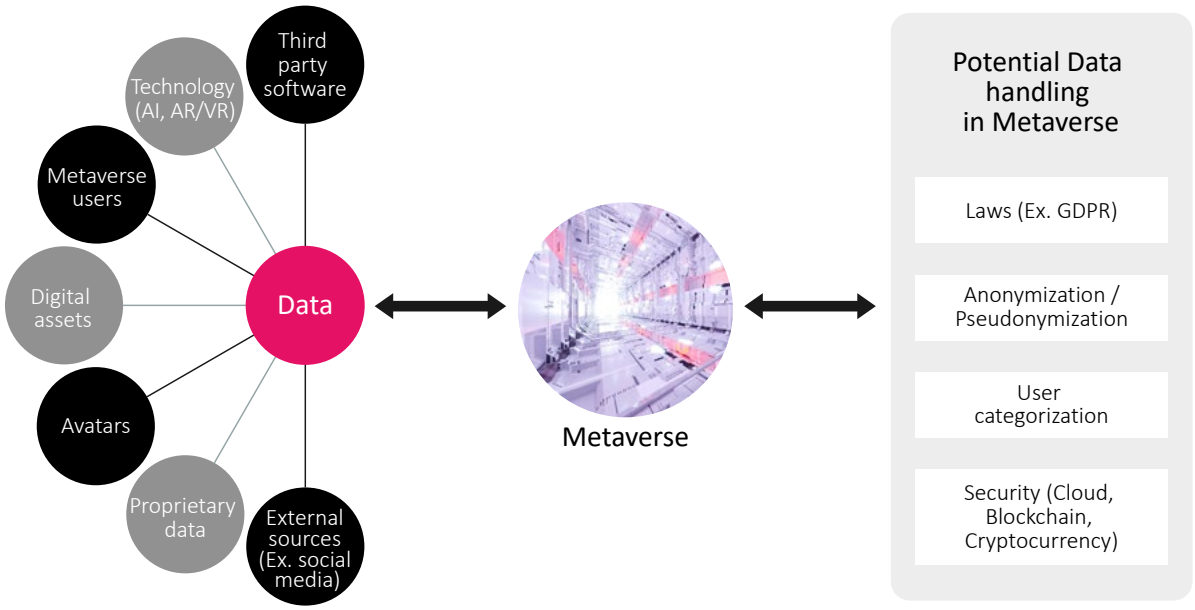

Figure1: Handling data safely in the metaverse

Dealing with metaverse data across industries

The metaverse is likely to be explored by all demographics, from children to corporate professionals. Authenticating data from all these users is crucial. For example, under the EU GDPR, processing the personal data of a child below 16 years would require consent. Consequently, a 12-year-old who wants to create an avatar of his favorite cartoon character and fight an opponent must consent to the collection of his or her Personal Identifiable Information (PII).

Metaverse also has the potential to transform the healthcare industry by facilitating complex surgeries in virtual environments, providing immersive surgical experiences to health practitioners, helping isolated elderly people interact with others, and enabling interactive experiences that improve mental health. However, major jurisdictions such as Europe and the US, have legislations like the GDPR, the Health Insurance Portability, and Accountability Act respectively, which strictly protect sensitive health-related data. Therefore, collecting and processing data that includes real-time interactions, facial gestures and results can prove to be challenging.

Another risk is the breach of a user's identity. A new collection of data might be developed, for example, if a youngster in the EU adopts the digital avatar of a Hollywood figure. And if the Hollywood character promotes a perfume brand in real life, adequate safeguards must be in place to ensure that the data collected and processed (from the child's physiological parameters to his digital avatar) is regulated and does not reveal the Hollywood character's personal information or link the child to the perfume brand.

Further, immense data will be generated and processed in real-time, i.e., while users may be exploring metaverse, their gestures and physiological responses may invariably change and get monitored or recorded. Anonymizing or pseudonymizing real-time data can prove problematic. If this data is unprotected, it may fall under the 'sensitive' category and violate privacy through social engineering, or other cyber-attacks. Unregulated organizations or intermediaries can misuse it for targeted advertising, such as for promoting health policies.

Data transfer can also pose serious risks. If a user in the US digitally associates with a shoe brand in the metaverse, data about this virtual experience may be transferred to the brand owner in the EU. There could also be issues related to protecting the sensitive data collected from dementia patients who have been actively engaging in the metaverse.

Blockchain and cryptocurrency may also pose risks. Questions like how to buy digital space in the metaverse without breaching PII will have to be answered. While decentralized technologies may be used for virtual asset transactions, authenticating a user would be critical as cybercriminals may create fake crypto domain names or smart contracts.

Non-Fungible Tokens (NFTs) will play a key role in the metaverse. Since each NFT is unique and linked to a virtual asset, any issue with digital assets such as server hosting or cyber-attack could eventually cause the loss of related NFT data and result in regulatory violations. In the absence of dedicated laws on cryptocurrency, risks may increase manifold.

Since there are no specific laws regulating avatars, the content that users interact with or explore via avatars may breach the personal details of a real-world person and make them identifiable. The Centre for Democracy and Rule of Law cited that 'the creation of a digital avatar particularly affects the right to personal data protection. It further cited that by 2030, about 23.5 million jobs will be using AR/VR. It is crucial to set the applicable standards and assess the risks to human rights[1].

Finally, privacy risks multiply when legal and intellectual property issues are not effectively mitigated. It will also be necessary to review the licensing agreements of third-party service providers operating in the metaverse.

Regulating metaverse - existing and upcoming legislations

A recent report recognizes that 'governments must enact or update legislation that limits data collection and processing'.[2] While the GDPR regulates privacy, it requires amendments to effectively regulate the metaverse. For example, if a data breach results in the loss of cryptocurrency, there must be more accountability for metaverse owners and third-party service providers like crypto platforms, so users can transact securely.

[1] CADEM.org; https://cedem.org.ua/en/analytics/tsyfrovi-avatary/

[2] Accessnow.org; Virtual worlds, real people: human rights in the metaverse; December 9, 2021; https://www.accessnow.org/human-rights-metaverse-virtual-augmented-reality/; Accessed March 16, 2022

Some regulations have been proposed. For instance, Europe's Digital Services Act mandates the explicit mention of restrictions on data usage, while the Digital Markets Act proposes the strict regulation of organizations providing core platform services if they qualify as 'gatekeepers.' The EU's Artificial Intelligence (AI) Act is likely to play a critical role in regulating the identity of avatars and related content.

Creators too will need to proactively engineer practices that run like a golden thread across the metaverse. In the days to come, we can expect countries to amend existing laws or introduce new ones to regulate metaverse privacy.

The University of Amsterdam suggested that 'Privacy of the virtual identity can neither be adequately protected by real world privacy rights, nor by privacy enhancing technologies in the virtual platform. Therefore, virtual right to privacy should be granted to avatars in respect of their bodily, locational, and informational privacy.[3]

Combating the battle – A proactive approach towards 'meta governance'

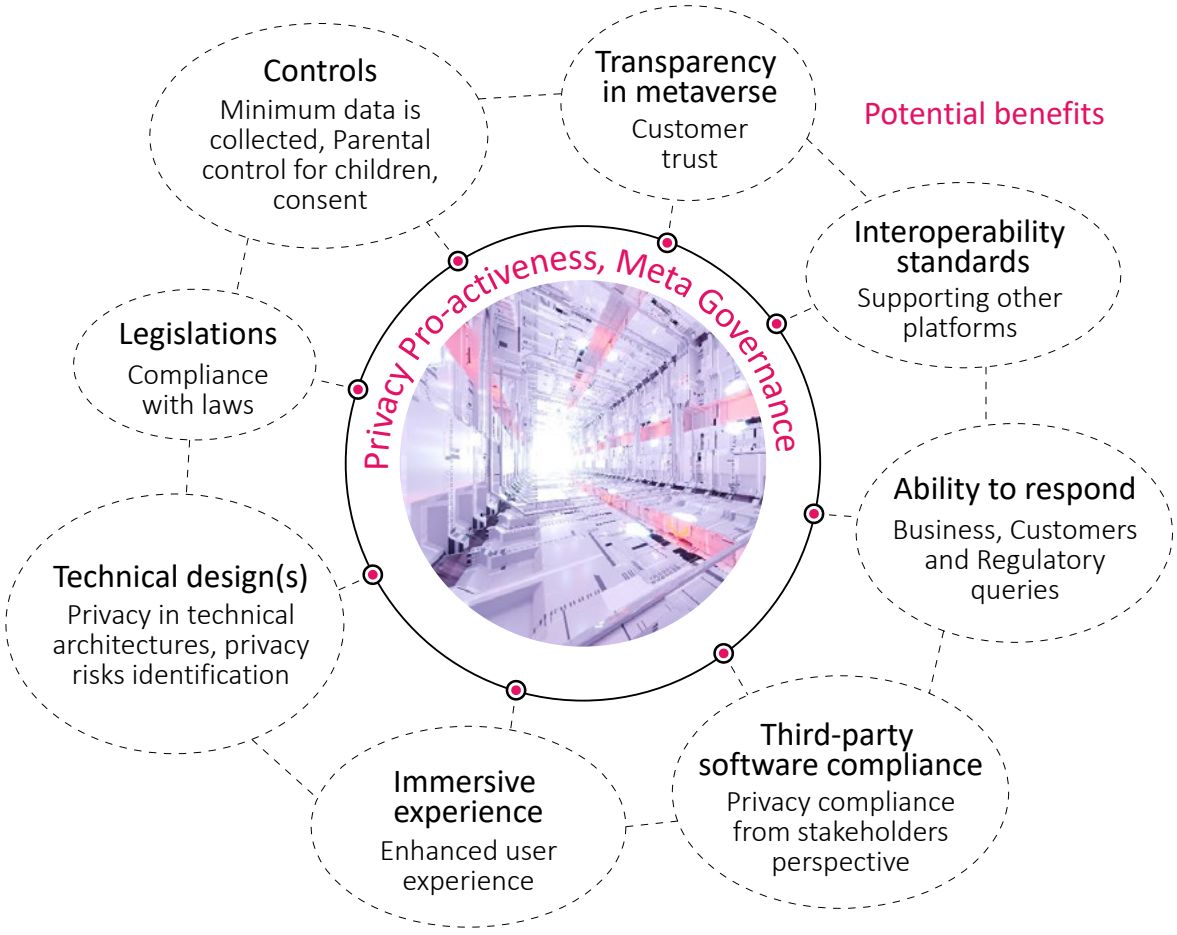

Figure 2: Potential benefits of privacy proactiveness

Figure 2 highlights some benefits of proposed proactive meta governance. These include transparency, compliance with legislation, ability to respond clearly to stakeholders, better controls, and so on.

[3] Forschung / Analyse; Virtual Identity and Virtual Privacy: towards a Concept of Regulation by Analogy; https://www.ivir.nl/publicaties/download/eGov_prasenz_2011_1.pdf; Accessed 16 March 2022

For cross border data security, technologies like Confidential Computing that facilitate protection of data in transit may be implemented. Privacy experts must ensure strict compliance with existing and proposed regulations and cross-border agreements like the GDPR Standard Contractual Clauses. Practices like transfer risk assessments and data privacy impact assessments can help mitigate privacy risks.

Children, who are more vulnerable to privacy risks, must be protected through a well-designed 'techno-privacy protection' approach. There must be controlled access for children with explicit parental consent, and real-time data transfer to ensure transparency. For instance, if a child assumes the avatar of an aggressive character, messaging alerts can be sent to parents. Such practices however must comply with established technical standards and regulations.

From a contractual due-diligence perspective, there must be well-defined and documented clauses between stakeholders. Agreements between metaverse creators and virtual asset service providers must include well-constructed anti-money laundering clauses, so parties will co-operate with investigative agencies in the event of a data breach. Similarly, since blockchain does not support data deletion, NFT transaction details may get permanently recorded. A privacy notice must inform users that they may not be able to exercise the 'right to be forgotten' after transacting virtual assets.

Advertisements in metaverse must be strictly regulated via a combination of technical and regulatory solutions like privacy-by-design, architectural security, and consent. Personal data must not be misused for targeted advertising. If a user interacts with a brand as an avatar, the PII obtained must not be utilized to identify the real user for the purpose of selling products in the physical world without their express consent. In the metaverse, blockchain may require improved designs. While smart contracts enable both secured and permissionless transactions, additional rules in terms of child consent may still be required. The protection of cryptocurrency and virtual asset data also necessitate a well-defined strategy. For example, if integrated metaverse platforms provide Initial Coin Offering (ICO), each participant must verify that user PII is not compromised.

While some countries have recognized cryptocurrencies, many others like India and China have not. This may create a complex situation, and to overcome such challenges, metaverse developers must proactively participate with governments and international bodies to develop universally recognized protocols and make them legally binding to mitigate potential risks.

Although blockchain provides decentralization and pseudonymity, issues may occur if data is shared with investigative agencies (mandatory disclosure). Cross-border investigations involving metaverse must be safeguarded by treaties that take a balanced approach between investigative powers of agencies and protections of persons' privacy and human rights. Adopting adequacy agreements may also aid in lowering the hazards associated with cross-border data exchange. Lastly, handling real-time data will require both technical and regulatory due diligence. While Confidential Computing and AI techniques may be used for real-time data anonymization, regulatory diligence may come via well-structured privacy and legal frameworks. Some measures may include defining the foundations of privacy in the early stages of design and development, while considering users and stakeholders' interests and concerns.

Toward enhanced security

While it may not be possible to foresee all the privacy risks that emanate in the metaverse, adopting the practices discussed above, especially while designing the metaverse can help in eliminate and mitigate major risks. Further, the EU's 'Guiding Principles on Business and Human Rights' may be expanded to include privacy protection, since many nations view the right to privacy as a basic right[4].

About the author

Ramandeep Singh

Ramandeep Singh is an Innovation Evangelist at TCS and advises on Legal, IP and Privacy related issues. He has over 15 years of consulting experience in IT industry and has also drafted many patent applications especially in AI, Digital Living, Image Processing, and related areas for all major jurisdictions. His areas of interest include IP, Privacy and Cloud Computing. He holds a Bachelor's, a Post-Graduate Diploma, and a Master's in Computer Applications from Indira Gandhi National Open University, India, and a post-graduate LL.B. degree from Delhi University.

[4] https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

TATA CONSULTANCY SERVICES

Awards and accolades

#1 IN CUSTOMER SATISFACTION 2020/21 EUROPE Whitelane Research

top EMPLOYER NORTH AMERICA 2021 CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

top EMPLOYER GLOBAL 2020 CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

ASIA'S OUTSTANDING COMPANIES POLL 2020 ASIAMONEY

STEVIE AWARDS 2020

CONGRATULATION CIO100 WINNERS 2020

FinanceAsia ASIA'S BEST COMPANIES 2020

DIGITAL IMPACT AWARDS WINNER

CANADIAN HR AWARDS 2020

THE CIVIC 50 POINTS OF LIGHT

FTSE4Good

CDP DISCLOSURE INSIGHT ACTION

2020 Brand Finance® Awards
TOP 3 IT SERVICES BRAND

2020 Brand Finance® Awards
FASTEST GROWING IT SERVICES BRAND FOR THE DECADE 2010 - 2020

AWARDED Superbrands BRITAIN'S CHOICE 2020

AWARDED Superbrands AMERICA'S CHOICE 2020

Contact

Visit the Research and Innovation page on www.tcs.com

Email: innovation.info@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is a purpose-led transformation partner to many of the world's largest businesses. For more than 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge. TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company's 500,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit **www.tcs.com** and follow TCS news **@TCS**.

Corporate Marketing | Design Services | M | 03 | 22