Deloitte.

Regulating the Metaverse

Santa Monica is using an augmented reality game to promote its downtown shopping district

Introduction

Government and public sector applications of the metaverse are considerably less popular and less eye catching than the heavily marketed consumer-focused use cases, such as becoming a real-time character in a video game, enjoying courtside sports action from the comfort of home, or owning a song or sports highlight as an NFT.

But government and public sector agencies can serve their constituents and enhance operations in a plethora of new ways via the metaverse—immersive virtual experiences accessible via augmented reality, virtual reality, haptic devices, and other technologies—which will open the door to improved, equitable access to government services and public goods.

Providing essential services in the metaverse may reduce the burden on citizens and government employees. For example, several governments are exploring the metaverse's potential to impact their operations and constituents. The city of Seoul has pledged to invest 3.9 billion won ($2.96 million) in a new metaverse platform for managing civil complaints, monitoring public works through digital twins, providing access to virtual replicas of historical monuments, and hosting cultural events.[1] Meanwhile, the city of Santa Monica is using an augmented reality game to promote its downtown shopping district. Users can access an augmented reality experience through a mobile application where they can earn tokens by exploring a replica of the city's downtown.[2]

There are also significant opportunities for military, defense, and public health organizations to enhance operations through metaverse applications. Militaries could conduct training simulations and wargames, while medical professionals can get real-time assistance from specialists hundreds of miles away. Real-time monitoring using digital twins could extend the useful life of mission-critical equipment.

While the technology brings significant promise to public sector operations, there are still a few concerns. Several barriers stand in the way of wide-scale adoption, including user safety and access risks. Users will want assurance that the necessary guardrails are in place to protect their privacy, finances, and mental and physical health.

At this writing, governments have acknowledged the potential threats present in the metaverse but have not instituted regulations, technology standards, or protocols to define universal user safety mechanisms that are applicable across virtual world platforms. To date, virtual world developers have been policing their own platforms and have instituted several mechanisms, but these are primarily reactive and responsive, not preventative. Examples include virtual "bubbles" that prevent predators from encroaching on personal space or the ability to report hateful and malicious language. Some virtual worlds are experimenting with community-driven approaches that bring users together to vote on safety procedures and decide on punishments for endangering others.

Moving forward, governments must decide whether to intervene in establishing transitory universal regulation to protect virtual citizens across platforms. In the following sections, we explore what could go wrong, key issues and agency stakeholders that could play a role in regulating the metaverse, and lessons learned from government intervention in the roll-out of similar paradigm-shifting technologies.

3.9B₩
($2.96M)
metaverse investment pledged by the city of Seoul

Understanding metaverse challenges

Dr. Thomas Furness, a pioneer in immersive technology, asserts that virtual reality experiences more closely resemble real-world experiences than social media or gaming platforms. He says the lack of separation between users and virtual spaces causes these experiences to be "drawn on the brain in permanent ink."[3] MRIs back this claim, demonstrating that people recall virtual, immersive events similarly to real-world events. The sense of realness makes for a more significant impact of trauma in virtual worlds since the lines between physical and digital are blurred.

Here are a few examples of how the metaverse could be misused:

What can go wrong?

The electronic health records of a patient visiting her doctor in the metaverse are hacked and leaked online by malicious users.

In a metaverse chat room, a user is verbally abused by others using derogatory and malicious language.

A metaverse user is targeted by malicious artificial intelligence in an elaborate phishing scheme and persuaded to send money to a cybercriminal.

A heavy metaverse user falls ill after keeping her virtual reality headset on for three days and forgetting to eat and drink.

A small artist selling artwork as NFTs in the metaverse realizes his work has been copied without his consent, and others are profiting from his IP.

A virtual landowner is devastated to discover that the virtual world developer has released a patch to the game that alters the layout of the virtual city without seeking consent, significantly impacting the virtual property value.

In addition to safety concerns, equitable access to the metaverse is another issue. Fully featured VR headsets still cost hundreds of dollars and are not yet affordable or available for every household.

Today, although multiple virtual worlds are open to the public, it is unclear who will be held accountable for protecting the safety of metaverse citizens and corporations doing business within their virtual borders.

Key issues and federal regulatory agencies

Metaverse interactions require a variety of technologies and technical components to create an extended and immersive reality, including hardware (e.g., servers to provide computing power and storage), software (e.g., platforms for building virtual worlds or for users to register, etc.), and peripherals for immersion (e.g., VR glasses, haptic tools, etc.).

In other words, the metaverse results from the convergence of multiple technologies, which introduces many potential risks and legal issues.

The constantly evolving nature of the metaverse complicates regulation. Current metaverse platforms—walled-in gaming or community-driven ecosystems—might offer pockets of issues that certain regulatory agencies could address. Still, a future decentralized and hyperconnected virtual world with its own internal economy raises new regulatory challenges. While there is no consensus on what to regulate, the general sentiment within the technology industry is that rules and enforcement mechanisms should be established. Governments should consider taking the possibilities presented by the future of the metaverse seriously, considering the risks and opportunities in the short and long term.

Telecommunications and connectivity

At its core, the metaverse is about connecting in the digital realm. Relevant elements of regulating telecommunications, technology, and carriers are under the Federal Communications Commission's (FCC) jurisdiction. But once users interact in virtual worlds, what happens when someone virtually "breaks the law?" Cyberbullying and image-based abuse on most communication and interaction platforms are relatively common; however, the metaverse may carry an increased risk of financial crimes due to the monetary value of items such as NFTs.

If developers or platform owners don't reprimand offending parties, is there any recourse to victims? For avatars to be held accountable for crimes, they would need to be treated as either their own legal digital personas or as an extension of the physical user by governments or law enforcement agencies, which raises its own concerns. From this perspective, the FCC's mandate would fall short of enabling the "policing" of individual interactions.

Data, privacy, and cybersecurity

Metaverse users provide multitudes of data points to the companies that own each metaverse platform. The collection, use, and transmission of personal data is an area of fragmented regulation. While several states have begun to codify what companies can and cannot do with user data, the U.S. does not have a singular federal data protection agency to regulate or enforce responsible use of all types of data.[4]

The danger of the status quo is that data mining provides excessive power over personal information—including financial, biometric, and health data, among others—to companies that may not place privacy or protection of information at the center of their operations. And without a federal privacy law specific to the metaverse it may be difficult for users to establish a clear understanding of the data points that are being collected and the privacy rights that apply.[5]

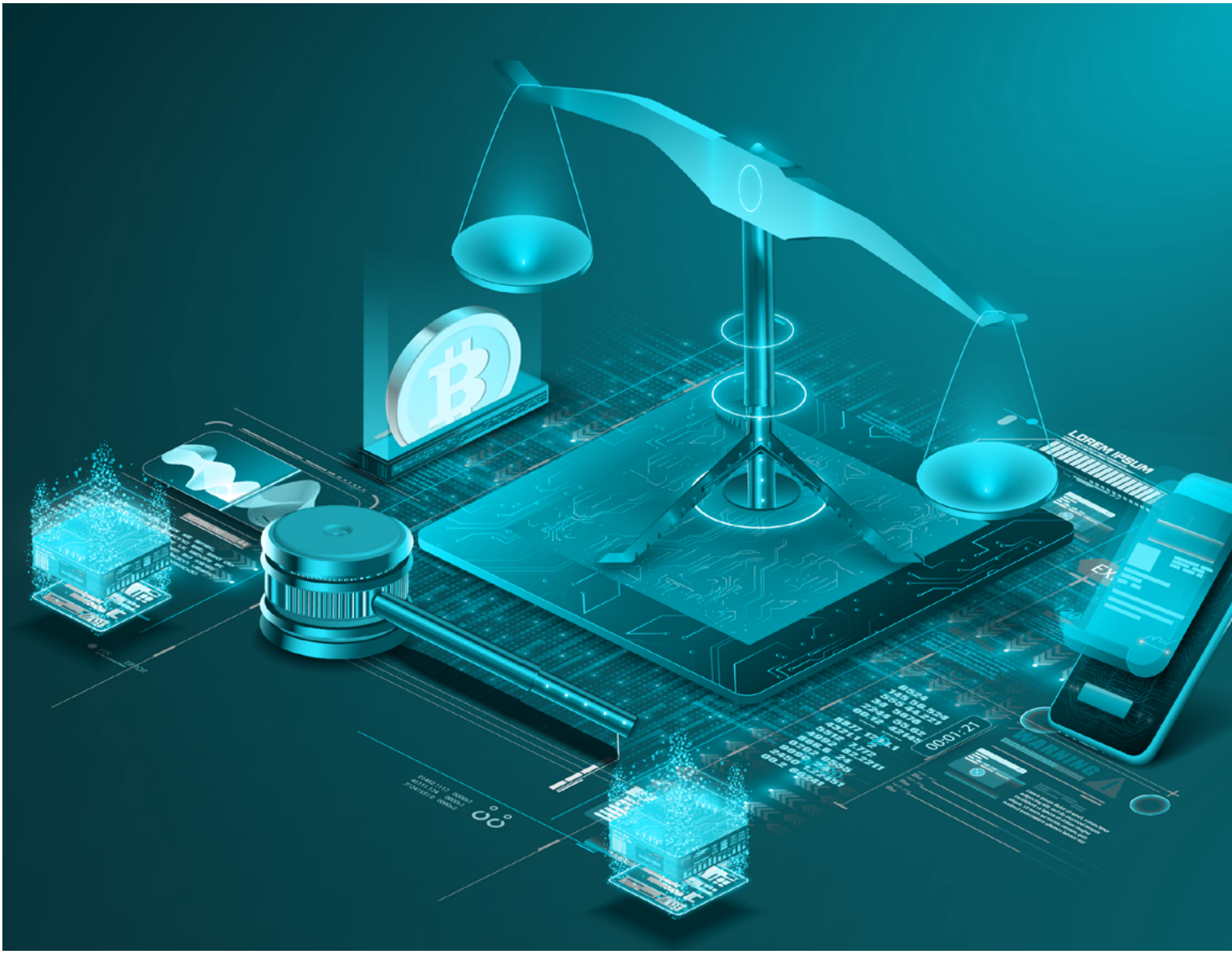
Similarly, the current enforcement of cybersecurity regulations is nebulous at best—users trust that companies developing metaverse platforms and applications maintain robust information security protections. Still, rulesets or guidelines for defining data protection expectations do not exist. Very few examples exist of governments holding companies or individuals accountable for data breaches and exposure. And businesses and federal agencies could potentially face threats from sophisticated domestic and foreign adversaries targeting data.

Commerce and marketplace

Multiple interrelated economic issues are at play in the metaverse because transactions can take place in both fiat and cryptocurrencies. In the future, the metaverse could present new ways to exchange digital and physical assets, create employment, process payments, or deliver services. However, the current state of regulation for the digital economy in the metaverse is nascent; consumers could question the safety of new financial instruments such as cryptocurrencies and NFTs because regulation of them is constantly in flux.

The legal status of cryptocurrencies—are they securities or commodities? —is still unclear and will likely have significant implications on investor protection. Classifying cryptocurrencies as securities would subject them to greater regulation promoting price transparency and market efficiency, among other regulations and laws.[6] In June 2022, the Responsible Financial Innovation Act was introduced as a bipartisan framework for classifying most cryptocurrencies as commodities, with certain exceptions worthy of the security designation.[7]

Several regulatory and enforcement agencies are critical stakeholders in metaverse regulation. The Federal Trade Commission (FTC)—with jurisdiction over antitrust enforcement, unfair and deceptive acts, and consumer protection—will play an essential role in regulating companies doing business in the metaverse. And from a transactional perspective, the Securities and Exchange Commission (SEC) will continue to be responsible for enforcing securities laws and regulations and oversight of banking, money transmission, and commodities—particularly if courts define digital currencies as specific types or classes of assets. The distinction between securities and commodities would have trickledown effects for consumers on matters such as income, sales, property tax, theft, and distribution, which may require the oversight of other governing bodies.



Lessons from the Past

From the progression of Web 1.0 to Web 2.0 and an always-connected mobile internet, governments often take reactionary measures to rectify issues that have emerged alongside internet technology development.

That's because technological innovation (and subsequent societal impact) is typically hard to predict, and innovation often outpaces the law. As a result, we've witnessed a drawn-out game of internet problem whack-a-mole, where one issue is addressed only to be quickly replaced by a new one. "This is the equivalent of trying to put your fingers in a sieve and stop the water flowing out; it's impossible," says Gregor Pryor, a UK-based digital media lawyer and intellectual property expert.[8]

The metaverse will likely present many of these same dynamics. Issues of the past 25 years of internet development could be amplified and rehashed in the metaverse, and new problems are almost guaranteed to emerge. As the metaverse continues to evolve, considering past events and rulings can help better understand the challenges and solutions governing bodies will face when regulating the metaverse. In the following section, we explore some specific examples.

Section 230

In the early years of the internet, the judicial system struggled to apply existing laws to internet communication. That changed in 1996 with the passage of Section 230, an amendment to the Communications Act of 1934 that became the *de facto* law of the land governing online communication.

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider
>
> **-47 U.S. Code § 230[9]**

Section 230 protects internet providers and users from liability of others' posts on the internet and allows platforms to remove objectionable content as necessary. The FTC and FCC are responsible for enforcing Section 230.

Section 230 encouraged internet development without the fear of liability from third-party users, yet this freedom has led to the proliferation of bad actors and harmful content. Hosting platforms can police user content, but these efforts are often construed as overreaching censorship initiatives. Alternatively, if a platform doesn't do enough to moderate content, it can be considered complicit.[10]

Platforms on the metaverse will continue to be impacted by Section 230. Some are calling for change to the policy or even wholesale repeal. In April 2022, former president Barack Obama called for the reform of Section 230 to curb harmful political misinformation, calling the current internet a breeding ground for "humanity's worst impulses" and implying that Section 230 is to blame.[11]

As legislatures weigh the pros and cons of Section 230 reform, metaverse development hangs in the balance. Will the metaverse be allowed to grow under the laissez-faire rules of decades past, or will policymakers move toward more regulation? Without the assurances of Section 230, it's hard to imagine how social platforms of Web 2.0 would have been able to flourish. The expanding metaverse will have to overcome a significant hurdle if these protections are removed.

FCC broadband requirements

The Telecommunications Act of 1996 empowered the FCC to define a minimally viable broadband speed to meet the average consumer's needs and determine if this defined broadband speed was being met throughout the country. If these needs are not being met, the FCC can take immediate action—including "price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment."[12]

The current FCC minimum broad speed standard—25Mbps download / 2Mbps upload— was originally established in 2015 and has been criticized as not being high enough to meet the bandwidth requirements for today's digital interactions and proliferation of connected devices. By the FCCs own guidelines, "moderate" internet usage of 4 connected devices needs more than 25Mbps for consistent performance, and the average American household has over ten connected devices.[13]

A growing metaverse will only further exacerbate the problem. For example, if virtual reality is needed to engage with the metaverse fully, accessibility to high-speed broadband will be paramount. In standard definition, entry-level video streaming in virtual reality requires a stable connection of 100Mbps with 30ms latency.[14] For high-definition resolution, a 400Mbps connection is needed.

In addition, VR motion sickness is caused, in part, by latency issues.[15] If the metaverse is to become the primary means of online interaction, all households must have access to the broadband infrastructure necessary to support higher internet speeds.

The federal government has acknowledged the gap in the existing standard and has raised the speed requirements for new federally backed broadband infrastructure initiatives. For example, the National Telecommunication and Information Administration (NTIA) Broadband, Equity, Access, and Deployment Program (BEAD) requires all funded projects to reach a minimum of 100Mbps download / 20Mbps upload. The precedent being set by peer agencies may provide further justification for the FCC to raise the metrics for minimum broadband speeds and, if required, take actions to rectify the issue to help improve connectivity across the country.[16]

Metaverse monopolies

With the metaverse in its early stages, it remains to be seen how the different platforms and providers will interoperate. A variety of platforms may maintain popularity, and metaverse users will be able to operate and interact across these different "worlds" and experiences. Alternatively, we could witness metaverse userbases merge into a few large platforms.

A sizable portion of today's internet traffic flows through a few prominent players,[17] incumbent tech companies that control the lion's share of daily internet users. The same can be said for the smartphone market, where a few companies dominate the market share of mobile internet access devices. This has spurred debate about monopolies and anti-competitive practices. In the recent past, these debates have typically played out in the courtroom, with various companies challenging each other over anti-competitive practices. With the advent of the metaverse, such legal battles are likely to persist and may warrant targeted legislation to curb anti-competitive practices. In addition, an ambitious presidential executive order issued in 2021 empowers many federal agencies to enforce antitrust laws and has placed technology companies' business practices and acquisition practices under federal scrutiny.

Net neutrality

Net neutrality is the principle of common carriage that ensures that internet service providers (ISPs) do not favor, throttle, or charge different rates for content transported on their infrastructure. As the metaverse becomes a key platform for individuals to interact virtually, net neutrality will help facilitate and ensure equal access to the metaverse.

The FCC repealed net neutrality in 2017, although previously, the agency had been generally supportive of the concept. At this writing, the status of net neutrality is in flux. Recently proposed Congressional legislation could enshrine net neutrality into law and give the FCC the authority to regulate internet traffic and revisit ISP net neutrality practices.

Data privacy and security

The 2020 IoT Cybersecurity Improvement Act established minimum security standards for internet of things devices owned or controlled by the federal government,[18] and the National Institute for Standards and Technology (NIST) has developed cybersecurity recommendations for IoT device manufacturers.[19]

These new acts and standards require organizations developing metaverse technology devices to abide by IoT regulations when used for government applications. Additional regulations may be needed to further adapt to the applications of metaverse technology devices and the subsequent security assurances.

Concluding thoughts

As metaverses grow and iterate, it is still unknown which, if any, metaverse platforms will become the de facto winner. Vendors are continuing to enter the race bringing new hardware, software, and protocols to market, and it is still too early to tell who will become the major players. The government will likely play a critical role in the metaverse development, and vendors will be keeping a watchful eye on any new regulations as they pertain to their growing industry. Still in their infancy, metaverse technologies will likely go through major iterations and changes over the coming years, and it will be the role of the government to keep up with that change of pace to ensure an equitable, neutral, and safe environment for all to participate in.

For the vendors in the space, competition will promote new value offerings for all users, which is a welcome side effect of the fast-paced advances the industry is currently seeing. The government has the opportunity to promote this competition and it is likely in the best interest of users and developers to establish the necessary guardrails for the metaverse now, so that they can have an equal chance at building the next best metaverse.

Regulating the metaverse is likely to cause several large challenges for the government. From financial fraud to cyber harassment to monopolies, it is clear that the government will have no shortage of difficult decisions regarding new laws and regulations over the next several years. However, the early days of the internet are not such a distant memory and serve as a useful analog. In the early 2000s, the blossoming of the internet resulted in an explosion of opportunities that completely disrupted the way everyday business was conducted. If metaverses are to provide a similar level of opportunities, how might the government act differently and become more of a partner of growth rather than just a regulator? We are eager to see how this plays out and where government organizations decide to establish their virtual presence. The entire industry is keeping a close eye on how the government will participate in the next great wave of technological advances.

End Notes

1. Jonathan Keane, "South Korea is betting on the metaverse - and it could provide a blueprint for others", CNBC, May 30th, 2022.
2. Decerry Donato, "Santa Monica is using the metaverse to gamify its shopping district", dot.LA, December 13th, 2022.
3. Brittan Heller, Carr Center for Human Rights Policy Harvard Kennedy School, Spring 2020.
4. Thorin Klosowski, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)". New York Times Wirecutter, September 6th 2021.
5. Andrea Vittorio, "Metaverse Technology Opens Up a Wider World of Privacy Concerns", Bloomberg Law, August 30th, 2022.
6. Skylar Wu, "SEC v. Ripple: The Regulation of Cryptocurrencies as Securities", Columbia Undergraduate Law Review, January 19th, 2022.
7. Deanna R. Reitman, Margo H. K. Tank, "How the Responsible Financial Innovation Act proposes to regulate cryptocurrencies and other digital assets – commodities perspective", DLA Piper, June 23rd 2022.
8. Salamander Davoudi and Maija Palmer, "File sharers sentenced to prison", Financial Times, April 17th, 2009.
9. "47 U.S. Code § 230 - Protection for private blocking and screening of offensive material", Legal Information Institute.
10. Casey Newton, "Everything you need to know about Section 230", The Verge, December 29th, 2020.
11. Isobel Asher Hamilton, "Barack Obama said social media is 'turbocharging some of humanity's worst impulses' and called for reform to Section 230" Business Insider, April 22nd, 2022.
12. "47 U.S. Code § 1302 - Advanced telecommunications incentives", Cornell Law School.
13. Federcia Laricchia, "Average number of connected devices residents have access to in U.S. households in 2020, by device", Statista, June 1st, 2022.
14. Simone Mangiante, Guenter Klas, Amit Navon, "VR is on the Edge: How to Deliver 360°Videos in MobileNetworks", Research Gate, August 2017.
15. Eunhee Changa, Hyun Taek Kim, Byounghyun Yoo, "Virtual Reality Sickness: A Review of Causes and Measurements", Tandfoline, July 2nd, 2020.
16. Amy Huffman, "NTIA Releases Requirements for $42.5B of BEAD Funding: Here's What It Says About Digital Equity", National Digital Inclusion Alliance, May 13, 2022.
17. J. Clement, "Most popular websites worldwide as of November 2021, by total visits", Statista, March 22nd, 2022.
18. "H.R.1668 - IoT Cybersecurity Improvement Act of 2020", Congress.Gov, December 4th, 2020
19. "Foundational Cybersecurity Activities for IoT Device Manufacturers", NIST, Computer Security Resources Center, May 2020.

Deloitte.