Regulating the metaverse: issues and regulatory strategies

Abstract
This paper provides a brief overview of some key policy issues that may arise in the metaverse such as privacy and security of personal user data, anti-competitive behavior, and dissemination of harmful and illegal content. Additionally, this paper beckons for policymakers to fully grasp the software and hardware that the metaverse is likely to be based on and the economics of the emerging metaverse marketplace. Lastly, this paper proposes that policymakers and regulators take a proactive approach by employing various regulatory strategies such as the command and control strategy, the incentive-based strategy and competition/anti-trust laws to address policy issues that may arise in the metaverse.

Introduction
The Metaverse has been touted as a transformative technological development that will completely reshape many aspects of our daily lives. Based on the colossal investments that have been made by many of the multinational corporations that are commonly referred to as ‘the tech giants’, it is clear that the metaverse is the next big thing and as such it appears as though an arms race has commenced for dominion over it. In October 2021, Facebook changed its name to Meta signifying that it will shift its primary focus from social media to the metaverse.\(^1\) Additionally, Meta has invested $10 billion in acquiring and developing metaverse related hardware and software. Microsoft has also substantially invested into the metaverse via its $70 billion acquisition of the video game maker Activision Blizzard\(^2\).

Considering the anticipated far-reaching impact of the metaverse\(^3\), it is prudent for policymakers to grasp key features of the metaverse such as its technology (software and hardware) and the emerging marketplace. Policymakers and regulators must also identify the issues that may potentially arise in the metaverse and propose relevant correlating regulatory strategies to attempt to mitigate the risk of serious harm from these issues. At this point in time, it is difficult to identify all the issues that may arise in the metaverse as it is still in its infancy. However, this paper will

---

3. Mark Zuckerberg, CEO of Meta, wrote in the October 2021 Founder’s Letter that “in the metaverse, you’ll be able to do almost anything you can imagine — get together with friends and family, work, learn, play, shop, create — as well as completely new experiences that don’t really fit how we think about computers or phones today accessed via Meta. 2022. Founder’s Letter, 2021 | Meta. [online] Available at: https://about.fb.com/news/2021/10/founders-letter/#:~:text=In%20the%20metaverse%2C%20you%27ll,use%20the%20metaverse%20one%20day [Accessed 10 June 2022].
examine some of the relevant policy issues that are likely to arise in the metaverse and consider some regulatory strategies to address them.

Potential Issues in the metaverse

The metaverse is projected to be a powerful tool which makes it inherently dangerous in the absence of regulatory restraint. Rosenberg (2022) argues that the Metaverse poses certain dangers to society as it will allow corporations to influence the products, services, and information that we are exposed to and the people we encounter and socialize with. The emergence of the internet and ubiquity of social media platforms have led to many social, legal, and regulatory issues that policymakers are still currently trying to resolve. Policymakers must consider amongst other issues, the use of digital assets, criminal activity, privacy and security of personal data, anti-competitive behavior, and content regulation in the metaverse. This paper will focus on the issues of privacy and security of data, anti-competitive behavior, and content regulation.

Privacy and security of personal data

The advancement of digital technology has led to the large-scale collection, processing, and distribution of personal user data. In 2006, British mathematician Clive Humby famously stated that “Data is the new oil.” Meta’s business model is based on using personal user data which it obtains via its social media platform to sell sophisticated and targeted advertising to advertisers. Meta has been accused by many, including lawmakers and Apple’s CEO Tim Cook, of exploiting personal user data. Interestingly, Mark Zuckerberg was questioned as to whether Facebook would change its existing model to better protect personal user data and Mr. Zuckerberg did not provide a direct answer to this question. Therefore, it is likely that Meta will continue and possibly increase its commercial use of personal user data and as such this is an issue that will need to be considered and addressed by policymakers.

Rosenberg (2022) argues that the exploitation of personal user data will be exacerbated by the mainstream use of the Metaverse as the technology will “not just track where each user clicks, but where they go, what they do, what they look at, even how long their gaze lingers.”

---


5 In December 2021, a female beta tester of Meta’s virtual reality game called ‘Horizon Worlds’ (“HW”) alleged that her avatar was verbally and sexually assaulted by male avatars while she was exploring HW via Business Insider. A woman claimed she was virtually groped by a gang of male avatars in Meta’s metaverse, report says. [online] Available at: https://www.businessinsider.com/meta-woman-claims-virtually-groped-metaverse-horizon-venues-2022-1 [Accessed 3 June 2022].


8 See note 6 above.

9 See note 4 above at pg. 4.
recently filed an application with the U.S. Patent and Trademark Office (USPTO) for head mountable eyeglasses which contain sensors that can track a user’s biometric data such as, facial feature detection, facial movement detection, facial recognition, eye tracking, user mood detection, user emotion detection, and voice detection.\(^\text{10}\)

Security of personal user data is another key issue that policymakers must consider. Major cyber-attacks have led to personal user data belonging to individuals, businesses and governments being circulated on the internet.\(^\text{11}\) Governments and business entities across the globe have had a challenging time detecting, responding to and recovering from cyber-attacks.\(^\text{12}\) As it is intended for individuals to be able to, amongst other things, work, shop, make friends and interact with family and friends in the metaverse, it will be a treasure trove of personal user data for hackers. Currently, there are many vulnerabilities in digital technology and the internet. For instance, hackers can gain access to mobile phones and wearable technologies and make phone calls without your permission, send, and receive texts without your permission, extract your personal information, track your location through GPS and record any of your health issues.\(^\text{13}\) Furthermore, it is anticipated that digital assets will be used in transactions in the metaverse marketplace. Hackers have already been able to steal cryptocurrency and NFTs.\(^\text{14}\) The current flaws in technology will likely be passed on to the metaverse. Moreover, there will likely be new weaknesses and vulnerabilities with respect to the metaverse that may be exploited. Therefore, it is important that policymakers take a proactive approach to create policies that mitigate risks of substantial cyber-attacks and data leaks in the metaverse.

**Anti-competitive behavior**

Undoubtedly, in any activity which generates or has the potential to generate substantial amounts of revenue, there will be a temptation for those entities involved therein to engage in anti-competitive agreements, abuse dominant positions and reduce competition via mergers or acquisitions, for economic gain. As stated previously several of the tech giants have made enormous investments into the metaverse, and as such they have real incentives to impede newcomers from entering this space.


\(^{11}\) See various Apple iCloud hacks where personal information and explicit photos have been leaked and sold on the internet.

\(^{12}\) SRIDHAR, V., 2020. EMERGING ICT POLICIES AND REGULATIONS. [S.l.]: SPRINGER.at pg.167


There are numerous anti-trust/competition law cases which illustrate tech companies abusing dominant positions to restrict competition in a particular market.\(^{15}\) Recently, the US Federal Trade Commission (FTC) commenced an anti-trust case against Meta, in which the FTC alleged that Meta was engaged in an illegal "buy or bury scheme" to stifle competition. In this complaint, the FTC alleged that Meta lured app developers to its platform, surveilled them for signs of success, and then buried or bought them when they became competitive threats.\(^{16}\)

As mentioned above Meta has recently made numerous metaverse related acquisitions including software, hardware, and virtual reality games, namely Oculus, Lemnis Technologies, and Beat Games.\(^{17}\) This rate of Metaverse related acquisitions by Meta is alarming and such activity may lead to a harmful reduction in competition. Earlier this year, it was announced that the FTC and multiple states are investigating Meta’s virtual reality (VR) eyewear Oculus for potential anti-competitive behavior. It was alleged that Meta may be stifling competition by engaging in predatory pricing and discriminating against third parties that are selling apps competing with Meta’s software.\(^{18}\) Considering the foregoing, it is essential for policymakers to consider the most appropriate regulatory strategy to mitigate these risks.

**Content Regulation**

It is anticipated that consumers will be able to enjoy a wide variety of content in the metaverse including live streams, television and movie catalogues, video games and virtual concerts and tours in a more engaging and immersive experience via VR and augmented reality (AR). Content regulation in the age of the internet, social media and over the top (OTT) platforms has proven to be a difficult task.

On the one hand human rights must be observed and protected and on the other hand one must be acutely aware that some content may contain hate speech, terrorism propaganda, bullying,

---

\(^{15}\) One famous example is the US Department of Justice (“the Justice Department”) anti-trust case against Microsoft in the 1990s. In this case, it was determined by the court that Microsoft abused its dominant position in the personal computer (PC) market by making it difficult for PC users that ran on Microsoft’s operating system to install competing software and simultaneously making it difficult to uninstall its web browser, Internet Explorer. This behavior impeded newcomers from entering the market and harmed consumers. Also see the 2010US Justice Dept. anti-trust complaint against Adobe, Apple, Google, Intel, Intuit, and Pixar. In this complaint, the Justice Department alleged that Apple and Google, Apple and Adobe, Apple and Pixar, Google and Intel, and Google and Intuit entered into agreements that prevented the said companies from directly soliciting each other’s employees. These agreements restrained competition for employees thus restricting their opportunities for career advancement and monetization of skills.


intellectual theft, content not appropriate for minors and other harmful content. On this point, Jørgensen (2021)\(^\text{19}\) argues that the challenge in regulating social media platforms lies in the fact that such platforms operate simultaneously in the public and private spheres. On the one hand, these platforms have become an important part of human social infrastructure, however these private commercial entities are mainly concerned with the interests of its shareholders rather than the public interest. The issues that exist currently with respect to content regulation will likely be carried over into the metaverse as metaverse platforms will likely, in most instances, be owned and operated by private commercial entities. Accordingly, it is essential that policymakers consider the appropriate regulatory measures that can address these issues.

**Regulatory strategies**

Regulation is a well-recognized means to, amongst other things, prevent anti-competitive behavior, educate consumers, protect those with unequal bargaining power, promote the efficient use of scarce resources and promote the protection of human rights.\(^\text{20}\) There are numerous regulatory strategies including command and control ("C & C"), incentive-based regulation, and competition law. Each of these forms of strategies have their own strengths and weaknesses.\(^\text{21}\)

**Regulatory Solutions: Command and Control**

The C & C strategy has been used to effectively address a myriad of regulatory issues, as such it is a key strategy that should be adopted to address regulatory issues that arise in the metaverse. The strength of the C & C strategy is that it uses the force of law to impose standards on regulated firms and prohibit them from engaging in activities that do not conform with such standards with relative immediacy. One major drawback of C & C is that there is a risk that it can lead to inflexible and complex rules that can stifle managerial freedom, competition, and innovation.\(^\text{22}\)

The C&C strategy should be used to address privacy issues in the metaverse. Many jurisdictions have adopted the C & C strategy via data protection law regimes which regulate the collection, processing, keeping, use and disclosure of personal user data and outline fines for non-compliance. Perhaps, the most well-known data protection laws are the EU’s General Data Protection Regulation (GDPR). The GDPR applies to entities that are based inside or outside of the EU that collect and process personal data of EU residents. However, policymakers in each jurisdiction must consider whether their current data protection laws are fit for purpose considering the advancements in technology and the increasing interconnectedness of the world and make necessary amendments. For instance, currently the Bahamian Data Protection (Privacy of Personal Information) Act ("DPA") does not specifically address the collection of biometric data. Furthermore, unlike the GDPR, the Jamaican Data Protection Act \(^\text{23}\) and the Barbadian Data

---


\(^{21}\) See note 20 above at pg.108

\(^{22}\) See note 20 above at pg. 113.

\(^{23}\) See section 3 of the Jamaican Data Protection Act, 2020
Protection Act\textsuperscript{24} the DPA does not apply to data processors that do not have some form of establishment\textsuperscript{25} in The Bahamas.

One issue that is apparent in the enactment of data protection laws is the enforcement of such laws against tech giants. Some of the European regulators have found it difficult to investigate and enforce against tech giants for breaches of the GDPR due to lack of resources. For instance, the Irish Council for Civil Liberties in its 2021 report on the enforcement capacity of data protection authorities entitled “Europe’s enforcement paralysis” ICCL’s 2021 found that 98% major GDPR cases referred to Ireland remain unresolved. If European countries are having such difficulties, it is likely that smaller countries such as The Bahamas, Jamaica and Barbados do not individually have the necessary human, financial and technical resources to properly enforce the data protection laws against tech giants. Perhaps, jurisdictions such as those in the Caribbean can harmonize data protection laws and form a unified data protection body with pooled resources and capacity to enforce data protection laws against tech giants.

The C & C strategy has also been used in some jurisdictions to regulate content broadcasted on television and radio via Codes of Practice.\textsuperscript{26} Internet intermediaries have been left to self-regulate content on the internet. However, considering the increase in misinformation and other harmful content on the internet, it is arguable that self-regulation has not been successful. As stated above, internet intermediaries are private commercial entities serving the interests of shareholders, therefore such entities cannot be expected to independently prioritize public issues. The EU has proposed a piece of legislation called the Digital Services Act (“DSA”) which is intended to compel internet intermediaries to aggressively police harmful content on their platforms by holding them responsible for their content moderation practices in the digital space.\textsuperscript{27}

The DSA proposes to implement, amongst other things, a clearer “notice and action” procedure where users will be allowed to report illegal content online and internet intermediaries will have to act quickly with respect to such reports, and stronger safeguards to ensure notices are processed in a non-arbitrary and non-discriminatory manner and with respect for fundamental human rights. Additionally, the DSA will require online platforms that are accessible to minors to implement specific measures to protect them, inclusive of prohibiting advertising targeted at minors.\textsuperscript{28}

Robust strategies such as the DSA will be useful in tackling content regulation in the metaverse, therefore policymakers must continue this approach.

\textit{Regulatory Solutions: Incentive based strategies}

Incentive-based strategies encourage firms to reduce harmful conduct by granting financial rewards to those firms with good behavior. Incentive-based strategies are cheaper, more flexible\textsuperscript{24} See section 3 of the Barbadian Data Protection Act, 2019
\textsuperscript{25} See section 4 (1) – 4(3) of the DPA.
\textsuperscript{26} See the Utilities Regulation and Competition Authority Code of Practice for Content Regulation ECS 08/2020
and encourage managerial freedom. However, one drawback of incentive-based strategies is that they are likely to influence the behavior of responsible firms more effectively than irresponsible firms.29

Incentive-based strategies should be considered to address some metaverse related issues30. As stated previously, the core business of some tech giants such as Meta is selling targeted sophisticated advertising to advertisers. This core business will likely be carried over into the metaverse as it is immensely profitable. Financial rewards can be granted to those platform owners in the metaverse that create subscription-based, ad-free metaverse platforms as an alternative to the traditional ad-based platforms. There are likely to be some consumers that are willing to pay for the use of the subscription based metaverse platforms as tradeoff for safeguards against their personal user data being sold to third parties.31 Also, financial rewards can be granted to those entities that can verify that they have implemented internal policies that (i) educate platform users on how their personal data is collected, stored and used and (ii) obtain consent from users on each occasion that their personal user data is collected and used.

**Regulatory Solutions: Competition laws**

Competition laws are thought to be less intrusive into the management of firms and allows a given market to be flexible. One drawback of competition laws is that they do not typically address technical or operational issues. Policymakers and regulators should be wary that platform owners, manufacturers of software and hardware and those entities conducting business in the metaverse will likely engage in anti-competitive behavior. Regulators and policymakers have long relied on competition/anti-trust laws to address unfair competition tactics. The use of the competition law/anti-trust strategy will be key in dissuading anti-competitive behavior and appropriately penalizing those that engage in anti-competitive behaviors. However, policymakers in each jurisdiction must identify and resolve those shortcomings in their respective competition law regimes. Moreover, it is necessary for policymakers to attempt to grasp the economics of the emerging marketplace in the metaverse to determine whether new rules need to be implemented.

The EU is leading the vanguard in this regard by its proposal of the Digital Markets Act32 (“DMA”). However, the US is taking a similar approach with the following bills currently before Congress, namely, the American Innovation and Competition Online Act, the Open App Markets Act and the ACCESS Act.33 It is anticipated that the DMA will address various digital issues in a borderless digital economy.34 The DMA is intended to supplement existing competition rules and aim to

---

29 See note 20 above at pg. 113.
30 See note 20 above at pgs. 115-116.
31 See note 4 above at page 7.
34 Carugati, C. and Martins, C., 2022. Insights for successful enforcement of Europe’s Digital Markets Act The European Commission will enforce digital competition rules against big tech; internally, it should ensure a dedicated process and teams; externally, it should ensure cooperation with other jurisdictions and coherence with
preventing ‘gatekeepers’ such as powerful social media platforms, online search engines, and web browsers from imposing unfair “conditions on businesses and end users and ensuring the openness of important digital services.”

The DMA proposes to impose certain obligations on those entities that fall within the scope of the term gatekeepers and penalize them for failure to comply with its provisions. For instance, gatekeepers will be required to allow end users to easily un-install pre-installed apps, allow end users to easily unsubscribe from core platform services of the gatekeeper, and allow third parties to inter-operate with the gatekeeper’s own services. Under the DMA, gatekeepers will be prohibited from, amongst other things, using the data of business users in circumstances where gatekeepers are competing with them on their own platform, requiring app developers to use gatekeeper’s services in order for their apps to appear in the gatekeeper’s app store, and promoting its own products in a more favorable manner compared to those of third parties.

Proposed competition rules such as these can definitely be used as a strategy to address competition related issues in the metaverse and as such policymakers must continue to act proactively.

**Conclusion**

Despite the numerous benefits of the proposed metaverse, policymakers and regulators must be wary of its inherent dangers. Although many are concerned that regulation of the metaverse will stifle innovation, platform owners cannot be left to self-regulate as evidenced by the numerous infringements of competition law by the tech giants, the dissemination of harmful content on social media, the ubiquitous misuse of personal user data and cyber-attacks. In this paper, it has been proposed that policymakers and regulators take vital steps to educate themselves on the metaverse so that they are in the position to proactively consider the possible issues that may arise therein. Moreover, this paper beckons policymakers and regulators to improve existing C & C strategies such as the GDPR, develop competition rules such as the DMA that specifically address metaverse related issues and to implement innovative incentive-based strategies.

---


36 See note 35 above.