RESEARCH ARTICLE OPEN ACCESS

The Normalization of Metaverse and the Myth of Data Privacy

Jayakrishnan M
Department of Hindi, Sree Sankaracharya University of Sanskrit, Kalady, Kerala, India

ABSTRACT
The rapid expansion of the Metaverse—a collective virtual shared space created by the convergence of virtually enhanced physical reality and physically persistent virtual space—raises significant concerns about data privacy. This paper aims to provide an overview of the Metaverse concept, outlining its key components and exploring the profound data privacy issues associated with its normalization. It delves into the objectives of protecting user data and emphasizes the significance of these concerns in ensuring a secure and trustworthy digital environment.
Keywords: Meta, Metaverse, Virtual Reality, Virtual Space, Data Privacy.

I. INTRODUCTION

A. Definition and Evolution

The Metaverse is often defined as a collective virtual shared space, created by the convergence of virtually enhanced physical reality and physically persistent virtual spaces, including the sum of all virtual worlds, augmented reality, and the Internet. The term "Metaverse" was first coined by Neal Stephenson in his 1992 science fiction novel "Snow Crash," where it was depicted as a fully immersive virtual world. In recent years, the concept has evolved, driven by advancements in technology such as virtual reality (VR), augmented reality (AR), and blockchain. These technologies enable the creation of immersive environments where users can interact with each other and digital objects in real-time, blurring the lines between the physical and digital worlds (Stephenson, 1992).

The evolution of the Metaverse can be traced through various stages, beginning with early virtual worlds like "Second Life" and massively multiplayer online games (MMOs), which laid the groundwork for more sophisticated, immersive environments. More recent developments include platforms like Facebook's Horizon Workrooms and Epic Games' Fortnite, which have become early iterations of the Metaverse, showcasing the potential for social interaction, commerce, and entertainment in virtual spaces (Mystakidis, 2022).

B. Components

The Metaverse comprises several components, including virtual reality (VR), augmented reality (AR), blockchain, and non-fungible tokens (NFTs). VR and AR technologies create immersive experiences by blending digital and physical worlds, enabling users to interact with virtual objects as if they were real. VR creates a fully immersive experience, while AR overlays digital content onto the physical world, enhancing users' perceptions of their surroundings (Cipresso, Giglioli, Raya & Riva, 2018).

Blockchain technology plays a critical role in the Metaverse by providing decentralized control, ensuring transparency, and facilitating secure transactions. It underpins the creation and exchange of NFTs, which are unique digital assets that represent ownership of virtual goods, real estate, and other items within the Metaverse. The integration of blockchain technology is crucial for establishing trust and security in these virtual environments, as it allows for verifiable ownership and the protection of users' digital assets (Brennan & Kreiss, 2019).

C. Importance of Data Privacy

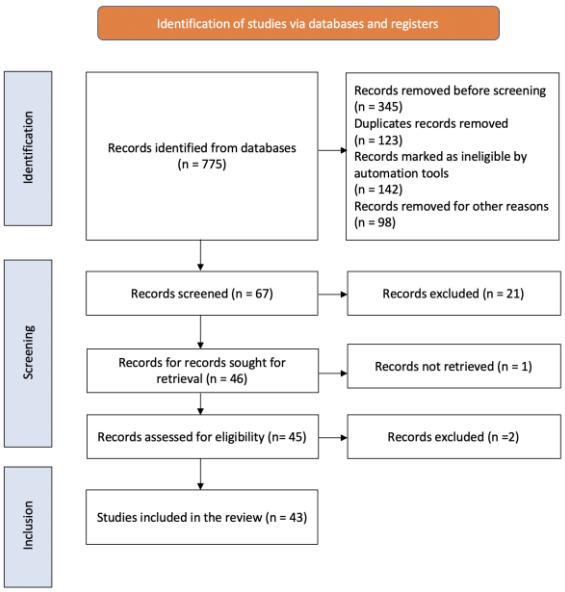
Data privacy is a critical concern in the digital age, particularly in the context of the Metaverse, where the collection and use of personal information are integral to its operation. As technology advances rapidly, privacy protections have struggled to keep pace, leading to significant concerns about data misuse and unauthorized access. The immersive nature of the Metaverse amplifies these issues, as users' actions and behaviours are extensively tracked, creating detailed profiles that can be exploited for various purposes, including targeted advertising and surveillance (Solove, 2006; Nissenbaum, 2010). The decentralized structure of the Metaverse further complicates privacy regulation enforcement, making it challenging to protect user data across multiple platforms and jurisdictions (Cohen, 2019; Véliz, 2020). Proactive measures, including clear policies and user control over personal information, are essential to safeguard privacy in these evolving digital spaces.

II. METHODOLOGY

To conduct a literature survey on “The Normalization of the Metaverse and the Myth of Data Privacy”, a search was conducted in August 2024 across various electronic databases, including PubMed, SCOPUS, EMBASE, COCHRANE library, and Science Direct. The search utilized MeSH terms/keywords such as "Metaverse", "Data Privacy", “Blockchain”, “Augmented Reality” and "Virtual Reality". In addition to the electronic search, cross-references and textbooks were manually searched for relevant articles. The inclusion criteria included articles published in the English language from August 2010 to August 2024 that fulfilled the

study objectives. The article selection process involved assessing the inclusion and exclusion criteria, as well as conducting a quality assessment. Out of the initial 775 articles identified, 67 were selected based on their titles and abstracts. After evaluating the full texts and applying the inclusion and exclusion criteria, 43 articles were chosen for the review, meeting the study's criteria (Figure 1).

Figure 1: Selection Criteria of the Studies



III. THE METAVERSE: CONCEPT AND DEVELOPMENT

A. Definition and Scope

The Metaverse is a collective virtual shared space that merges the physical and digital worlds, enabling users to interact with each other and digital content in real-time. It is characterized by its immersive, interactive, and persistent nature, allowing users to engage in various activities ranging from socializing and gaming to shopping and working. The Metaverse is not a single entity but rather a network of interconnected virtual worlds, each offering unique experiences and opportunities for users (Dionisio, Burns, & Gilbert, 2013).

The scope of the Metaverse extends beyond mere entertainment or gaming. It encompasses a wide range of applications, including virtual offices, online education, digital art galleries, and even virtual real estate. The Metaverse represents a new frontier in digital interaction, where the boundaries between the physical and virtual are increasingly blurred, and users can experience a seamless integration of both realms (Ball, 2022).

B., Technological Foundations

1) VR and AR Technologies:

Virtual Reality (VR) and Augmented Reality (AR) are fundamental to the Metaverse, providing the immersive experiences that define these virtual environments. VR creates fully immersive digital worlds, isolating users from the physical world and allowing them to interact with entirely virtual environments. AR, on the other hand, overlays digital content onto the physical world, enhancing users' perceptions and interactions with their surroundings (Cipresso, Giglioli, Raya, & Riva, 2018).

These technologies rely on advanced hardware, such as VR headsets, AR glasses, and haptic devices, to deliver realistic and interactive experiences. The development of these technologies has been driven by significant advancements in computer graphics, motion tracking, and artificial intelligence, enabling more sophisticated and lifelike virtual environments (Milgram & Kishino, 1994).

2) Blockchain and Decentralized Systems:

Blockchain technology is another critical component of the Metaverse, providing the infrastructure for decentralized control, secure transactions, and digital asset ownership. By using blockchain, the Metaverse can operate without centralized authority, ensuring transparency and trust in virtual transactions. This is particularly important for platforms like Decentraland and The Sandbox, where digital land and assets are traded as non-fungible tokens (NFTs) (Tapscott & Tapscott, 2016).

Decentralized systems also play a role in the governance of Metaverse platforms, allowing users to participate in decision-making processes through decentralized autonomous organizations (DAOs). These systems ensure that control over the platform is distributed among users, rather than concentrated in the hands of a single entity, aligning with the ethos of decentralization that underpins the broader blockchain ecosystem (Buterin, 2013).

C. Social and Economic Impact:

The Metaverse is poised to have a profound impact on social interaction, entertainment, and commerce. In terms of communication, the Metaverse offers new ways for people to connect, collaborate, and socialize in virtual spaces, breaking down geographical barriers and creating a sense of presence and immersion that traditional online platforms cannot match (Zhao, 2021).

In the realm of entertainment, the Metaverse provides a platform for immersive experiences that go beyond passive consumption. Users can actively participate in virtual concerts, sports events, and other forms of entertainment, creating a more engaging and interactive experience. The success of virtual events,

such as Travis Scott's concert in Fortnite, demonstrates the potential of the Metaverse to revolutionize the entertainment industry (Hamilton, 2020).

The economic impact of the Metaverse is also significant, with the emergence of new markets for digital goods, services, and experiences. Virtual real estate, digital fashion, and NFTs are just a few examples of the new economic opportunities that the Metaverse has created. The rise of virtual economies within these platforms has the potential to disrupt traditional business models and create new avenues for commerce (Davidson, 2021).

IV. DATA PRIVACY IN THE METAVERSE

A. Nature of Data Collected

1) Types of Data:

The Metaverse collects a wide range of data from its users, including personal, behavioural, and biometric information. Personal data includes information such as names, addresses, and payment details, while behavioural data encompasses users' interactions, preferences, and activities within the virtual environment. Biometric data, such as facial recognition, voice patterns, and even physiological responses, is increasingly being collected to enhance the immersive experience and personalize interactions (Ohm, 2010).

The collection of this data is essential for creating personalized experiences and maintaining the functionality of the Metaverse. However, it also raises significant privacy concerns, as the sheer volume and sensitivity of the data collected can be exploited if not properly protected (Solove, 2006).

B. Methods of Data Collection and Tracking

Data collection in the Metaverse is achieved through various methods, including direct input from users, tracking of their interactions, and the use of sensors and devices that monitor biometric data. For example, VR headsets can track users' movements, gaze, and even emotional responses, while AR devices can capture information about users' surroundings and overlay digital content based on their location (Cummings & Bailenson, 2016).

Tracking technologies, such as cookies and beacons, are also used to monitor users' activities within the Metaverse, collecting data on their behaviours and preferences. This data is often used for targeted advertising, content recommendations, and other forms of personalization. However, the lack of transparency in how this data is collected and used raises concerns about user consent and control over their information (Zuboff, 2019).

C. Privacy Concerns and Risks

1) Surveillance and Data Breaches:

One of the primary privacy concerns in the Metaverse is the potential for surveillance. The detailed data collected from users can be used to monitor their behaviours and interactions, creating profiles that can be exploited for various purposes, including targeted advertising, manipulation, and even control (Lyon, 2007). The pervasive nature of data collection in the Metaverse increases the risk of surveillance, as users are constantly being tracked and monitored while engaging in virtual activities.

Data breaches also pose a significant risk, as the large amounts of sensitive information stored by Metaverse platforms make them attractive targets for hackers. A breach of this data could have severe consequences for users, including identity theft, financial loss, and damage to their reputation (Solove & Hartzog, 2014). The decentralized nature of some Metaverse platforms can complicate efforts to secure data, as it may be spread across multiple servers and jurisdictions, making it more difficult to protect against breaches.

2) Inadequate Privacy Policies and User Consent:

Another major issue is the inadequacy of privacy policies and the lack of informed user consent. Many Metaverse platforms have complex and opaque privacy policies that users may not fully understand or may not even read. As a result, users may unknowingly consent to the collection and use of their data in ways that they are not comfortable with or that violate their privacy rights (Nissenbaum, 2010).

The issue of consent is further complicated by the immersive nature of the Metaverse, where users may not be fully aware of the extent to which their data is being collected and used. This lack of transparency and control can lead to a loss of autonomy and trust in the platform, undermining the potential benefits of the Metaverse (Westin, 1967). Addressing these privacy concerns is crucial to ensuring that the Metaverse remains a safe and secure space for all users.

D. Case Studies

1) Case Study 1: Meta's Horizon Worlds:

Meta's Horizon Worlds has been one of the most prominent early iterations of the Metaverse, offering users the ability to create and interact in virtual spaces. However, the platform has faced significant scrutiny regarding its data privacy practices. One major concern involves the extensive data collection methods used by Meta, which include tracking users' movements, interactions, and even their gaze direction through VR headsets. This data is used to create detailed profiles for targeted advertising and other purposes.

In 2022, Meta faced backlash after reports emerged that the platform's privacy settings were not transparent enough, and users were not fully informed about the extent of data being collected. Critics argued that the platform's complex privacy policies made it difficult for users to understand what they were consenting to, raising concerns about informed consent and the potential for misuse of personal information (Stein, 2022). This case highlights the need for clearer privacy policies and greater transparency in how data is collected and used in the Metaverse.

2) Case Study 2: Decentraland:

Decentraland, a blockchain-based virtual world, has also encountered privacy challenges, particularly related to the decentralized nature of its platform. While Decentraland's use of blockchain technology allows for greater user control and transparency, it also presents unique privacy risks. For instance, because transactions and ownership records are stored on a public blockchain, they are visible to anyone with access to the blockchain. This transparency, while beneficial for ensuring trust and security, can also expose users' activities and transactions to scrutiny, potentially compromising their privacy.

In 2021, a security researcher discovered a vulnerability in Decentraland's smart contracts that could have allowed an attacker to gain unauthorized access to users' data, including their digital assets and personal information. Although the vulnerability was quickly patched, the incident underscored the risks associated with decentralized platforms and the importance of robust security measures to protect user privacy (Cuen, 2021).

3) Case Study 3: Roblox:

Roblox, a popular online platform that allows users to create and play games within a virtual environment, has also faced privacy issues, particularly concerning its younger user base. In 2020, concerns were raised about the platform's data collection practices, especially regarding how it handles the personal information of minors. Despite its popularity among children and teenagers, Roblox's privacy policies were criticized for being unclear and not providing sufficient protection for younger users.

The platform was accused of collecting more data than necessary, including tracking users' interactions and in-game purchases, without adequately informing them or their parents. This led to concerns about compliance with child privacy laws, such as the Children's Online Privacy Protection Act (COPPA) in the United States. Roblox has since made efforts to improve its privacy practices, including updating its privacy policies and implementing stricter data collection protocols for minors (Levy, 2020). However, this case highlights the ongoing challenges of ensuring data privacy for vulnerable populations in the Metaverse.

4) Case Study 4: The Sandbox:

The Sandbox, another blockchain-based virtual world, has similarly faced privacy concerns, particularly related to the security of users' digital assets and personal information. In 2022, The Sandbox experienced a data breach in which a hacker gained access to the email addresses and personal data of thousands of users. The breach raised concerns about the platform's data security measures and the potential for future attacks.

Following the breach, The Sandbox took steps to enhance its security protocols, including implementing two-factor authentication and conducting regular security audits. However, the incident highlighted the risks of storing sensitive information on decentralized platforms and the need for continuous vigilance in protecting user data (Wright, 2022). This case demonstrates the potential consequences of data breaches in the Metaverse and the

V. THE MYTH OF DATA PRIVACY IN DIGITAL SPACES

A. Historical Context of Data Privacy

1) Evolution of Privacy Concerns in Digital Environments:

The concept of data privacy has evolved significantly with the advent of digital technologies. In the early days of the internet, privacy concerns were primarily focused on the collection and sharing of personal information through websites and online services. As the internet grew, so did the sophistication of data collection methods, leading to increased awareness and concern about how personal data was being used and who had access to it (Westin, 1967).

In the 1990s and early 2000s, privacy concerns were largely centered around the use of cookies and other tracking technologies that allowed companies to monitor users' online activities without their explicit consent. This led to the development of privacy laws and regulations, such as the European Union's General Data Protection Regulation (GDPR) and the United States' Children's Online Privacy Protection Act (COPPA), aimed at protecting users' privacy and giving them greater control over their personal information (Bennett, 2011).

However, as digital environments have become more complex and interconnected, privacy concerns have grown beyond traditional data collection methods. The rise of social media platforms, mobile apps, and now the Metaverse has introduced new challenges in ensuring data privacy, as these platforms often collect vast amounts of personal, behavioural, and even biometric data, often without users fully understanding the implications (Nissenbaum, 2010).

2) Comparison with Traditional Internet Privacy Issues:

Traditional internet privacy issues were largely centered around the collection of personal data for targeted advertising and marketing purposes. While these concerns are still relevant today, the advent of the Metaverse and other immersive digital environments has amplified the scope and scale of data privacy challenges. Unlike traditional websites, where users have some degree of control over the information they share, the Metaverse involves continuous, real-time data collection that is often more invasive and less transparent (Solove, 2006).

Moreover, the integration of technologies like virtual reality (VR), augmented reality (AR), and artificial intelligence (AI) in the Metaverse introduces new dimensions to privacy concerns. These technologies not only collect data about users' online behaviours but also capture physical and emotional responses, creating a more comprehensive profile of the user that can be exploited for various purposes (Cummings & Bailenson, 2016).

B. The Illusion of Control

1) User Perceptions vs. Actual Control Over Data:

One of the most significant challenges in digital privacy is the gap between user perceptions of control and the reality of data management practices. Many users believe they have control over their personal information through privacy settings and user agreements, but in practice, these mechanisms often provide limited protection. The complexity of privacy policies and the prevalence of "dark patterns"—design strategies that manipulate users into making choices that benefit the platform—further diminish users' actual control over their data (Acquisti, Brandimarte, & Loewenstein, 2015).

For instance, studies have shown that users often do not fully understand the implications of consenting to data collection, particularly in immersive environments like the Metaverse. They may believe they have opted out of certain types of data collection, only to discover that their information is still being tracked and used in ways they did not anticipate. This disconnect between perception and reality contributes to the myth of data privacy, where users are led to believe they have more control than they actually do (Calo, 2013).

2) Limitations of Privacy Settings and User Agreements:

Privacy settings and user agreements are often touted as tools that give users control over their data, but these mechanisms have significant limitations. Privacy settings are frequently designed to be confusing or difficult to navigate, making it challenging for users to make informed choices about their data. Moreover, even when users do manage to adjust their privacy settings, they may find that their data is still being collected and used in ways they did not explicitly authorize (Mattioli, 2020).

User agreements, or terms of service, also present significant challenges to meaningful user control. These documents are often lengthy, written in complex legal language, and presented as non-negotiable contracts that users must accept to access the platform. As a result, users typically agree to these terms without fully understanding the extent of data collection and usage they are consenting to. This practice undermines the notion of informed consent and perpetuates the illusion of control in digital environments (Bakos, Marotta-Wurgler, & Trossen, 2014).

C. Commercial Interests and Data Exploitation:

1) Role of Data as a Commodity:

In the digital age, personal data has become one of the most valuable commodities in the global economy. Companies collect and analyse vast amounts of data to gain insights into consumer behaviour, preferences, and trends, which they can then monetize through targeted advertising, personalized marketing, and other business strategies. This commodification of data has led to the development of sophisticated data mining techniques and the creation of data brokers who specialize in buying and selling personal information (Zuboff, 2019).

The Metaverse takes this commodification of data to new levels, as the immersive and interactive nature of these environments generates even more detailed and granular data about users. This data is highly valuable to companies, as it provides insights not only into what users do online but also how they think, feel, and interact with their environment. As a result, the Metaverse presents a lucrative opportunity for data exploitation, where user data is not just a by-product of digital interaction but a core component of the business model (Srnicek, 2017).

2) Business Models Based on User Data:

Many of the most successful digital platforms today are built on business models that rely on the collection and exploitation of user data. Social media companies, for example, offer free services to users while generating revenue through targeted advertising based on the data they collect. In the Metaverse, this model is likely to become even more prevalent, as companies seek to monetize the vast amounts of data generated by users' interactions in these immersive environments (Van Dijck, 2013).

However, this business model raises significant ethical and privacy concerns, as it incentivizes companies to collect as much data as possible, often at the expense of user privacy. The pressure to maximize profits can lead to the erosion of privacy protections and the exploitation of user data in ways that are not transparent or in the best interests of the user. This creates a conflict between commercial interests and the protection of individual privacy, further contributing to the myth of data privacy in digital spaces (Turow, 2017).

D. Regulatory, Ethical, and Technological Considerations

The current landscape of data privacy is shaped by stringent regulations like the GDPR and CCPA, which set the groundwork for protecting personal information. However, applying these laws to the Metaverse is challenging due to the immersive nature of the environment and the collection of complex data types like biometric information. Jurisdictional issues further complicate regulation, as the Metaverse spans multiple legal domains, making enforcement difficult. Ethical considerations demand that Metaverse creators prioritize user privacy, ensuring transparency, data security, and meaningful user control. Technological solutions such as encryption and decentralized identity management, alongside privacy-by-design principles, are essential for safeguarding data. Additionally, policymakers must update regulations to address the unique challenges of the Metaverse, focusing on transparency and real-time consent mechanisms.

VI. CONCLUSION

The Metaverse offers immense opportunities for innovation and social interaction but also presents significant privacy challenges. To ensure user trust and safety, it is crucial to balance innovation with robust privacy protections. This requires a combination of technological advancements, updated regulatory frameworks, and increased user education. By proactively addressing these challenges, we can create a secure Metaverse that fosters confident and safe user participation.

REFERENCES

1. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509-514.
2. Bakos, Y., Marotta-Wurgler, F., & Trossen, D. R. (2014). Does anyone read the fine print? Consumer attention to standard-form contracts. The Journal of Legal Studies, 43(1), 1-35.
3. Ball, P. (2022). The Metaverse: How will it change the world? Nature, 601(7894), 208-209.
4. Bennett, C. J. (2011). In defense of privacy: The concept and the regime. Surveillance & Society, 8(4), 485-496.
5. Brennan, P., & Kreiss, D. (2019). Digitalization and datafication: A conceptual overview and implications for data governance. Journal of Information Technology & Politics, 16(2), 124-140.
6. Buterin, V. (2013). Ethereum: A next-generation smart contract and decentralized application platform. Ethereum White Paper.
7. Calo, R. (2013). Digital market manipulation. The George Washington Law Review, 82(4), 995-1027.
8. Cavoukian, A. (2010). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada.
9. Cohen, J. E. (2019). Between truth and power: The legal constructions of informational capitalism. Oxford University Press.
10. Cuen, L. (2021). Decentraland vulnerability shows the risks of smart contracts. CoinDesk. Retrieved from coindesk.com.
11. Cummings, J. J., & Bailenson, J. N. (2016). How immersive is enough? A meta-analysis of the effect of immersive technology on user presence. Media Psychology, 19(2), 272-309.
12. Davidson, S. (2021). The Metaverse and virtual economies: The opportunities and challenges. Journal of Virtual Worlds Research, 14(1), 5-10.
13. Dionisio, J. D. N., Burns III, W. G., & Gilbert, R. (2013). 3D virtual worlds and the metaverse: Current status and future possibilities. ACM Computing Surveys (CSUR), 45(3), 1-38.
14. Dwork, C. (2008). Differential privacy: A survey of results. Proceedings of the 5th International Conference on Theory and Applications of Models of Computation (TAMC).
15. Floridi, L. (2013). The ethics of information. Oxford University Press.
16. Gellert, R. (2020). Data protection: From principles to practice. Routledge.
17. Hamilton, I. A. (2020). How Travis Scott's Fortnite concert ushered in a new era of virtual experiences. Business Insider. Retrieved from businessinsider.com.
18. Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. Information & Communications Technology Law, 28(1), 65-98.
19. Levy, S. (2020). Facebook: The inside story. Blue Rider Press.
20. Lyon, D. (2007). Surveillance studies: An overview. Polity.
21. Mattioli, D. (2020). The Privacy Paradox. The Wall Street Journal. Retrieved from wsj.com.
22. Meta (2022). Meta's Horizon Worlds: A platform for the future of the Metaverse. Meta Blog. Retrieved from meta.com.
23. Milgram, P., & Kishino, F. (1994). A taxonomy of mixed reality visual displays. IEICE Transactions on Information and Systems, 77(12), 1321-1329.
24. Mystakidis, S. (2022). Metaverse. Encyclopedia, 2(1), 486-497.
25. Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.
26. Nissenbaum, H. (2011). A contextual approach to privacy online. Daedalus, 140(4), 32-48.
27. Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review, 57(6), 1701-1777.
28. Schwartz, P. M., & Peifer, K. N. (2017). Transatlantic data privacy law. Georgetown Law Journal, 106(2), 115-181.
29. Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. NYU Law Review, 86(6), 1814-1894.
30. Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477-560.
31. Solove, D. J., & Hartzog, W. (2014). The FTC and the new common law of privacy. Columbia Law Review, 114(3), 583-676.
32. Srnicek, N. (2017). Platform capitalism. Polity Press.
33. Stein, S. (2022). Meta's data privacy challenges: Lessons from Horizon Worlds. TechCrunch. Retrieved from techcrunch.com.
34. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Penguin.
35. Tavani, H. T. (2020). Ethics and technology: Controversies, questions, and strategies for ethical computing. John Wiley & Sons.
36. Turow, J. (2017). The aisles have eyes: How retailers track your shopping, strip your privacy, and define your power. Yale University Press.
37. Van Dijck, J. (2013). The culture of connectivity: A critical history of social media. Oxford University Press.
38. Véliz, C. (2020). Privacy is power: Why and how you should take back control of your data. Bantam Press.
39. Voigt, P., & Von dem Bussche, A. (2017). The EU general data protection regulation (GDPR): A practical guide. Springer International Publishing.
40. Westin, A. F. (1967). Privacy and freedom. Atheneum.
41. Wright, R. (2022). Data breach in The Sandbox raises concerns about security in decentralized platforms. Blockchain News. Retrieved from blockchainnews.com.
42. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.
43. Zhao, L. (2021). The role of the Metaverse in redefining social interaction. Social Media + Society, 7(4), 1-13).