



HARVARD Kennedy School

MOSSAVAR-RAHMANI CENTER
for Business and Government

Who Will Make the Rules for the Metaverse?

Tom Wheeler
Harvard Kennedy School

November 2022

M-RCBG Associate Working Paper Series | No. 195

The views expressed in the M-RCBG Associate Working Paper Series are those of the author(s) and do not necessarily reflect those of the Mossavar-Rahmani Center for Business & Government or of Harvard University. The papers in this series have not undergone formal review and approval; they are presented to elicit feedback and to encourage debate on important public policy challenges. Copyright belongs to the author(s). Papers may be downloaded for personal use only.

Who Will Make the Rules for the Metaverse?

By Tom Wheeler

EXECUTIVE SUMMARY

The future of online platforms is a pastiche of the digital platforms we know today – Facebook, TikTok, YouTube, etc. – enhanced by virtual reality, artificial intelligence, and a chilling expansion of the invasion of personal privacy. Called the metaverse (a term combining “meta” meaning “transcending” and “universe”), the new platforms create a video game-like pseudo-world – this time, however, it is no game, but personally identifiable avatars interacting with each other. The internet platforms we have experienced thus far have been an observational experience that principally harnessed text and video. The metaverse is an experience of participatory immersion in which real world people, problems, and patterns come to life.

The metaverse brings the promise of new tools for education, entertainment, medicine, and commerce. At the same time, it imports the problems associated with the current digital platforms while creating a host of new issues as well. We have yet to successfully deal with the problems created by the current digital platforms; the metaverse should be the impetus to rectify those abuses while getting in front of the challenges to come.

We are told the metaverse is years away, giving us time to figure out how to deal with its ill effects while encouraging its positive features. Failure to develop meaningful policies now - on an international basis - however, will mean we did not learn the lesson of the last multiple decades of internet exploitation by a handful of companies and how the companies write their own rules at the expense of the public interest.

The online challenges with which we wrestle today, such as privacy, competition, and misinformation, will be supercharged by the intrusive, immersive, individually identifiable, and manipulative nature of the metaverse. On top of this, the metaverse expands the problems

inherent in unsupervised online communities such as harassment, manipulation, personal safety and the safety of children.

The problems created by the digital platforms of today were, for the most part, an unexpected surprise. We cannot claim such innocence about the metaverse. The experience with social media is a warning about what happens when public interest expectations are not part of digital innovation, when “build it and be damned” is the rule. Policy makers need to come to grips with – preferably get ahead of – the new technology with focus equal to those who are creating the new challenges.

An advertising campaign by Meta Platforms, Inc. (the former Facebook) promises, “The metaverse may be virtual, but its impact will be real.” That reality is barreling down on us now. Now is the time to deal with the public interest issues the metaverse raises.

FROM SOCIAL MEDIA TO SOCIAL VIRTUAL REALITY

The United States has failed to control or mitigate the adverse effects of online digital platforms. The next online innovation – the metaverse – will reinforce these old problems while launching an expanded collection of new challenges.

The move from the internet we know today to the metaverse is a transformational move from observation to participation. Today’s online activity began as an observational experience that gradually expanded through social media and online games to become more participatory. The metaverse accelerates that expansion utilizing virtual reality (VR), augmented reality (AR), and artificial intelligence (AI) to create an immersive 3-D first person experience that puts the user “inside” a new pseudo-world.

We are moving from social media to social virtual reality without a plan.

But we are told by its proponents not to worry, that the full realization of the metaverse is still a long time off. That very well may be true, but that cannot be a reason to delay dealing with its

challenges. Early metaverse services are a reality. Billions are being spent by the dominant digital platforms to further expand the capabilities of the metaverse. We the public – acting through our government – cannot stand idly by as the pseudo-world begins to redefine our real world.

When asked by a reporter what his company was doing “to ensure the problems of today’s internet don’t carry over into – or, worse, get amplified by – the metaverse,” Mark Zuckerberg, Meta CEO and metaverse evangelist, responded, “We have some time to try and work some of this stuff out up front.”¹

No, we don’t have time.

Gartner Research forecasts that by 2026 – that’s less than four years away – one-quarter of the population will spend at least one hour per day in the metaverse.² Even if the Gartner research is optimistic (as some reports seem to indicate³), the clock is ticking. The companies that hope to profit from the metaverse are charging ahead. The effects of the metaverse on individuals and the public interest will be determined by who uses the next few years better: those with private interests, or those concerned about the public interest.

The evolution from social media to social virtual reality is upon us. We must reverse the experience of digital pioneers charging ahead to exploit the capabilities of technology without considering the consequences, and then acting surprised about the adverse effects they created. Now is the time to get in front of the coming transformation to assert the role of the public interest and societal norms...before it is once again too late.

An Existential Question

“Move fast and break things,” the Silicon Valley mantra coined by Mark Zuckerberg in the early days of Facebook, has found a new application in the metaverse. To “move fast” is essential in the metaverse strategy – as it was in the original internet strategy – to define corporate behavior before the public fully understands the consequences. The “things” that are broken are not physical objects, but the societal and economic norms that have previously provided stability.

Both the public and policymakers were caught unprepared by the internet and platforms such as Facebook, YouTube, Twitter, Google, Amazon, and others. The “move fast” blitzkrieg of new products, services, and convenience allowed the companies to make their own behavioral rules. The profits generated by those self-serving rules then financed public relations and lobbying campaigns opposing the imposition of public interest-oriented regulation.⁴

Whether the metaverse will be a replay of the companies’ making their own rules is the internet’s new existential question. We have learned from experience that adverse consequences result from self-serving corporate decision-making. We have not, however, learned how to regulate in the “move fast and break things” world.

The appearance of the metaverse has created both the incentive and the opportunity to reclaim the public interest to determine what we want in our digital future.

Old Problems Expanded and New Problems Created

“The Metaverse will also render more acute many of the hard problems of digital existence today,” Matthew Ball observed in *The Metaverse: And How It Will Revolutionize Everything*.⁵ Whether the metaverse’s amplification of today’s online problems is the force that finally galvanizes public policy makers to address the ongoing digital policy gauntlet remains to be seen. What is not in doubt, however, is how the metaverse will metastasize the problems of digital privacy, competition, and misinformation beyond our current experience.

Privacy – Today online platforms combine user information such as location, interaction with other users, and online usage patterns into cohorts of users with similar characteristics. The metaverse will expand the tracking of users to include personal biometric data, and apply that information to individuals, not just groups. Biometric data such as eye movement reveals our emotions and can be used to influence behavior. And because metaverse avatars will have personal identities, user identification will move from grouping into cohorts to the specific identification and authentication of individual users.

Competition – Today a handful of companies are gatekeepers that dominate the online world. These companies control vast amounts of the data necessary for the metaverse to operate. The companies’ high margins in their current business allow them to extend their dominance, including through the acquisition of potential metaverse competitors.

Misinformation – Today online technology has automated the distribution of untruths, hate, and propaganda. The metaverse will have the capability to bring such information to life by inserting each user into a world that measures their emotions and uses that information to manipulate behavior. Inventing a new world does not absolve those building the metaverse of the responsibility over abuse in the world they are creating.

Beyond how the metaverse expands and exacerbates such traditional digital abuses, it also expands the potential for other abuses.

Harassment – Social media today is a vehicle for harassment in words and images. When individuals “step in” to the metaverse they expose themselves through their virtual representation to new levels of physical, verbal, and sexual harassment.

Safety – Concerns about the safety of children on today’s digital platforms are well documented. The metaverse will invite those same children – along with potential predators – into a virtual world with increased ability to manipulate their emotions.

Digital Chasm – The digital divide of haves and have nots has been a long-running challenge of the internet. Beyond current issues of economics and availability, early experiences with artificial intelligence (AI) have raised discrimination concerns. With AI as the engine of the metaverse, such biases could move us from a digital divide to a digital chasm.

Fraud – Today’s online world is built on advertising. The new business opportunity of the metaverse is real time transactions involving everything from virtual real estate to virtual clothing. Accompanying these transactions is the opportunity for virtual world fraud.

Larceny – The ownership of virtual goods creates the opportunity for theft of those goods.

Will Privatized Governance Continue?

Thus far in the internet age the dominant companies have privatized governance and made their own behavioral rules free of much effective governmental oversight. Too often, public policy makers' lack of technological understanding has been exploited to promote a fear that regulation will break the magic of the tech innovators.

As we consider the effects of a multi-decade lack of oversight of the activities of digital companies it is imperative to reassert a role for public interest oversight of digital private interests. Such a prioritization becomes even more urgent as we watch the unsupervised creation of a new virtual world with unprecedented powers.

We may have been technologically naïve and surprised by the new world the digital revolution ushered in and, as a result, lulled into giving the digital companies free rein. But we have no such excuse this time.

Now is the moment to decide about the kind of digital world in which we want to live. The metaverse will – like the digital platforms that preceded it – deliver wondrous new capabilities. The development of such capabilities must be encouraged and expedited, but not at the cost of trampling the rights of individuals and the public interest. The coming metaverse gives us the opportunity to both rectify the abuses of the early internet era while getting in front of the changes to come.

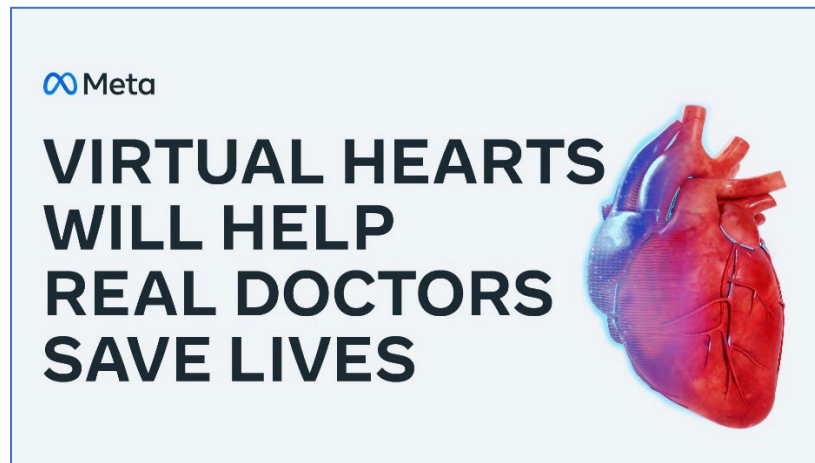
METaverse WONDERS AND WOES

Mark Zuckerberg has described the metaverse as “an embodied internet that you are inside of rather than just looking at.”⁶ Being immersed in an unreal world will bring with it both amazing new capabilities and frightening new threats.

Metaverse Wonders

Meta Platforms, Inc. (the renamed Facebook) has been the champion of promoting the metaverse and its wonders. Its advertising campaign to promote a benign explanation of the metaverse proclaims “The metaverse may be virtual, but its impact will be real.”⁷

“Imagine how a surgeon could train,” one of the ads asks as video shows a medical student bending over a virtual patient. “A surgeon will one day be able to practice virtually as many times as needed before laying her hands on a real patient.”⁸ It is a message reinforced in print advertisements.



In another commercial, the camera pans across a lecture hall to promote the value of the metaverse to education. “One day, this lecture hall will be made of code,” it promises. Switching to a scene from the Roman Forum the ad explains, “These students aren’t really back in 32 BCE, but they can still watch Mark Antony debate in ancient Rome.”⁹

How we work will also be changed by the metaverse. “Boeing wants to build its next airplane in the ‘metaverse,’” Reuters reported.¹⁰ Farmers will utilize the metaverse to improve crop yields, a Meta commercial promises.¹¹ Meta’s 2022 Connect conference heavily promoted the metaverse in business.¹²

Beyond its application in traditional businesses, the metaverse will create a whole new economy, just like the internet did. New companies, new jobs, and new job descriptions will

come into being to build and manage the metaverse. One research group called it “tech’s next trillion-dollar opportunity.”¹³

With economic growth and wonderous new capabilities – what’s there not to love about the metaverse?

More Powerful than a Lie Detector

The metaverse is a world of expanded surveillance. That this new surveillance is being developed by the same companies that have already trampled personal privacy should be of concern.

When the world’s leading neurologists assembled in Seattle in June 2022 for a Symposium on Eye Tracking Research and Applications, sponsors included Google and Reality Labs, a division of Meta Platforms.¹⁴ The companies that have set out to build the metaverse have taken an interest in neurology because of the insights it provides into human behavior.

Poets say the eyes are the window into a person’s soul. Neurologists are less romantic. Neurological studies have found that eye movements can reveal our thought processes.¹⁵

Thus far in internet history, the digital platform companies have collected previously private information about each of us by tracking keystrokes, mouse clicks, or location coordinates. That all changes when consumers don virtual reality headsets to access the metaverse and thus open the door to the collection and manipulation of even more powerful biometric information.

Today, the metaverse requires a bulky headset over your eyes. Tomorrow it will be lightweight glasses and eventually contact lenses. These devices are designed to harness virtual reality (VR) and augmented reality (AR) to deliver users to the metaverse. Influencing the user’s actions in the metaverse will be the devices’ ability to read physical cues and turn them into data for artificial intelligence (AI) algorithms. Eye movements, heart rate, facial expressions, even perspiration will create new data points to be measured, then manipulated in the metaverse in order to be monetized in the real world.

The companies' interest in neurological research is, therefore, quite understandable. After all, it was these same companies that relied on psychological research to design their current products.¹⁶ Using psychological studies of casino gambling behavior, social media companies copied techniques that kept people at slot machines. The goal was to similarly make the online experience as addictive as possible. Playing off human psychology to get users to stay online for as long as possible allowed the platform companies to both sell more advertisements and collect more information on each user.

Harnessing neurological patterns can be even more powerful. Research shows that understanding how to interpret eye movements creates data that can be used to manipulate behaviors. One study even demonstrated how eye-tracking can be exploited to influence the moral decisions people make.¹⁷

Metaverse devices able to collect personal information from our bodily functions are a potent new tool for the digital companies. Meta Platforms has already patented technology to build eye tracking and facial movement tracking into the equipment used to access the metaverse.¹⁸ All of this means that putting on metaverse gear will have more far-reaching and revealing results than hooking up to a lie detector.

POLICY OVERSIGHT OR PERFORMANCE ART?

Mark Zuckerberg has observed that the metaverse will require “new forms of governance.”¹⁹ Now, while the metaverse is relatively rudimentary, is the time to get in front of the new issues it raises and, in the process, tackle the platform problems that have long bedeviled us. We are being told, however, to chill, that the time necessary for the development of the metaverse will give us time to resolve the problems it creates.

History, however, teaches us the opposite is true. The establishment of digital norms is a matter of getting there first. Once new digital patterns are established, they are difficult to correct.

We Have Seen This Play Before

For the past few decades, we have all been the audience in a performance presented by the dominant digital platform companies. Their new services have been amazing while some of the consequences of their behavior have been appalling. As companies revise their business plans for the metaverse we are witnessing a reprise of the old performance.

In Act One, visionary innovators imagine what the wonders digital technology can deliver and then bring it to life. The hype and hustle surrounding the metaverse recycles the “move fast and break things” mantra of the early internet. The focus last time was on what can be built rather than consideration of its consequences – should we expect anything different this time?

Act Two was the refinement of the technology’s application. By marrying computer science with behavioral science such as the casino psychology research, the platform companies were able to design applications to maximize their monetary potential. Today’s reprise moves beyond psychological science to embrace neurological science. One commentator has called out the “Three M’s of the Metaverse” – monitor users, manipulate users, and monetize users.²⁰

The unfinished Act Three features governments trying to keep pace with how the tech companies race ahead to establish their own behavioral rules. In the United States policymakers have stumbled around trying to determine what actions (if any) to take. Across the Atlantic, the European Union and the United Kingdom have moved forward to establish new rules for the internet we know today.

The challenge society now faces is determining whether there will be a stage manager for the new activities. Not a director that dictates, but a supervisor that coordinates what is needed for the performance and its effect on the audience. Will the metaverse companies put their own stage management in place for the metaverse just like they did for their internet platforms? Or will the governments that were slow on the uptake in the early generation internet see the vast new developments of the metaverse as the trigger to assert themselves?

The Clegg Manifesto

The loudest voice touting the metaverse seems to be Meta Platforms, Inc. This does not mean that other dominant digital platforms are not also hard at work, simply that one company is outspoken (and as such features prominently in this discussion).

In mid-May, Meta Platform's President for Global Affairs (and former Deputy Prime Minister of the UK) Sir Nick Clegg published a lengthy discussion about the metaverse.²¹ Sir Nick's over-eight-thousand-word manifesto was a kind of *Das Kapital* of the metaverse – the theoretical underpinning of a new economy.²²

In building that new economy, Clegg observes, "Companies like Meta have lots of work to do both to build the credibility of the metaverse as an idea, and to demonstrate to people that we are committed to building it in a responsible way." Truer words were never written.

Only a few sentences later, however, the focus of the manifesto is redirected to the responsibility of others. "There is nothing deterministic in the way a technology impacts society," Clegg wrote. "Technology isn't good or bad in and of itself. People will use it as they see fit – and people will misuse it as well. Just as we have seen how problems in our physical society have manifested on the internet, they will reoccur in any system or platform regardless of what it is or who builds it." Of course, this is true, yet it is the design decisions of those who develop and manage the technology that creates the opportunity for misbehavior that could potentially be mitigated by early intervention.

The recognition that "people will misuse" the metaverse has opened the window to a discussion to identify and attempt to mitigate the potential for such misuse. Mr. Clegg perceptively and correctly observes, "This is why we must create thoughtful rules and put guardrails in place as the metaverse develops to maximize its potential for good and minimize the potential harms."

Step One in developing such rules begins with the dialog the Clegg Manifesto has initiated and the identification of issues to be addresses up front. The full realization of the metaverse may be years off, as Mr. Clegg's boss has suggested, but we are already speeding down its on-ramp.

Waiting until we are ensconced in the metaverse before dealing with the issues it raises is a fool's errand.

The rapidly evolving and expanding metaverse makes manifest the need to quickly develop meaningful policies, not simply window-dressing. The effort to create metaverse rules cannot be a rerun of the Facebook advertising campaign that loudly proclaimed, "We support updated regulations on the internet's most pressing challenges" while offering hollow solutions to important problems.²³

Nick Clegg is correct, "Guardrails need to be put in place to mitigate the risks and accentuate the positive." This invitation to develop metaverse oversight should be embraced by both the companies, policymakers, and public interest advocates. The debate cannot be whether there should be regulatory oversight, but the specific goals for and implementation of such oversight.

META POLICY ISSUES

We know from hard experience what happens when a handful of companies take advantage of the low cost, high-margin internet to establish market dominance. There is no reason to believe these experiences will not be repeated and expanded in the metaverse. As Matthew Ball observed, "One of the larger challenges facing the Metaverse is that a handful of vertically and horizontally integrated platforms collect a significant share of total time, content, data and revenues"²⁴

In the industrial era rules were eventually adopted to protect the public interest from corporate abuse. It remains to be seen whether the arrival of the metaverse will finally stimulate timely public interest protections for the internet era.

User Privacy

We have already experienced what happens when the capabilities of digital technology combine with monetary incentives to convert private personal information into a corporate asset to be monetized free of any comprehensive data protection law. The metaverse's

expansion of corporate intrusion into personal biometric information will make today's privacy infractions seem like a picnic.

Today, for instance, Meta has a real name policy for its social media platforms that links users to outside credit bureaus and data brokers to improve the user's targeting profile. The biometric data gathered by metaverse devices will enrich and individualize that information. A question that should be answered today is whether companies such as Meta should be able to merge such databases.

"Privacy and safety need to be built into the metaverse from day one," Mark Zuckerberg promised at the October 2021 rollout of his company's metaverse plans.²⁵ As has so often been the case, however, the term "privacy" was immediately reshaped from its commonly accepted meaning to one more suitable for the monetization of user information.

Following the blanket "privacy" promise, Zuckerberg qualified it to mean, "You'll decide when you want to be with other people, [or] when you want to block someone from appearing in your space." In his manifesto, Nick Clegg established privacy as one of the "priority areas that will guide our work." The Clegg definition of privacy protection: "how we can build meaningful transparency and control into our products."²⁶

Such characterizations hijack the meaning of the word "privacy" – a concept that is not limited to transparency or who to invite into your metaverse. *Webster's New World Dictionary* defines "privacy" as, "The quality or condition of being private...one's private life or personal affairs."²⁷

For decades the platform companies have obfuscated that simple and direct definition with "privacy policies" that, instead of protecting individual privacy, were permissions to exploit it. As the obfuscation became obvious, Facebook started running advertisements that further redefined "privacy" as, "You should be able to understand who has your data and how they use it."²⁸ Now, for the metaverse, "privacy" is apparently, yet again, redefined in a manner that obscures the behavioral, biometric, and other private personal information the metaverse platforms will siphon and monetize.

The personal nature of metaverse avatars requires the use of personally identifiable information. How participants will reach each other and third parties requires a new “identification layer” in the platform. As global social media platforms transition to social virtual reality they will need to be able to identify and authenticate users individually and persistently. Now is the time, as innovators work to develop such capabilities, to anticipate problems and design in privacy protections.

Protecting “one’s private life or personal affairs” should be designed into the metaverse from the outset.* Whether this can be accomplished absent a mandatory requirement is doubtful – but it is important to ask why not. The metaverse’s incorporation of biometric data to read emotions and influence behavior accentuates the increased importance of the already important privacy issue.

Privacy protections such as limiting the data collected to only that which is necessary to run the application and restricting its storage should be a forethought in the design of the metaverse, not an afterthought when the consequences of a lack of oversight become apparent. It is an encouraging start when Meta promises that biometric data will only be stored in the headset and will be deleted after use. Codifying that commitment would be better. If we have learned anything in the online experience it is that early intentions often do not survive subsequent revenue realities, and/or are often ignored by others.

What About Innovative Competition?

“Facebook is quietly buying up the metaverse,” a *Vox* headline proclaimed, asking the question, “Can Mark Zuckerberg M&A a new monopoly?”²⁹ Meta Platforms has proposed purchasing the virtual reality fitness company Within for a price reported to be north of \$500 million. Others

* A structure for designing privacy into the metaverse was outlined in 1995, long before the term had gained widespread awareness. Ann Cavoukian, the Commissioner of Information and Privacy for the Canadian province of Ontario, proposed the concept of “privacy by design” as a default mode of online operations.* Such principles have only gained in importance, including: proactive not reactive; preventive not remedial; privacy as the default setting; privacy embedded into design, and others.

are scrambling to shore up their VR activities as well. Microsoft is offering to purchase Activision Blizzard, maker of the popular *Call of Duty* and other VR games for \$69 billion.³⁰ On both sides of the Atlantic, governments are reacting to the transactions. The U.S. Federal Trade Commission (FTC) has sued to block the Meta transaction while the UK Competition and Markets Authority is investigating the Microsoft deal.

The control of personal data has been the key to the riches of the social media companies. After capturing private information, the companies build a moat around that data to deny access to others. The result of such data hoarding has been to thwart competition through the unequal distribution of the essential asset necessary for competition.

The major platform companies are dominant because they control the digital information on which advertisers rely, while denying it to others. As FTC Chair Lina Khan told congress, “Control over data has enabled dominant firms to capture markets and erect entry barriers.”³¹ The operation of the metaverse will expand the amount of private information collected to feed data dependent algorithms. Such increased dependence thus can become a new tool used by incumbents to stifle competition and the innovation competition brings.

The power structure of the metaverse will be shaped by decisions regarding access to digital information which has already been collected and hoarded as well as the new biometric data.

The Clegg Manifesto positions the issue of data access much as Facebook has historically portrayed the topic through linguistic jujitsu and the term “data portability.” Nick Clegg explained, “If they buy a t-shirt at the [metaverse] concert, they’ll want to be able to take it with them and not just be limited to wearing it in Meta-built experiences.” It is the same way Mark Zuckerberg repositioned the issue for social media in in a *Washington Post* op ed: “If you share data with one service, you should be able to move it to another,”³² It may sound like opening Meta’s data hoards, but moving a virtual item from one company’s platform to another is simply a business decision to enhance the user experience and nowhere near the

equivalent of the interoperability among the data collected from consumers in a manner that both spurs innovation-driving competition and protects personal privacy.[†]

The formulation for metaverse interoperability is a replica of the structure that has protected social media companies from meaningful competition: that the technology should be open and interoperable allowing services to siphon and store as much data as possible, but the data itself should not be interoperable.

If the metaverse is to live up to its potential, a thousand flowers must be allowed to bloom, not just a few potted plants protected by competition-preventing practices. The Clegg Manifesto states, “no single company can or should control the metaverse.” Whether the metaverse is vibrantly competitive or becomes like the current non-competitive social media landscape is a matter that rests on the availability of the necessary digital assets. It is a decision that is too important to be left to the companies to determine.

Content Moderation and Manipulation

In today’s world toxic hate groups exploit technology to extend their bile. To expect something different in the metaverse is whistling past the graveyard.

Today’s social media has been a vehicle for misinformation, disinformation, and malinformation. Editorial decisions by digital platforms have become tribal political issues. The metaverse’s expansion of the user’s experience from observational to participatory will accentuate the importance of editorial input while increasing its emotional impact.

Tech journalist Casey Newton identified such issues in an interview with Mark Zuckerberg, “Who gets to augment reality?” he asked.³³ Newton went on to imagine “a world where we’re all wearing our headsets, and we’re looking at the U.S. Capitol building...most of us have an overlay that says, ‘This is the building where Congress works’ ...[but] some other people might see an overlay that says, ‘on January 6, 2021, our glorious revolution began.’” Zuckerberg’s response called this “one of the central questions of our time” before he diverted the

[†] As a part of metaverse policy decisions there should be privacy-protection initiatives allowing for users’ discretion as well as technical requirements such as differential privacy and synthetic data techniques.

discussion to talk about his childhood experience with baseball. Later in the interview he observed, “In order to have a cohesive society, you need to have a shared foundation of values and some understanding of the world and the problems we face together.”

Instead of bringing us together, social media companies, whether Facebook, YouTube, TikTok, or others, program their algorithms to prioritize revenue by driving users into echo chambers that are the antithesis of a “shared foundation of values.” It is hard to find the rationale for metaverse algorithms to behave differently. For social media, the incentive is to program algorithms to maximize user engagement that keeps the user around to see advertisements. That user engagement goal does not change in the metaverse, in fact, it can be greater: to tie user engagement with the purchase of virtual goods with even higher profit margins.

Social media platforms have been described as “automated propaganda” as algorithms direct information to audiences likely to respond favorably. In the Cambridge Analytica scandal, personal information ended up targeting political messaging. That messaging, however, was a lifeless product in the form of preprepared text or video targeted to a cohort of users. The metaverse, in contrast, is designed to be life-like and personal. Reading the biometric data of a user, a propaganda avatar could be capable of adapting its look, tone and message to fit what the sensors are reporting about the emotions of the user. “Virtual reality environments turn out to be really ideal environments for doing emotional manipulation of all sorts,” according to Rand Williamson, a scientist at the RAND Corporation.³⁴

To date, social media platforms have been unsuccessful in sufficiently moderating hate, lies, and half-truths.³⁵ The metaverse will move that problem into virtual worlds in which the user’s biological activities could reveal more about the user than they know about themselves.

NEW METAISSUES

Thus far, this discussion has considered the “known unknowns” of the metaverse: the expansion of the problems of social media into social virtual reality. The metaverse also creates

a new set of challenges: how (and whether) to import the social norms of the real world into the virtual world.

Nick Clegg was not encouraging about the ability of metaverse companies to deal with the new challenges. He told *The Washington Post*, “You simply can’t have corporate employee moderators moderating what will be private ephemeral communication in privately created spaces.”³⁶

“Private ephemeral communication in privately created spaces,” is a brave new world. This new reality will amplify and expand the wonders of the connected world. At the same time, it will also amplify and expand the darkest side of digital connectivity and algorithms. To address these kinds of issues, Mark Zuckerberg explained, is “going to take ecosystem building, norm setting and new forms of governance...And this is something that we’re really going to focus on.”³⁷

We need that focus now.

Harassment

The pseudo-world precursor of the metaverse, video games, already runs rampant with “harassment, assaults, bullying and hate speech.”³⁸ A study from the Center for Digital Hate found Metaverse “users, including minors, are exposed to abusive behavior every seven minutes.”³⁹

My nightmare trip into the metaverse,” is how one reporter described the, “barrage of assault, racism and rape jokes” she experienced.⁴⁰ Within minutes of entering a virtual reality (VR) chat room, “I saw underage kids simulating oral sex on each other. I experienced sexual harassment, racism and rape jokes...despite using a profile that I’d listed as being 13 years old.”

The New York Times reported how a 29-year-old woman who, while using her Meta Oculus Quest VR headset, was accosted by a male avatar who groped and ejaculated onto her avatar. When she asked the player to stop, “He shrugged as if to say: ‘I don’t know what to tell you. It’s the metaverse – I’ll do what I want.”⁴¹

Research has identified the “online disinhibition effect” that leads people to behave differently online than in the real world.⁴² It is no wonder, therefore, that “70 percent of women say personal safety in the metaverse is a concern, while 73 percent are worried about online abuse and 64 percent are concerned about sexual harassment.”⁴³

Four employees of Meta’s Oculus VR project studied harassment in virtual reality.⁴⁴ Their research, *Harassment in Social Virtual Reality: Challenges for Platform Governance*, concluded virtual reality experiences of harassment “can be exacerbated by features such as synchronous voice chat, heightened feelings of presence and embodiment, and avatar movements that that can feel like violations of personal space.” The researchers observed that efforts to govern these developing spaces are “made more complex by the distributed landscape of virtual reality applications and the dynamic nature of local community norms.”

Horizon Worlds, Meta’s metaverse platform, has been responsive to these kinds of issues. *The New York Times* reported Horizon “has user tools to deter virtual assaults and threatening behavior...a ‘safe mode’ that allows a user to escape into a solitary confinement cell [to avoid unwanted behavior]; and a polling function that can gauge whether a group feels a disruptive user should be kicked out.”⁴⁵ It is a set of responsible actions, but the question is whether it will be sufficient.

Therein lies the conundrum and challenge. Hooray for Meta’s efforts to anticipate and deal with potential harassment problems. Yet, the research by the Meta employees demonstrates how the metaverse can exacerbate harassment utilizing a technology that makes the establishment and enforcement of behavioral norms difficult.

Property Rights, Financial Transactions, Fraud, Death and Taxes

Does the combination of zeroes and ones represent tangible “property”? When Non-Fungible Tokens (NFT)⁴⁶ – a collection of code that, by definition, is “not interchangeable for other assets because they have unique properties”⁴⁷ – sell for millions of dollars, what exactly is the asset?

Early in 2021, Christie’s sold an NFT of Mike Winkelmann’s digital artwork “Everydays - The First 5000 Days” for \$69 million.⁴⁸ Just what did the purchaser buy? It’s not as if the piece can only

be seen in the buyer's metaverse, it can be viewed via any internet browser.⁴⁹ What was purchased, it seems, is the technological ability to authenticate the NFT via blockchain as a unique version of the art.

What happens when virtual things that are not real are fraudulently transferred? When a digital Gucci bag sold for \$4,100; what was being purchased?⁵⁰ Presumably, it was to be worn by an avatar and thus was a product just like a real Gucci bag. But what if it was a fraudulent knockoff like so many real-life Gucci bags? What if the virtual bag is stolen by another avatar?

In 2009 a court in The Netherlands convicted three minors of stealing virtual furniture from an online multiplayer computer game.⁵¹ The result has been a legal debate as to whether a non-real item can be "stolen," and if so, what criminal statutes apply? An even more basic question in the metaverse is the location of any remedy, both in the identification and apprehension as well as the adjudication of the offenders?

And we haven't even begun to get into Franklin's "two certainties" of death and taxes. Does homicide exist if you "kill" a personally identifiable something that is not alive? Certainly killing is rampant in video games; does that mean that killing a personally identifiable avatar should be morally acceptable in the metaverse? Insofar as taxes, if the metaverse is going to be the new venue for online commerce and the value of those transactions is held in the metaverse rather than transferred to hard cash, what should be the taxation policy and who has jurisdiction?

Safety

In September 2022 a British coroner concluded the 2017 suicide of 14-year-old Molly Russell was a result of platform algorithms that had systematically shown her graphic self-harm and suicide images and videos. "She died from an act of self-harm while suffering from depression and the negative effects of online content," Senior Coroner for North London Andrew Walker concluded.⁵² "The sites normalized her condition" and created "binge periods" of material that "affected her mental health in a negative way and contributed to her death in more than a minimal way."

“The platform operated in such a way using algorithms as to result, in some circumstances, of binge periods of images, video clips and text, some of which were selected and provided without Molly requesting them.” Referring to Meta’s Instagram, the coroner concluded that in the six months before her death, roughly 13 percent of the 16,000 Instagram posts that Molly viewed were related to suicide, depression or self-harm.

The transferability of the effects of the social media experience to the social virtual reality experience is at this point only problematic, but it certainly seems logical. Blundering ahead into the metaverse unawares and unresponsive to such problems is inexcusable.

Andrew Bosworth, Meta’s Chief Technology Officer, told *The New York Times* that he wants Horizon Worlds, Meta’s current VR social network, to be “almost Disney levels of safety.” It is a highly commendable objective. Now, how will it be implemented, not just for Meta, but for everyone?

Digital Chasm

In 2019 it was discovered that the algorithm used to predict the prognosis of hospital patients favored white patients over black patients. A similar AI program used in court sentencing predicted twice as many false positives for recidivism for black offenders than white offenders.⁵³

A recent study on structural racism in the digital revolution reported how a Google search, “matched ‘Black-sounding’ names with the profiles of arrest records, even when false...[and] Facebook apologized for an AI model that asked viewers of a British tabloid video featuring Black men if they wanted to ‘keep seeing videos about Primates.’”⁵⁴

Digital algorithms have created new opportunities for discrimination, often subtle and perhaps unintentional, but discriminatory nonetheless. The difficulties of algorithmic bias in online services have been well documented.⁵⁵ Feeding algorithms with the expanded amount of personal information gathered by metaverse companies opens the door to the potential of platform-induced discrimination, whether intentional or not.

A NEW REALITY REQUIRES NEW OVERSIGHT

“In the past, the speed at which new technologies arrived sometimes left policy makers and regulators playing catch up,” Nick Clegg told the October 2021 Connect conference. “It doesn’t have to be the case this time around because we have years before the metaverse we envision is fully realized.”⁵⁶ One year later, at the 2022 Connect conference, Mark Zuckerberg gave a similar answer: “we have some time to try and work some of this stuff out.”⁵⁷

But we don’t have time. The early incarnation of the metaverse is already upon us and tens of billions are being spent annually to speed its completion. Meta has already sold nearly 15 million metaverse-enabled virtual reality (VR) headsets⁵⁸ and \$1.5 billion in games and apps in its Quest store.⁵⁹ Microsoft and Meta have announced they are partnering to bring the metaverse to the enterprise.⁶⁰

As we move deeper into new online worlds, it is time to collectively decide where we want to be going. That Microsoft, Meta, Google, Apple, and others are spending billions to develop the metaverse is the signal that it is also time to develop new policies to oversee those activities. These policies should be in addition to the application of antitrust law to protect and promote competition in the space.

Both the old and new realities discussed in this paper demand oversight that is technologically adept and functionally agile enough to keep up with technology, innovation, and marketplace developments. In other papers, my colleagues and I have called for the creation of a new federal Digital Platform Agency (DPA) with a new agile approach to oversight.⁶¹ If ever there was a clarion call for such oversight and for a new approach to its implementation, it is the metaverse.

While time is not on the side of metaverse users and the public interest, it is on the side of those seeking to design how they will profit in the metaverse. As long as there is no public interest oversight, the companies are free to design their own rules. Just as in the pre-metaverse world, those rules will be in the companies’ best interest. If policymakers languidly assume that “we have years,” the companies will once again determine their behavior before the public realizes what has been imposed.

The challenge – and importance – of rules built on the public interest rather than corporate interest is heightened by the nature of the metaverse. The metaverse requires focused and agile oversight in two dimensions: the real-world activities of corporations, and the behavior inside pseudo-world communities. Remaining observers to either dimension is not an acceptable option.

New Technology and Old Responsibilities

A basis for establishing behavioral expectations for the metaverse has long existed. For hundreds of years English common law has provided guidance for legislators, regulators, and judges. Those same concepts can also form the basis for oversight of the metaverse.

Common law concepts reach back to the time when England was emerging from the bonds of feudalism. Like the platform barons of today, feudal lords made their own rules. As markets and a middle class began their post-feudal ascendancy there developed a standard set of behavioral expectations. These were referred to as “common law” because, as opposed to the random rules of the nobles, the principles were “common” in courts across the land.

One of the principal concepts of common law was the Duty of Care. This holds that the provider of a product or service has the responsibility to anticipate and mitigate harms that could result from its use. It is the root of tort negligence. It should similarly define expectations in the online world.

Unfortunately, the timeless principles of common law have been hit by the blitzkrieg of the digital revolution. As the digital innovators made their own rules, they often conveniently sidestepped or blatantly ignored their duties to others. The question for oversight of the metaverse thus becomes how to impose a common duty of care in place of policies made by the dominant companies for their own benefit?

A New Regulatory Model

The statutes and structures that were created to protect individuals and a competitive marketplace from the abuses of the industrial era are inadequate for the internet era. The pace of technological change and its marketplace assimilation was slower in the industrial economy

that in today's digital economy. The regulatory model thus reflected the industrial management model with rigid, rules-based micromanagement.

The torrid pace of technology today means that such command-and-control regulation can be counterproductive. Prioritizing regulatory micromanagement comes at the cost of deprioritizing innovation and investment and the ability to keep pace with technology and its effects.

Oversight of digital activities calls for replacing the dictation of specific operational details with dynamic regulation that is focused on identifying and mitigating significant risks with agile solutions.

We have experienced how industrial era statutes and structures have been out maneuvered by the decisions of the digital companies. Further stressing these old structures with the far-reaching implications of the metaverse is unimaginable. Oversight of the metaverse requires a new federal agency and a new regulatory paradigm.

Fortunately, the model for such a new paradigm has already been developed by the agile management practices of the digital companies themselves. One of those practices is the use of technical standards developed through a "multistakeholder process" involving a collection of interested parties.

The internet itself is a set of standards that assure different networks will work together. The platforms that ride that network similarly operate based on standards that, for instance, allow email from one service provider to be received and displayed on a different email service. Similarly, computing and telecommunications equipment are built to common standards in order to be usable for all.

Technical standards have been the backbone of the digital platform companies. Extending those concepts to behavioral standards, however, has been largely ignored. The digital companies utilize standards to protect themselves when they are consumers, but when they deliver products and services to marketplace consumers there is no standardization of their Duty of Care.

In developing the metaverse, the companies have, once again, reverted to the standards process. Over 1,500 companies have joined the Metaverse Standards Forum to develop common technical standards.⁶² According to the Forum’s website, “The activities of the Forum will be directed by the needs and interests of its members.”⁶³ Included in the list of goals for the Forum are standards for “Privacy, Safety, Security, Inclusion.”⁶⁴ That the companies are using the standards process not only to develop technology, but also to deal with its behavioral effects is precedent-setting. But the question remains whether it is the foxes that should make the rules for guarding the digital henhouse.

The Clegg Manifesto appears to have opened the door to a new approach to regulatory oversight. It proposes, “developing a system of governance for the metaverse. And it must not be shaped by tech companies like Meta on their own. It needs to be developed openly with a spirit of cooperation between the private sector, lawmakers, civil society, academia, and the people who will use these technologies.”⁶⁵ Add a meaningful role for government to identify issues and enforce results, and this sounds strikingly similar to the proposed Digital Platform Agency which Mark Zuckerberg, in fact, endorsed in congressional testimony.⁶⁶

What is needed for the entire digital platform environment, not just the metaverse, is neither the weakness of voluntary self-regulation nor the rigidity of top-down regulatory dictates. The new era requires a new model of participatory oversight in which government identifies issues, then works with representatives of the companies and civil society to develop acceptable – and enforceable – standards.

Community Governance

But what about governance within the pseudo-world of the metaverse? A government overseen process for real-world oversight reaches its limits outside that real world. While it may be possible to establish rules for when the metaverse interacts with the real world, governance within the pseudo-world, by definition, is a world of its own, with the potential to create new problems.

“The current debate about how to handle bad-but-not-illegal conduct on social media and the internet hints at the debates to come about how to treat anti-social behavior in the

metaverse,” Nick Clegg wrote.⁶⁷ His previously cited comments to *The Washington Post*, “You simply can’t have corporate employee moderators moderating what will be private ephemeral communication in privately created spaces,” however, would seem to be a corporate washing-of-hands.⁶⁸

In *Harassment in Social Virtual Media: Challenges for Platform Governance*, the authors suggest that behavior in the metaverse is out of the hands of the companies that created the new world. “Given the complications of top-down governance across VR platforms and the transient nature of these social spaces,” they conclude, “our results underscore the importance of relying on community-led governance to regulate behavior.”⁶⁹

Parsing the community behavior issue leads to at least two conclusions. The first is that corporate decisions about the metaverse can affect community behavior. Reddit, for example, has created the ability for subreddit groups to create and enforce their own rules.⁷⁰ Those building the metaverse can facilitate such governance – an issue that would be appropriate for the new digital agency to address. Ultimately, however, the question comes down to determining what are acceptable norms inside the metaverse, who will be their protector/enforcer, and what are the responsibilities of the companies that profit by creating the metaverse?

The second conclusion is that while users have little control over the technical aspects of their experience, they do have control over the behavior of their avatars. This creates a need for the development of behavior norms, and possibly even virtual cops on the beat. The authors of *Harassment in Virtual Social Media* worry, however, “the lack of shared understanding of social norms in social VR makes users reluctant to categorize certain activities as problematic in intent, even when they are experienced as annoying or hurtful.”⁷¹

In the days of the early internet there was an optimistic belief that the developing internet communities would make their own rules and should be left alone. If you didn’t like the rules of one community, it was argued, you could simply migrate to another. Experience had demonstrated the naivety of that assumption.

Ultimately, the metaverse is going to require its builders to play a role in community-driven rules and their enforcement. Accomplishing this in the real-world is difficult enough; achieving it in a world where the user can leave the expectations of the real-world behind is an order of magnitude increase in difficulty. This is not a challenge to be kicked down the “we’ve got time” road.

International Governance

The interconnected world of the internet has already demonstrated the need for multinational policy cooperation as decisions in one jurisdiction travel at the speed of light to reverberate in other nations. When it comes to digital platform policy development, however, the United States has been satisfied to sit back and allow others to do the heavy lifting. Unfortunately, the failure of American policy makers to deal with the platform problems we know has denied the policy underpinning to deal with what comes next.

There is a first mover advantage in policy as surely as there is a first mover advantage in the market. As a result, the United States appears, once again, destined to live in an online world in which Americans’ lead in technological development can be compromised by the lead of others in policy development.

In the European Union, the Digital Markets Act⁷² and Digital Services Act⁷³ have staked out the responsibilities of the gatekeeper digital platforms we know today. The European Commission, the oversight body of the EU has indicated that while those tools can extend to the metaverse.⁷⁴ The EU will nonetheless launch “a broad consultation” on the metaverse “by the first quarter of next year [2023].”⁷⁵

In the United Kingdom, Melanie Dawes, Chief Executive of UK regulator Ofcom, has indicated the pending Online Safety Bill is comprehensive enough to include the metaverse. That legislation grants Ofcom authority over online activities that are “legal but harmful.”⁷⁶ Dismissing the idea of self-regulation, Dawes commented, “I’m not sure I really see that ‘self-regulatory phase’, to be honest, existing from a UK perspective.” “I think that things like metaverses are adding intensity” to the issues inherent in digital platforms, she explained.⁷⁷

While the U.S. sleeps, other Western liberal democracies are stepping up to the new challenge. Because these activities are in their early stages, there still exists the opportunity for liberal democracies to work together to cooperatively identify the risk factors associated with the metaverse and how to deal with them.

Eyes Open, Time to Act

As the advertisements say, “The metaverse may be virtual, but its impact will be real.” And so will be its responsibilities, for users as well as those who profit from the technology.

We, as citizens, cannot be passive observers allowing others to make the rules for the metaverse. We must enter the rollout of the metaverse with our eyes open. Decisions are now being made that will determine our relationship with the metaverse and affect our relationship with each other. We have already experienced the effects of “move fast and break things.” Now is not the time for a reprise of that performance. Establishing the responsibilities of the metaverse companies can neither be overlooked nor delegated to the companies themselves.

¹ Ina Fried, “For Meta, new headset but same old problems,” *Axios*, October 12, 2022, https://www.axios.com/newsletters/axios-login-27612ce2-a550-4957-86d0-04b98b4186a4.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioslogin&stream=top

² “Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026,” February 7, 2022, <https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026>

³ Jeff Horowitz, “Company Documents Show Meta’s Flagship Metaverse Falling Short,” *The Wall Street Journal*, October 15, 2022, <https://www.wsj.com/articles/meta-metaverse-horizon-worlds-zuckerberg-facebook-internal-documents-11665778961>

⁴ Tom Wheeler, “History repeats itself with Big Tech’s misleading advertising,” *Brookings Tech Tank*, June 15, 2022, <https://www.brookings.edu/blog/techtank/2022/06/15/history-repeats-itself-with-big-techs-misleading-advertising/>

⁵ Matthew Ball, *The Metaverse: And How It Will Revolutionize Everything*, Liveright, 2022, p. 17

⁶ Facebook Second Quarter 2021 Investor Call, https://s21.q4cdn.com/399680738/files/doc_financials/2021/q2/FB-Q2-2021-Earnings-Call-Transcript.pdf

⁷ Meta Platforms, “The metaverse may be virtual, but the impact will be real,” https://about.meta.com/metaverse/impact/?utm_source=about.facebook.com&utm_medium=redirect

⁸ *Ibid*

⁹ *Ibid*

¹⁰ Eric M. Johnson and Tim Hether, “Boeing wants to build its next airplane in the ‘metaverse,’” *Reuters*, December 17, 2021, <https://www.reuters.com/technology/boeing-wants-build-its-next-airplane-metaverse-2021-12-17/>

¹¹ *Op Cit*, Meta Platforms

¹² Phil Wainwright, “Meta brings VR to business meetings – is this the enterprise gateway to the metaverse?,” *Diginomica*, October 21, 2022, <https://diginomica.com/meta-brings-vr-business-meetings-enterprise-gateway-metaverse>

¹³ “The metaverse could be tech’s next trillion-dollar opportunity: These are the companies making it a reality,” CBINSIGHTS, <https://www.cbinsights.com/research/metaverse-market-map/>

¹⁴ ACM Symposium on Eye Tracking Research & Applications, <https://etra.acm.org/2022/>

¹⁵ Jacob Leon Kroger, Otto Hans-Martin Lutz and Florian Muller, “What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking,” *IFIP Advances in Information and Communications Technology*, vol 576, Springer, Cham., https://link.springer.com/chapter/10.1007/978-3-030-42504-3_15#citeas

¹⁶ Mattha Busby, “Social media copies gambling methods ‘to create psychological cravings,’” *The Guardian*, May 8, 2018, <https://www.theguardian.com/technology/2018/may/08/social-media-copies-gambling-methods-to-create-psychological-cravings>

¹⁷ Philip Parnaments, Petter Johansson, Lars Hall, and Daniel C. Richardson, “Biasing moral decisions by exploiting the dynamics of eye gaze,” February 13, 2015, PNAS, <https://www.pnas.org/doi/full/10.1073/pnas.1415250112>

¹⁸ Hannah Murphy, “Facebook patents reveal how it intends to cash in on metaverse,” *Financial Times*, January 18, 2022, <https://www.ft.com/content/76d40aac-034e-4e0b-95eb-c5d34146f647>

¹⁹ “Meta (Facebook) Connect 2021 Metaverse Event Transcript,” at 07:13, October 28, 2021, <https://www.rev.com/blog/transcripts/meta-facebook-connect-2021-metaverse-event-transcript>

²⁰ Louis B. Rosenberg, “Regulating the Metaverse, a Blueprint for the Future,” *ACM Digital Library*, August 26, 2022, https://dl.acm.org/doi/abs/10.1007/978-3-031-15546-8_23

²¹ Nick Clegg, “Making the metaverse: What it is, how it will be built, and why it matters,” May 18, 2022, <https://nickclegg.medium.com/making-the-metaverse-what-it-is-how-it-will-be-built-and-why-it-matters-3710f7570b04>

²² https://en.wikipedia.org/wiki/Das_Kapital

²³ Meta Platforms, “We support updated regulation on the internet’s most pressing challenges,” https://about.meta.com/regulations/?utm_source=about.facebook.com&utm_medium=redirect

²⁴ *Op Cit*, Ball Metaverse, p. 295

²⁵ “Meta (Facebook) Connect 2021 Metaverse Event Transcript,” at 07:45, October 28, 2021, <https://www.rev.com/blog/transcripts/meta-facebook-connect-2021-metaverse-event-transcript>

²⁶ Nick Clegg, “Making the metaverse: What it is, how it will be built, and why it matters,” *Tech at Meta*, May 19, 2022, <https://tech.fb.com/ideas/2022/05/making-the-metaverse/>

²⁷ David B. Guralnik, ed., *Webster’s New World Dictionary of the American Language: Second College Edition*, (New York: Simon and Schuster, 1980), p. 1131.

²⁸ Meta “An Open Conversation with Rochelle,” YouTube video, October 13, 2021, <https://www.youtube.com/watch?v=qV79Dvwqo9Y>

²⁹ Peter Kafka, “Facebook is quietly buying up the metaverse,” *Vox*, November 11, 2021, <https://www.vox.com/recode/22776461/facebook-meta-metaverse-monopoly>

-
- ³⁰ Steve Kovach, "Microsoft to buy Activision in \$68.7 billion all-cash deal," CNBC, January 18, 2022, <https://www.cnbc.com/2022/01/18/microsoft-to-buy-activision.html>
- ³¹ "Statement of Chair Lina M. Khan Regarding the Report to Congress on Privacy and Security," Federal Trade Commission, October 1, 2021, <https://www.ftc.gov/public-statements/2021/10/statement-chair-lina-m-khan-regarding-report-congress-privacy-security>
- ³² Mark Zuckerberg, "The Internet needs new rules. Let's start with these four," *The Washington Post*, March 30, 2019, https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html
- ³³ Casey Newton, "Mark in the Metaverse," *The Verge*, July 22, 2021, <https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview>
- ³⁴ Andrew S. Chow, "A Year Ago, Facebook Pivoted to the Metaverse. Was It Worth It?" October 27, 2022, <https://time.com/6225617/facebook-metaverse-anniversary-vr/>
- ³⁵ Paul M. Barrett, "Who Moderates the Social Media Giants?," NYU Stern Center for Business and Human Rights, June, 2020, <https://bhr.stern.nyu.edu/tech-content-moderation-june-2020>
- ³⁶ Christiano Lima, "Meta's Clegg: Facebook's rule book won't work in the metaverse," *The Washington Post*, May 18, 2022, <https://www.washingtonpost.com/politics/2022/05/18/meta-clegg-facebooks-rule-book-wont-work-metaverse/>
- ³⁷ *Op Cit.*, Zuckerberg Transcript at 07:13,
- ³⁸ Sheera Frenkel and Kellen Browning, "The Metaverse's Dark Side: Here Come Harassment and Assaults," *The New York Times*, December 30, 2021, <https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html>
- ³⁹ "Facebook's Metaverse," Center for Countering Digital Hate, December 30, 2021, https://counterhate.com/research/facebooks-metaverse/?_ga=2.39938658.1985441126.1665761340-1467858480.1665761340&_gl=1%2A1vr8yuk%2A_ga%2AMTQ2Nzg1ODQ4MC4xNjY1NzYxMzQw%2A_ga_V7WR404SEC%2AMTY2NTc2MTQwOS4xLjEuMTY2NTc2MTQ0MC42MC4wLjA.
- ⁴⁰ Yinka Bokinni, "A barrage of assault, racism and rape jokes: my nightmare trip into the metaverse," *The Guardian*, April 25, 2022, <https://www.theguardian.com/tv-and-radio/2022/apr/25/a-barrage-of-assault-racism-and-jokes-my-nightmare-trip-into-the-metaverse>
- ⁴¹ *Op Cit.*, Dark Side
- ⁴² Lauren Farrar, "Is the Internet Making You Meaner?" KQED, August 5, 2019, <https://www.kqed.org/education/532334/is-the-internet-making-you-meaner#:~:text=Yes.,in%20face%20to%20face%20conversations>.
- ⁴³ Morning Consult, April 16, 2022, <https://twitter.com/MorningConsult/status/1515451970781392906>
- ⁴⁴ Lindsay Blackwell, Nicole Ellison, Natasha Elliott-Deflo, Raz Schwartz, "Harassment in Social Virtual Reality: Challenges for Platform Governance," *PACM on Human-Computer Interaction*, vol. 3, No. CSCW, Article 100, November 2019, <http://www.lindsayblackwell.net/wp-content/uploads/2019/09/Harassment-in-Social-Virtual-Reality-CSCW-2019.pdf>
- ⁴⁵ Kashmir Hill, "This Is Life in the Metaverse," *The New York Times*, October 7, 2022, <https://www.nytimes.com/2022/10/07/technology/metaverse-facebook-horizon-worlds.html>
- ⁴⁶ "Non-fungible tokens (NFT)," Ethereum, <https://ethereum.org/en/nft/>
- ⁴⁷ *Ibid*
- ⁴⁸ Josie Thaddeus-Johns, "What Are NFTs, Anyway? One Just Sold for \$69 Million," *The New York Times*, March 11, 2021, <https://www.nytimes.com/2021/03/11/arts/design/what-is-an-nft.html#:~:text=Christie's%20Images%20Ltd.&text=The%20artist%20Mike%20Winkelman%2C%20also,achieved%20by%20a%20living%20artist>.
- ⁴⁹ Beeple, The First 5000 Days, <https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924>
- ⁵⁰ Randeep Sudan, "How should governments prepare for the metaverse?," *Digital Diplomacy*, July 20, 2021, <https://medium.com/digital-diplomacy/how-should-governments-prepare-for-the-metaverse-90fd03387a2a>

-
- ⁵¹ Litska Strikwerda, "Theft of virtual items in online multiplayer computer games: an ontological and moral analysis," *Ethics and Information Technology*, January 6, 2012, <https://link.springer.com/article/10.1007/s10676-011-9285-3>
- ⁵² Angus Crawford and Bethan Bell, "Molly Russell inquest: Father makes social media plea," *BBC News*, September 30, 2022, <https://www.bbc.com/news/uk-england-london-63073489>
- ⁵³ Terence Shin, "Real-life Examples of Discriminating Artificial Intelligence," *Towards Data Science*, June 4, 2020, <https://towardsdatascience.com/real-life-examples-of-discriminating-artificial-intelligence-cae395a90070>
- ⁵⁴ Nicol Turner Lee, "It's Time for an Updated Big Tech Civil Rights Regime," *PolicyLink*, https://www.policylink.org/sites/default/files/Nicol_Turner_Lee_082522a.pdf
- ⁵⁵ "Racial Discrimination In The Sharing Economy," *HBS Working Knowledge*, February 24, 2014, <https://www.forbes.com/sites/hbsworkingknowledge/2014/02/24/racial-discrimination-in-the-sharing-economy/?sh=1d85d64b5c44>
- ⁵⁶ *Op Cit*, Bloomberg
- ⁵⁷ *Op Cit*, Ina Fried
- ⁵⁸ Kashmir Hill, "This is Life in the Metaverse," *The New York Times*, October 7, 2022, <https://www.nytimes.com/2022/10/07/technology/metaverse-facebook-horizon-worlds.html>
- ⁵⁹ Casey Newton, "Meta's metaverse turns pro," *Platformer*, October 11, 2022, https://www.platformer.news/p/metas-metaverse-turns-pro?utm_source=email
- ⁶⁰ Tom Warren, "Microsoft partners with Meta to bring Teams, Office, Windows, and Xbox to VR," *The Verge*, October 1, 2022, <https://www.theverge.com/2022/10/11/23397251/meta-microsoft-partnership-quest-teams-office-windows-features-vr>
- ⁶¹ See, Tom Wheeler and Phil Verveer, "A Turning Point in the Oversight of Digital Platforms: A Challenge for American Leadership," Harvard Kennedy School, Shorenstein Center on Media, Politics, and Public Policy, February 25, 2021, <https://shorensteincenter.org/turning-point-oversight-digital-platforms/>
- ⁶² <https://metaverse-standards.org/>
- ⁶³ *Ibid*
- ⁶⁴ "Setting Course for an Open Metaverse Part 1: Updates from the First 60 Days of the Metaverse Standards Forum," The Metaverse Standards Forum, <https://metaverse-standards.org/news/blog/setting-course-for-an-open-metaverse-part-1-updates-from-the-first-60-days-of-the-metaverse-standards-forum/>
- ⁶⁵ *Op Cit*, Clegg
- ⁶⁶ At a March 2021 hearing Zuckerberg was [asked](#) by Vermont Rep. Peter Welch if he would support creating a new federal agency to regulate digital platforms. His reply was: "The solution that you're talking about could be very effective and positive for helping out," https://archive.org/details/CSPAN2_20210326_070100_Part_1_Facebook_Google_and_Twitter_CEOs_Testify_on_Combating_Online...
- ⁶⁷ *Op Cit*, Clegg
- ⁶⁸ Christiano Lima, "Meta's Clegg: Facebook's rule book won't work in the metaverse," *The Washington Post*, May 18, 2022, <https://www.washingtonpost.com/politics/2022/05/18/meta-clegg-facebooks-rule-book-wont-work-metaverse/>
- ⁶⁹ *Op Cit*, Harassment
- ⁷⁰ "Rules," *Reddit*, <https://mods.reddithelp.com/hc/en-us/articles/360023379211-Rules>
- ⁷¹ *Op Cit*, Harassment
- ⁷² [https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/0374\(COD\)](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/0374(COD))
- ⁷³ <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
- ⁷⁴ "Answer given by Mr. Breton on behalf of the European Commission, January 6, 2022, https://www.europarl.europa.eu/doceo/document/E-9-2022-000656-ASW_EN.pdf
- ⁷⁵ Laura Kabelka, "European Commission turns its gaze towards the metaverse," September 14, 2022, <https://www.euractiv.com/section/digital/news/european-commission-turns-its-gaze-towards-the-metaverse/>
- ⁷⁶ https://en.wikipedia.org/wiki/Online_Safety_Bill

⁷⁷ Ryan Browne, “Meta and Microsoft can’t self-regulate their metaverses, UK regulator warns,” CNBC, October 26, 2022, <https://www.cNBC.com/2022/10/26/meta-and-microsoft-cant-self-regulate-their-metaverses-ofcom-warns.html#:~:text=Investing%20Club-,Meta%20and%20Microsoft%20can't%20self%2Dregulate,their%20metaverses%2C%20UK%20regulator%20warns&text=Ofcom%20Chief%20Executive%20Melanie%20Dawes,under%20U.K.%20online%20safety%20laws>.