Global Counsel

Regulating the metaverse

Blog post by Senior Practice Lead Conan D'Arcy, 19 January 2022

"The metaverse will present new markets and a range of different businesses. There will be a marketplace where someone may have a dominant position." The comment this week from European Commission Vice-President Margrethe Vestager marks a remarkable transformation in the metaverse from being a concept few in Brussels had heard of four months ago to an emerging priority in EU anti-trust scrutiny. Vestager's comment came before news broke that Microsoft was planning to acquire Activision Blizzard, the maker of Warcraft and Call of Duty. This is destined to accelerate and intensify scrutiny, not only of that particular acquisition but also the commercial plans of large tech platforms for developing the metaverse.

And while competition questions will be front and centre of initial scrutiny of the metaverse, in the longer-term governments and regulators will be as anxious about online harms, misinformation and illegal content and activity online, echoing today's debates over social media regulation.

The term metaverse originated in science fiction literature in the early 1990s and has been embellished by pop culture, from Iron Man and Spider Man's augmented reality (AR) glasses to the virtual reality (VR) worlds of Ready Player One. Most definitions relate to the ideas of virtual worlds and interactions built on VR and AR technology, often revolving around the use of avatars, but there is no consistent view of what the metaverse should be or will become. Commonly cited applications for the metaverse range from gaming and virtual worlds, to staff training and workplace interactions. Early movers in this space include Fortnite, which has a 'virtual rooms' feature, and VR social networks, such as Facebook Horizon and Microsoft AlspaceVR. The development of the metaverse is also not confined just to the tech sector, with 'real economy' companies like Walmart and Nike considering how to develop their customer offer through metaverse applications.

Taken together, this reinforces the observation of tech commentator Benedict Evans that the discussions about the metaverse are comparable to the "information superhighway" concept in the 1990s, which tried to predict what the internet would become. At that time, it was assumed by many that telecoms operators like AT&T would drive the internet revolution rather than start-ups like Google and Facebook. There is an open question of whether Big Tech's big bet on the metaverse will pay off or whether it will remain – as with gaming today – a notable but ultimately niche part of the digital market. This uncertainty poses challenges for anti-trust authorities to evaluate the significance of acquisitions of gaming or other metaverse companies. "We're trying to figure out how to ask the right questions" admitted Vestager.

In contrast, there is certainty that the metaverse will face unprecedented political and regulatory scrutiny early in its development. When Facebook re-branded and re-structured to create Meta, few commented on the announcement that Meta would create 10,000 jobs in Europe to work towards developing an "ethical" metaverse. This was a recognition that the next wave of digital

technologies will not be afforded a honeymoon period of regulatory forbearance like that enjoyed by the tech sector in the 1990s and 2000s. “Move fast and break things” is over and regulators and legislators will not wait nearly as long next time before intervening. It was also an acknowledgement that the regulatory backlash will likely be at its most intense in Europe, building on US tech’s experience of the ‘techlash’ and EU regulation like the General Data Protection Regulation (GDPR).

These insights were undoubtedly correct, though they have been accentuated by Meta’s own commercial intentions for the metaverse. In the mid-2010s, industry insiders in the ‘on-demand’ or ‘gig’ economy complained privately that they didn’t get a hearing because Uber had “nuked the landscape” for all other companies that followed. Other metaverse companies will no doubt be feeling similarly towards Meta, particularly as many fear Meta’s commercial plans may cut across the development of a de-centralised and open model for the metaverse.

Looking beyond competition policy, it is the ability to effectively supervise the metaverse which will likely prompt sleepless nights in government and law enforcement agencies. On social media and content-sharing platforms, the primary problem is the viral spread of written and audio-visual content, and how that content is shared in closed groups and messaging services, which are often encrypted. Virtual worlds and social networks within the metaverse are likely to face similar challenges and prompt a fresh debate about encryption. The Centre for Countering Digital Hate, which is prominent in debates around the UK’s Online Safety Bill, has launched a campaign that “the metaverse is not safe for kids”, accusing Meta’s VR Chat of being “rife with abuse, harassment, racism and pornographic content”.

But going beyond the current debate, the immersed nature of VR applications prompts a new wave of questions about harmful activity, not just harmful content. For example, to what extent is a crime, such as an assault, against an avatar comparable to crimes in the real world and what psychological impact will this have on virtual victims. For law enforcement, there could be challenges in tackling organised criminals, terrorist groups and sex offenders operating on metaverse platforms. Authorities will fear a scenario of a de-centralised metaverse with dozens of platforms, with many using both encryption and untraceable NFTs as their currency.

While Meta and other Big Tech companies will no doubt be the central target for scrutiny, it could instead be this de-centralised and open metaverse model – propagated by many in Silicon Valley – which prompts the greater regulatory challenge, should it emerge. While Meta and other large platforms may be distrusted by Europe’s policymaking community, at least policymakers have them as a clear target to regulate to tackle harms. In a decentralised metaverse that could be a whole lot harder.