BIZCOMMUNITY

The metaverse and data privacy: Will regulation keep up?

By Ahmore Burger-Smidt

3 Dec 2021

On 28 October 2021, Facebook's CEO Mark Zuckerberg announced the rebranding of his company to Meta. More importantly, though, was the announcement of a new vision for Facebook or Meta which will see the metaverse succeed the so-called mobile internet.

Source: Unsplash

But what is the metaverse? The metaverse is a set of interconnected, always-on virtual environments that allow a person to effectively transcend the physical world. In essence, it is the convergence of physical, augmented and virtual reality in a live virtual world that is shared amongst users just as our existing physical world is shared amongst all of us.

The metaverse encompasses three key aspects:

Presence

Presence is the feeling of actually being in the metaverse which is achieved through virtual reality technologies such as head-mounted displays.

This means that a person, through the use of their avatar, can experience the feeling of being in the virtual space along with other people irrespective of where they might be in the physical world.

Interoperability

Interoperability is the ability to seamlessly travel between virtual environments using the same virtual tools or assets such as avatars. In other words, it is the ability of the individual to exchange and make use of information through the metaverse.

For example, individuals will be able to make use of blockchain technologies such as cryptocurrencies and nonfungible tokens to facilitate commerce in the metaverse.

Standardisation

Standardisation is the use of common technological standards for widespread adoption.

Meta aims to position the metaverse as the go-to place for various online activities including work, entertainment, education, commerce, and social interactions.

But from a privacy perspective, a number of concerns arise considering the metaverse and this cannot be ignored.

Privacy concerns in the metaverse

Facebook currently offers its services, mostly for free, to roughly 2.91 billion active users. In turn, it makes money by allowing businesses to advertise on its various platforms.

It is well established that Facebook makes the majority of its income from marketing (98% of its revenue).

This business model has not been without major privacy and security concerns, the most notable being the Cambridge Analytica scandal which resulted in a $5bn penalty (approximately R79.3bn) from the Federal Trade Commission in 2019.

The reason why so many businesses, political parties and governments go to Facebook for advertising is the fact that Facebook knows a lot about individuals/data subjects whether it be through Facebook itself, Messenger, Instagram, or WhatsApp. Data subject activity on these apps reveal a lot about behaviour such as whom data subjects communicate with, what content a data subject prefers and reacts to, and more. Facebook's algorithms can then build a profile of each user and categorise the users which creates a lot of value for a business seeking to advertise its products or services.

The metaverse - to boldly go where no retailers have gone before

Ryan McFadyen 3 Dec 2021

Consequently, the question beckons what that commercial exchange is going to look like in the metaverse and to what extent national regulators are going to be able to intervene, where necessary, on potential privacy issues.

It can be envisioned that a user that is connected to the metaverse will present a ripe opportunity for an even broader range of personal information to be collected at all times. It also presents an opportunity for more nuanced sets of information to be collected in comparison to what can be drawn from a user's interaction with a social media app. For example, the metaverse can a reveal a lot about one's biometric data, movements and gestures, reactions to certain situations and environments and other sensory data points.

The Protection of Personal Information Act, 4 of 2013 (PoPIA) has as one of its fundamental conditions openness. Openness requires that the data subject whose information a responsible party collects must be aware that the responsible party is collecting such personal information and the purposes thereof. In essence, the data subject must be afforded a reasonably transparent view into how, why, with whom, where and when a responsible party processes their personal information.

This is meant to provide the data subject with sufficient particularity to satisfy them as to whether the responsible party is engaging in lawful processing. If not, then the data subject has enough information to exercise their rights in terms of PoPIA.

Online activities that can now put you in prison

Ahmore Burger-Smidt 2 Dec 2021

An example of how important the openness condition is can be gleaned from WhatsApp's recent revision of its privacy policy. This came as a result of a significant data protection fine earlier this year. Following an investigation, the Irish data protection supervisory authority issued a €225m (approximately R4bn) penalty to WhatsApp for GDPR transparency infringements. This was the largest penalty handed down by the Irish Data Protection Commission and second-largest under the European Union.

It remains to be seen how open and transparent companies like Meta will be when it comes to informing data subjects about the information being collected and use thereof. It also remains to be seen how issues such as the lawfulness of processing will be worked around. Considering the unprecedented volume of personal information that will be opened up to processing through the metaverse, it will be interesting to see how further issues such as the reasonableness and minimality of processing will be satisfied.

Further, the metaverse can and probably will present cybercrime issues such as illicit data mining and identity theft.

Consequently, the question will be whether national regulators and governments are well equipped and prepared to deal with the abovementioned concerns. Although the issues themselves aren't new, the playing field is. As such, it will be interesting to see whether governments will be able to demonstrate the necessary digital resources and understanding to resolve the governance, content moderation and huge implications for privacy and data protection that new technologies such as the metaverse will inevitably present.

But more importantly, the question begs as to how data subjects i.e., individual users of Meta will demand their privacy and personal information to be protected.

ABOUT THE AUTHOR

Ahmore Burger-Smidt is renowned in her field for her deep experience, working as a Director across a number of practice areas - Africa; business crimes and investigations; competition; construction and engineering; healthcare and life sciences; media and communications; and technology. She extensively advises local and international clients on all aspects of regulatory compliance. She regularly undertakes compliance audits and oversees the implementation of compliance programmes including policy formulation and rollout, she is also the principle driver of the Werksmans risk assessment and e-learning tools as well as the co-leader of the Werksmans Dawn Raid Team. She has acted as advisor for several major telecommunications clients and has extensive regulatory expertise in compliance with numerous pieces of legislation.