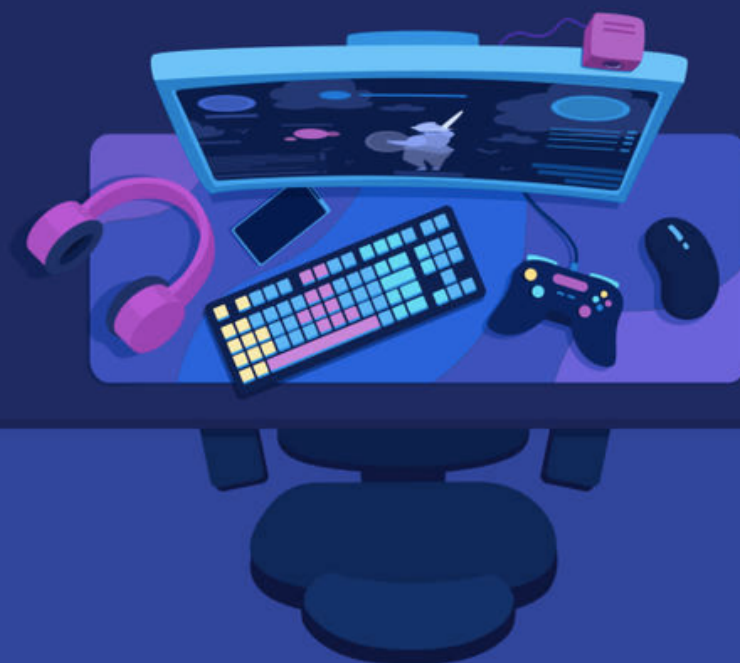




Game On!

Roadmap For User Centric Gaming Regulation In India

July 2022



Koan Advisory Group

Game On!

Roadmap For User Centric Gaming Regulation In India

July 2022



Authors

Aditi Chaturvedi, Akshat Agarwal, Priyesh Mishra

©2022 Koan Advisory Group

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from Koan Advisory Group

contactus@koanadvisory.com | www.koanadvisory.com

TABLE OF CONTENTS

List of Abbreviations	05
------------------------------	----

Executive Summary	07
--------------------------	----

Introduction	10
---------------------	----

Regulatory Landscape	11
-----------------------------	----

Chapter I: Addressing Behavioural Issues in Gaming	12
---	----

Introduction	12
I. Gaming Disorder	12
II. Associated Harms	13
III. Vulnerability to Cybercrimes	14
IV. Contemporary Regulatory Responses	14
a. Gaming disorder and associated harms	14
b. Inappropriate content	15
V. Lessons from International Best Practices	16
VI. Recommendations for India: The Case for Self-Regulation	18

Chapter II: Addressing Financial Issues	22
--	----

I. Financial Integrity	22
Current Practices	23
a. Financial propriety in user accounts through self-regulation charters	23
b. Lessons from International Best Practices	23
II. Virtual Currencies	24
Current Practices	26
a. Activity based regulation	26
b. Risk-based approach	26
c. Regulatory sandbox	26
d. Value based regulation	26
e. Customer due diligence	27

III. Microtransactions	27
Current Practices	29
a. Regulating closed virtual currencies as CVCs	29
b. Regulating chance-based elements in online games (lootboxes)	29
c. Value-based approach	29
d. Legal clarity	30
e. Self-regulation	30
IV. Recommendations for India	32
a. Financial integrity of gaming platforms	32
b. Recommendations for the use of CVCs	32
c. Recommendations for micro-transactions	33

Chapter III: The Metaverse and Future Issues in Gaming 34

Introduction	34
Issues in the Metaverse	34
I. User Protection	35
a. Online harassment	35
b. Data collection and Manipulative advertising	36
II. Ownership and Competition in the Metaverse	37
a. Mods, User created content and Intellectual property	37
b. Virtual items, NFTs and Ownership	38
c. Competition law, Gatekeeping and the Metaverse	38
III. Contemporary Regulatory Responses	39
a. South Korea	39
b. Case study for standard-setting: The OASIS Consortium	40
IV. Recommendations for India	41

Notes 43

LIST OF ABBREVIATIONS

ADHD	Anthropometry refers to the measurement of the size and proportions of the human body.
AI	Artificial Intelligence
AIGF	All India Gaming Federation
AR	Augmented Reality
ASA	Advertising Standards Authority (UK)
ASCI	Advertising Standards Council of India
AVGC	Animation, Visual Effects, Gaming and Comic
BIS	Bureau of Indian Standards
BSA	Bank Secrecy Act
CAGR	Compound Annual Growth Rate
CDD	Consumer Due Diligence
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CFT	Combating the Financing of Terrorism
CVC	Convertible Virtual Currencies
DLT	Digital Ledger Technology
DPA	Data Protection Authority
DPIIT	Department for Promotion of Industry and Internal Trade
DSM	Diagnostic and Statistical Manual of Mental Disorders
EGBA	European Gaming and Betting Association
EGF	E-Gaming Federation of India
ESRB	Entertainment Software Rating Board
EU	European Union
EULA	End User License Agreement
FATF	Financial Action Task Force

FIFS	Federation of Indian Fantasy Sports
ICD	International Classification of Diseases
ICO	Information Commissioner's Office's
IEEE	Institute of Electrical and Electronics Engineers
IPC	Indian Penal Code
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
IT	Information Technology
KCC	Korean Communications Commission
KYC	Know Your Customer
LGBTQI	Lesbian, Gay, Bisexual, Transgender, Queer, Intersex
MGA	Malta Gaming Authority
MIB	Ministry of Information and Broadcasting
MMORPG	Massively Multiplayer Online Role-Playing Games
NFT	Non-Fungible Token
NITI	National Institution for Transforming India
P2P	Peer to Peer
PEGI	Pan-European Game Information
PMLA	Prevention of Money Laundering Act
RBI	Reserve Bank of India
RMG	Real Money Games
RTS	Remote Gambling and Software Technical Standards
SRO	Self-Regulatory Organization
STQC	Standardisation Testing and Quality Certification
UNODC	United Nations Office on Drugs and Crime
VFA	Virtual Financial Assets
VR	Virtual Reality
WHO	World Health Organization

Executive summary



Behavioural Issues in Gaming

This report argues for the adoption of a harm-reduction approach to deal with the behavioural issues related to gaming, with industry playing an active part in these efforts. So far, India's gaming interventions have largely been reactive bans at the state level, an approach ill suited to the ambitions of a Digital India with a thriving gaming industry. In fact, approaches that limit themselves to restricting individual access to games are falling out of favour worldwide. For instance, in August 2021, South Korea removed its 'Cinderella Law' that prohibited children from gaming late at night, instead focusing on harm reduction through in-game warnings and clinical treatment.

Elsewhere, the harm reduction approach has shown immense promise in addressing concerns around problematic gambling. Jurisdictions like the United Kingdom, Sweden, and Denmark have created a holistic framework to provide for preventive and curative interventions. These interventions range from responsible game design so that games do not exploit or encourage problem gambling behaviour, to clinical treatment facilities for problem gamblers. They also oblige gambling service providers to monitor user behaviour and patterns of play to identify vulnerable players.

Active industry participation is an essential ingredient for the success of a harm reduction approach. The pace of technological change has challenged state regulatory capacity and working with industry will provide the much needed expertise. The United States' Entertainment Software Rating Board (ESRB) is a good illustration of this point – it was an industry-led response to concerns of inappropriate content in gaming and is today one of the most reliable and recognised content rating systems in the world. In India, industry bodies like FIFS and AIGF have initiated their own efforts through self-regulation charters. The government could work with these and similar bodies to develop principles-based rules to ensure informed user choice and responsible game design, empowering users and ensuring that games are not deliberately designed to foster addiction. By targeting harms and allowing for flexibility in solutions, India can tackle behavioural issues in gaming while fostering the growth of the industry.

Financial Issues in Gaming

With a large diversity of gaming products on offer, it is important to ensure financial integrity on the part of operators of real money games and prevent virtual currencies and micro-transactions being used for illegal purposes such as money laundering. We suggest the first objective is best fulfilled by leveraging self-regulatory organisations (SROs) like the FIFS and AIGF, which prescribe certain measures that include requiring members to adopt an escrow mechanism and maintain a separate account for the prize pool and another for operational expenses and prescribe user verification for payments. Further, SRO charters can improve financial conduct by prohibiting conflicts of interest (such as platforms offering a line of credit or payday loans to players to play real-money games) and imposing standards of consumer empowerment through technology and design. Additionally, global best practices have useful guidance for developing financial responsibility for real money games of skill.

To deal with money laundering, we recommend a risk-based approach to identify which virtual currencies or microtransactions will most likely be used for illegal transactions. For instance, convertible virtual currencies (CVCs), which can be exchanged for fiat currency, need greater scrutiny. The US FinCEN designates some operators such as Linden Lab (the creators of Second Life and convertible Linden Dollars) as ‘money transmitters,’ making them subject to anti-money laundering laws. Further, high-risk users can be identified and asked to fulfil more stringent consumer due diligence requirements. Value limits on account balance, transaction limits, transaction frequency restrictions may be assigned to customers depending on diligence requirements. We recommend that India’s anti-money laundering law be updated to explicitly cover transactions made using CVCs, and that high-risk use cases, products and behaviours be proactively identified in partnership with industry SROs for focused regulation.

Developers in the meantime have introduced new ways to monetise their games. Of these, in-game microtransactions are the most successful and popular mechanisms to earn money. Data show that user spends to acquire in-game items have increased significantly. Our report considers two challenges associated with in-game microtransactions. One, it explains the money laundering associated with the exchange of in-game items in secondary markets. To address the challenge, virtual items can in certain cases be treated as convertible virtual currencies so anti-money laundering (AML) laws apply to them. The report also asks whether chance-based elements such as loot boxes need better monitoring and scrutiny, as they tend to introduce the risk of gambling into games of skill. Countries vary in their approach to regulating lootboxes, based on their assessment of the value of the items in the box. For example, while the Netherlands and Belgium have sought to regulate loot boxes as gambling, the Netherlands regulates lootbox items only if they have economic value, while in Belgium lootboxes are covered under gambling law if they can be considered money’s worth due to their subjective value to the players. That said, there is a need for legal clarity on whether a lootbox embedded in a game of skill can be considered separate from the game. Some of these questions are before the courts. Owing to these complexities, though many countries acknowledge the harms linked to some lootboxes, there is no regulatory certainty, and they are reluctant to classify them as gambling. In the case of India, we recommend that MeitY and SROs collaborate to develop guidance for the gaming industry that would minimise the harms associated with chance-based items embedded in games of skill.

Besides financial concerns, lootboxes are also associated with concerns of an adverse behavioural impact on users. Several countries have responded with measures to increase consumer information, with China and South Korea introducing rules that require lootboxes to disclose the odds of winning certain items. The EU too has recommended a consumer-protection focused approach to mitigate psychological and financial harms to consumers. A study by the European Parliament recommended protective measures including transparency, age restrictions and parental controls, at every stage of the consumer journey. While encouraging industry self-regulation efforts, the study does not rule out prescriptive regulation if industry efforts are found inadequate. These approaches contain principles that India can integrate into any regulation lootboxes. First, user empowerment measures to enhance consumer agency and choice through greater transparency. Second, proportionality to let regulators target the offending portions of the game, treating these as severable from the rest of the game, and preventing broad bans. Finally, as highlighted earlier, a risk-based approach to allow for comprehensive understanding of the harms caused by a particular issue and a focus on mitigating these harms.

Metaverse and Future Issues

The metaverse refers to simulated digital environments that mimic a shared physical space, using technologies such as AR and VR. It is a collection of virtual worlds where users can play, create, work and communicate, characterised by immersiveness, persistence and interoperability. The metaverse is intrinsically linked to gaming,

which pioneered concepts like virtual worlds (in games such as World of Warcraft and Second Life) and raises new regulatory questions and challenges.

Even in its infancy, we can identify some challenges raised by the metaverse. Existing issues like online bullying and harassment will be exacerbated, with user immersion deepening the impact of such behaviour on survivors. Reported incidents of sexual harassment in Meta's Horizon Worlds underline the need to enhance user safety, through ex-ante and ex-post measures by both industry and regulators. While industry can offer greater control to users, such as the option to block offending users or creating a 'personal zone' around themselves that other players cannot enter, governments can extend existing laws around harassment to the metaverse, offering aggrieved parties remedy. Similarly, as data collection skyrockets with the metaverse, and physiological data enters the fray through wearable technologies, a combination of industry and government initiatives may be required to safeguard privacy. While industry can evolve minimum standards for advertising and transparency, a future data regulator could outline categories of data that cannot be used for advertising or tracking.

Constructs of ownership and intellectual property may also see changes with the metaverse, which is likely to see a creator economy of user-generated content including virtual items, outfits, and other artefacts. The enhanced contribution of user content in games may prompt changes in how user generated content or 'mods' are protected. While the current jurisprudence (based on a 1998 case) treats mods as derivative works that are unprotected, economic and business realities might prompt changes to this approach. Beyond intellectual property, the actual ownership of virtual items is likely to be based on non-fungible tokens or NFTs, which will help track the authenticity and provenance of such items. NFTs may also be an interoperability solution, allowing users to carry items from one metaverse 'world' to another. Finally, competition regulators around the world are likely to keep a close eye on metaverse markets as part of an overall shift in attitudes toward technology markets. The metaverse is likely to require users to purchase hardware resembling game consoles, giving manufacturers the opportunity to bundle software or control distribution through closed online stores. With platform-based services and distribution models under scrutiny in the mobile ecosystem, the consolidation and concentration of power in gaming or metaverse markets may also draw increased attention from competition authorities.

Nascent efforts to regulate the metaverse can be relied on to guide India's own forays in this area. South Korea has been a first mover, announcing a long-term road map for metaverse related industries, including metaverse academies to train local experts, Korean language institutes in the metaverse, and making metaverse avatars for officials as part of a 'Metaverse Seoul'. The Korean Communications Commission (KCC) has also constituted a 30 member expert committee to look into safety aspects of the metaverse. Industry-led efforts can be seen in the form of the OASIS Consortium, which counts Roblox and Epic Games amongst its members. OASIS seeks to promote ethical standards and released its first User Safety Standards in January 2022. These efforts can be replicated in India with an expert body. Industry should be encouraged to develop standards that ensure user safety, data privacy and the sustainable and inclusive growth of the metaverse. Capacity building, ensuring user safety and basing future regulatory interventions on multidisciplinary research are key steps in developing India's metaverse industries, including metaverse gaming products.





Introduction

In a 2019 letter to its shareholders, video streaming giant Netflix said that in terms of screen time, it competed with (and lost to) the hit game *Fortnite* more than with HBO.¹ The statement captures an important truth of today's media and entertainment landscape, which is characterised by variety, dynamism and changing boundaries. With user generated content, multiple formats of audio and audio-visual products and increasing internet bandwidth, the most precious commodity remains consumer attention. The years following Netflix's statement went on to prove it – the global gaming industry grew at a CAGR of over 38% in 2020 amidst the pandemic to reach a value of USD 229 billion in 2021², and is estimated to reach a value of USD 546 billion by 2028.³

As more people turn to gaming for entertainment and recreation, it is far from being the niche hobby it may have been considered in earlier decades and has become one of the drivers of technology and innovation in the global media and entertainment market. Interestingly, in November 2021, Netflix announced its own foray into gaming, adding a mobile games catalogue to its subscription benefits, showing an understanding of the shifting sands of entertainment.⁴

In this global surge in the gaming industry, India stands uniquely positioned to become a new world leader. With a large young demographic, a proven track record in the IT/ITeS sectors and growing domestic demand for gaming (over 500 million Indians played online games in 2022),⁵ India has the potential to establish a foothold in gaming markets around the world. Encouragingly for the Indian gaming industry this understanding is shared by the Prime Minister, who has articulated an aspiration for Indian games to entertain people around the world, while also being a powerful vehicle for Indian soft power.⁶ Ironically however, the largest obstacle to realising this potential lies in the lack of any coherent framework of governance or regulation for this sector. This is a result of policymakers' lack of interest in the area, and a paucity of understanding. Bridging the gap will require an articulation of the issues and challenges in the gaming industry, the various approaches that other jurisdictions have taken to tackle them, and potential policy and regulatory paths for India to take to balance market and consumer interest.

This report is an attempt to bridge that gap, in the form of a ready resource for policymakers and practitioners on today's most prominent public interest issues in gaming. These are divided into the two categories of concerns most often raised by Indian legislators and policymakers – the behavioural harms associated with gaming addiction and other unhealthy gaming practices, and the financial harms associated with the monetary aspect of gaming, whether in games played for stakes or in virtual items, in-game purchases and micro-transactions. This is followed by a closer look at a specific issue that combines behavioural and financial concerns: a case study of the 'lootbox' mechanic that has become a fixture in many games. The report concludes with a look at what we can expect in the future, examining some of the early issues emerging from the development of the metaverse, touted by some as the future of the internet, and the expected trends in metaverse gaming.

We examine jurisdictions including the United States, the United Kingdom, the European Union, Singapore, and Japan, and hope to provide the context and perspectives to enrich discussions around gaming regulation in India, to flag key issues policymakers will need to grapple with, and some tools and resources to begin thinking about solutions. With an encouraging regulatory framework and a dynamic, future-ready approach to problem solving, we hope to see India's gaming industry grow to its real potential in the coming years.

Regulatory Landscape



Before delving into the specific issues discussed in this report, we briefly describe the legislative/ regulatory landscape around gaming in India. Gaming refers to engagement with or the playing of games over a digital or electronic network, using an electronic device like a mobile phone, computer, or a dedicated console. As they are played using a digital/electronic network, these games are also referred to as 'online games'. Gaming operates in a rather uncertain regulatory environment in India. For regulatory purposes, games are classified into two categories:

1. **Games of chance** – These include games like ludo and roulette, where the winning outcome is determined predominantly by an element of chance.
2. **Games of skill** – These include games like chess and fantasy sports, where the winning outcome depends on the skill of the player/s.

The jurisprudence around gaming has undergone a sea change in the last few years. While the laws governing games of chance are fairly clear, the regulation of games of skill is still evolving in India.

Regulation of Games of Chance

Under Indian law, games of chance, when played for monetary stakes, constitute betting and gambling. As per the division of legislative powers in the Constitution of India, betting and gambling falls under the jurisdiction of states. It is governed by state-specific gaming and police laws, closely modelled on the Public Gambling Act, 1867. It is prohibited to facilitate such activities for the general public in most Indian states. However, states like Nagaland, Sikkim, Meghalaya, and Goa permit certain forms of chance-based games as licensed activities. While these laws clearly apply to physical/offline betting and gambling, their application to online betting and gambling is debated. This is because the ambit of state laws is limited to the state's territorial boundaries. Online games transcend these boundaries, making the enforcement of these laws more challenging.

Regulation of Games of Skill

Until recently, skill based games were also governed by state laws on betting and gambling. Many states including Tamil Nadu, Andhra Pradesh, Karnataka and Telangana enacted laws to prohibit games of skill played for monetary stakes. As a result, skill game formats like rummy, poker and fantasy sports were banned in these states. Upon judicial challenge, these laws failed the test of constitutionality and were consequently read down by several high courts. In separate decisions of the high courts of Madras, Karnataka and Kerala, the regulation of games of skill under betting and gambling laws was held to be legally untenable. These decisions have created a regulatory vacuum around games of skill.

Recent developments

In February 2022, the question of jurisdiction over online games gained some clarity. Responding to a parliamentary question the Ministry of Electronics and Information Technology (MeitY) clarified that all online gaming platforms are intermediaries under the Information Technology Act, 2000 and the rules thereunder. As such they are bound to observe the due diligence prescribed under IT Rules, 2021. This was a shift from the central government's previous stance that online gaming regulation is a state subject. It is important to point out that the due diligence requirements prescribed under the IT Rules, 2021 are intended for social media platforms and digital content platforms (like Netflix or Hotstar). As such they may not be fit to regulate the rather complex online gaming space. We foresee that at some point, MeitY will have to issue specific guidelines for the online gaming sector.

Chapter I: Addressing Behavioural Issues in Gaming

Introduction

India is home to more than 510 million gamers, and by 2025 the number is expected to reach 650 million. Most gamers enjoy playing games as part of a balanced lifestyle. Besides entertainment, games also offer educational, physiological, psychological, recreational and social benefits.⁷ For people with physical disabilities or any form of neurodiversity, immersive gaming provides a sense of enablement and social connect.⁸ Nevertheless, a small minority of gamers face significant challenges in striking a balance between gaming and other physical, social, educational or occupational activities. This behaviour is clinically recognised as ‘gaming disorder’. Over a period of time, such a lifestyle results in serious physical and mental health risks for such gamers.

Gaming disorder has emerged as a key concern for policymakers in India. The existing regulatory interventions are paternalistic in their approach and evince a lack of understanding. This chapter aims to address the knowledge gap and facilitate better informed policymaking. It unpacks the spectrum of behavioural issues associated with gaming, equipping the reader to differentiate between passionate engagement with games and pathological gaming. It suggests a more nuanced regulatory approach than is currently followed in India, one informed by global best practices, intended to strike a balance between social welfare and market innovation.

I. Gaming Disorder

In 2018 the World Health Organisation (WHO) formally included gaming disorder in its International Classification of Diseases (ICD). It defined⁹ gaming disorder as a behavioural issue characterised by a *pattern of persistent or recurrent gaming behaviour* (either online or offline) that manifests as:

1. Impaired control over gaming (e.g., onset, frequency, intensity, duration, termination, context)
2. Increasing priority given to gaming to the extent that it takes precedence over other life interests and daily activities
3. Continuation or escalation of gaming despite the occurrence of negative consequences.

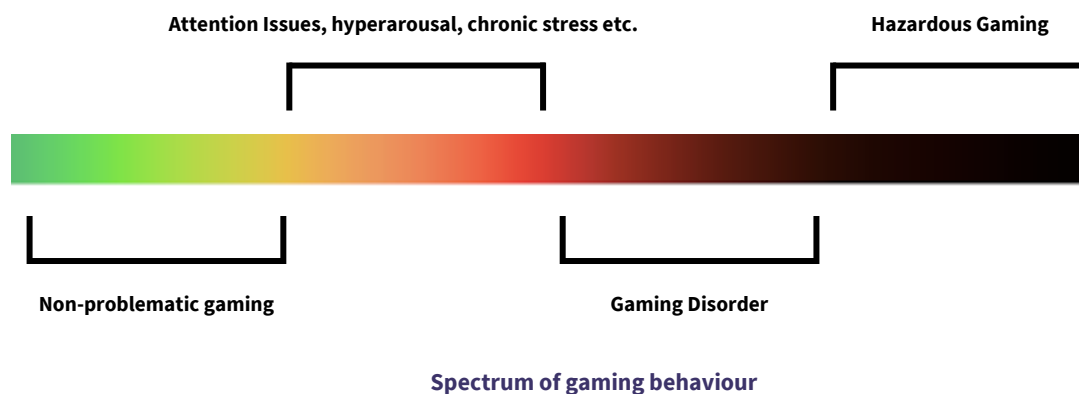
For the disorder to be diagnosed, the behaviour pattern must be *‘of sufficient severity to result in significant impairment in personal, family, social, educational, occupational, or other important areas of functioning and would normally have been evident for at least 12 months’*.¹⁰

The ICD also recognises an aggravated form of gaming disorder called hazardous gaming. It is defined as a pattern of gaming, either online or offline, that appreciably increases the risk of harmful physical or mental health consequences for the individual or others around the individual.

Academic controversy over the classification of gaming disorder

The inclusion of gaming disorder in the ICD has been criticised. A group of 34 academics from around the world questioned the move in a joint letter, citing the lack of sufficient evidence.¹¹ They argued that while problematic gaming behaviour is a legitimate concern that needs further research, the volume of evidence required to classify it as a behavioural disorder is lacking. The Diagnostic and Statistical Manual of Mental Disorders (DSM), the American Psychiatric Association’s authoritative manual on mental health issues, echoes a similar view. In its fifth edition published in 2013, the DSM classified *‘internet gaming disorder’* as a condition that requires further research.¹²

It is important to note that the ICD conceptualises problematic gaming as a spectrum of behaviour, with positive or non-problematic gaming at one end and addictive and hazardous gaming¹³ at the other. Psychological harms like attention disorder and chronic stress lie between the two extremes. These harms are associated with factors like the duration of gaming and the game content. Policymakers should be mindful of the fact that while addictive and hazardous gaming require urgent interventions, other associated harms also need due consideration.



II. Associated Harms

Prolonged engagement with video games does not always result in gaming disorder. It may however lead to other physical and psychological harms. These harms relate to multiple factors, including the duration of engagement and gaming content. People who spend more time playing video games may develop issues like attention deficit disorder (ADHD).¹⁴

The most common concern expressed about video games relates to virtual violence. In the past, games like *Mortal Kombat* and the *Grand Theft Auto* series faced headwinds due to their depictions of violence. In 2014, Target and Kmart, two of the leading retail stores in Australia, removed *Grand Theft Auto V* from sale in their stores following complaints about their depiction of violence on women.¹⁵ In the United States, video games like *Counter Strike* and *Call of Duty* are repeatedly blamed for incidents of mass shootings.

Violent games have a stronger correlation with behavioural issues like impulsiveness and can cause psychological stress resembling Post Traumatic Stress Disorder.¹⁶ While there is a substantial body of research establishing a correlation between exposure to violent content and growing aggression in teenagers and young adults, it has yet to establish a causal connection between the two.¹⁷ Experts do agree however that children should not be exposed to violent content,¹⁸ as it may desensitise them to violence and in some cases lead to behavioural issues.

The issue of exposure to violent content is exacerbated by ubiquitous internet access and the sheer number of games on market. More than fifty thousand games were added to the Google Play Store in the first quarter of 2021 alone.¹⁹ In many countries, video games are age-rated and the physical sale of games regulated to ensure that they are not sold to children younger than the prescribed age. As game distribution channels move online, however, enforcement becomes difficult. Global platforms like Steam are not bound by such ratings as age-rating laws are not uniform worldwide.²⁰ Thus, children of any age can access games with mature themes like violence, sexual activity, nudity, and substance abuse.

III. Vulnerability to Cybercrimes

Some of the most played games in the world like Minecraft, Fortnite and PUBG allow multiple players to play simultaneously and interact in real time. While such communication enhances the gaming experience, it also makes children vulnerable to cybercrimes like grooming.²¹ Grooming can be sexually abusive in nature, but it can also force victims into crime such as distributing drugs or moving money between bank accounts.²²

Communication for the purpose takes place either through in-game chat or through gaming-adjacent communications platforms such as Discord and Twitch.

Online gaming communities are also hotbeds of extremist propaganda. Europol's EU Terrorism Situation and Trend Report (TE-SAT) 2021 found that video games and video game communication applications were increasingly used in 2020 to share terrorist and extremist propaganda to radicalize young people. The report also notes that suspects arrested for planning right-wing terrorist or extremist attacks are increasingly young, and some are minors. Some online communities are also propagating hatred against minority groups including (though not limited to) Black and ethnic minorities, Jewish people, women, and the LGBTQI community. Gamers identifying with such sub-groups are disproportionately subjected to many forms of bullying and harassment.

IV. Contemporary Regulatory Responses

a. Gaming disorder and associated harms

Given the correlation between length of engagement with games and gaming disorder, limiting access to games is an obvious policy response. Most early interventions across countries like China and South Korea adopted this approach by either prohibiting access to games or imposing selective or qualified shutdowns. For example, in China, game time for children younger than 18 is limited to an hour a day - from 8 pm to 9 - and on Fridays, Saturdays and Sundays. Similarly, in April 2020, the local government of the Kagawa prefecture in Japan passed an ordinance limiting game time for minors to 60 minutes on weekdays and 90 minutes on holidays. Prohibition as a regulatory approach is ineffective in addressing gaming disorder. For example, in 2011, South Korea enacted a shutdown law known as the 'Cinderella Law', which prohibited children under 16 from playing video games for a six-hour period from midnight. A subsequent impact analysis revealed that the law had failed to limit the time spent by minors on gaming activities.²³ In August 2021 the South Korean government announced its decision to abolish the shutdown law. The approach further presumes that all gaming formats are equally addictive – an incorrect assumption. For example, research suggests that formats like Massive Multiplayer Role-Playing Games (MMORPGs) pose a higher risk of addiction.

An alternative to limiting access is to explore balanced approaches designed to reducing harm. Harm reduction refers to policies that aim to reduce the adverse consequences associated with the use of addictive substances, without necessarily reducing the degree of substance use itself. Thus, instead of restricting or limiting access to games, the approach seeks to address the harms associated with gaming disorders. This may be achieved through ex-ante measures like in-game warnings, reminding users to take a break from gaming, or ex-post measures like specialised clinical treatment for people displaying problematic gaming behaviour. South Korea, for example, has included counselling and treatment as a part of its national policy to address gaming addiction. Similarly, the UK's National Health Service recognises gaming addiction as a mental health issue and offers clinical treatment for patients 13-25 years old.²⁴ Unlike blanket bans, harm reduction interventions are proportional and constitutional.

Targeted harm reduction interventions in India will require enhanced understanding of factors like the principles of game design, vulnerable demographics, the addiction potential of different games etc. However, there is a paucity of local research in this regard. Even in advanced jurisdictions like the UK, there is a recognition that the

lack of quality research is preventing appropriate action.²⁵ Similarly in India, prolonged engagement with games is erroneously equated with addiction. For example, on December 3, 2021, while discussing the issue of gaming addiction in Parliament, an increase in the duration of playing games was cited as evidence of increased gaming addiction.²⁶ While there is a correlation between the time spent playing and the incidence of gaming disorders, the duration of play by itself does not signify gaming disorder. In similar vein, the prevalence of gaming disorder is often overstated. Research involving several studies of adults in the US, UK, Canada and Germany estimated a 0.3 to 1.0% incidence of gaming disorder. A study published in 2018 estimated an overall prevalence of 3.50% among schoolchildren in India.²⁷

Game Design and Behavioural Issues

Games involving interactive gameplay are designed to maximise user engagement. This is especially true for games that require continuous inputs from gamers. In the past the gaming industry relied on a ‘premium’ model, where users paid a sum of money upfront to buy a hard copy of a game, which was the only form of monetisation available to the creators and publishers of games. The advent of online gaming introduced novel avenues for monetisation like microtransactions or subscriptions. These incentivise game design to keep users engaged.²⁸

According to Dr Mark Griffiths, a leading expert on gaming disorder, there are structural similarities in the tools used by the video game industry and the gambling industry to keep a user hooked. These include ‘high event frequencies (speed of play), near misses, variable ratio reinforcement schedules (rewarding players on irregular intervals instead of regular, predictable intervals), and use of light, colour, and sound effects’.²⁹ Random rewards are also among the most common techniques used to prolong engagement. Match-three puzzle games such as King’s Candy Crush Saga demonstrate reward mechanics in action: the game rewards players with incentives, such as pop-up motivational slogans or free ‘spins’ offering another random chance to win ‘boosters’ to enhance gameplay, at random intervals.

Another example of tools used by the industry are ‘dark game design patterns’.³⁰ These are game design elements which trick a user into playing continually. A common example of dark gaming design patterns is ‘grinding’. This refers to making gamers perform repetitive tasks to make progress in a game. Grinding prioritises the time spent by a gamer over their skill as a metric of making progress. The trick is generally used in multiplayer games or social media games like Farmville. In Farmville, a player can grow crops which can be harvested to earn in-game rewards. The more crops one grows, the more rewards they earn and the easier it becomes to ‘level up’ in the game. Another design trick is called ‘*playing by appointment*’, which encourages players to return to the game at a particular time. For example, in Farmville each crop takes a certain amount of time to grow before it can be harvested. If a crop is not harvested within a certain time period after it is ready, it withers and loses its value. This puts an obligation on the player to play according to the schedules offered by the game.³¹

b. Inappropriate content

Globally, the best practice to safeguard against inappropriate content is through a graded age-rating system, which is an example of a harm reducing regulatory approach. Here, instead of classifying gaming content based on a fixed age of majority, it is rated in a tiered manner. For example, the ESRB rating system grades games into – E (suitable for all age groups), E10+ (suitable for ages 10 and above), T (suitable for ages 13 and above), M (suitable for ages 17 and above) and A (suitable for ages 18 and above). The rating system also uses content descriptors to inform users that a certain game contains themes that may be of concern. Examples of such themes include violence, language, nudity, sexual references etc.

This approach has precedent in Indian law. The code of ethics for digital media platforms, under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, provides for a graded content classification framework. The rules mandate online curated content providers like Netflix or Hotstar to classify the content on their platform based on factors like themes and messages, violence, nudity etc. The certification of films for public exhibition under the Cinematograph Act also embodies the same principle.

V. Lessons from International Best Practices

Besides gaming laws, it is worthwhile to analyse the regulatory approaches adopted by different jurisdictions. Towards this, we study the regulations put in place across countries like the UK, Sweden and Denmark to address problematic gambling. While gaming and gambling are separate subjects, gambling regulations are a good proxy to identify analogous practices for the gaming industry for two reasons:

- i. Problematic gaming and problematic gambling share similar structural and psychological underpinnings. Game design elements like high frequency events and variable ratio reinforcement schedules, which keep users engaged, are borrowed from design strategies used in gambling devices like slot machines.
- ii. Unlike gaming, regulatory efforts to address problematic gambling are much more systematised and time tested.

We reiterate that we do not intend to conflate gaming with gambling. The focus of the report is limited to skill games, which are distinct from gambling, which involves games of chance. Gambling regulations around the world have certain common elements like self-exclusion mechanisms, responsible advertising, and referral services for problem gamblers. From our assessment of regulatory approaches to problematic gambling, the following principles are observed:

- **Agile self-regulation** – Instead of prescriptive rulemaking, gambling regulators prefer principles-based self-regulation. In most jurisdictions the law defines the regulatory objectives and allows industry to meet those objectives through self-regulation. For example, in Sweden, the gambling law expects the gambling industry to act in a manner which does not jeopardize consumer health and well-being. However, instead of prescribing how exactly to achieve this, it allows the industry to present a roadmap describing the steps that they will take to fulfil the obligation. Such an approach eliminates the need for frequent amendments to laws and mitigates the pacing issues often associated with digital regulations.
- **Responsible game design** – Many jurisdictions prescribe standards of game design aimed at minimising the potential harms to consumers. The idea is to ensure that games do not use unethical tactics to exploit vulnerable gamers. For example, UK's Gambling Commission issues technical standards for remote gambling software. One of the standards, called RTS 14, mandates responsible product design aimed at minimising the likelihood that gambling software will exploit or encourage problem gambling behaviour.³² Similarly, under Swedish gambling law, developers are not permitted to specifically design or program a game to give players the impression of being close to winning when it is not the case. Another example of regulations guiding better game design is the UK Information Commissioner's Office's (ICO) Age-appropriate Design Code. Also called the Children's Code, it is a code of practice for the protection of children's data. Among its 16 data protection provisions are those related to the use of 'nudge techniques' and 'strategies to extend user engagement', and to default settings, which can be configured to encourage children towards behaviours that aren't in their best interests (including compulsive use). Importantly, the Code insists that online services protect children and their data by design and by default

RTS 14 Standards

- ✦ Users should not be given the option to cancel their withdrawal request.
- ✦ Once a customer has made a request to withdraw funds, they should not be given the option to deposit using these funds. Operators should make the process to withdraw funds as frictionless as possible.
- ✦ The gambling system must not celebrate a return which is less than or equal to the total stake gambled.
- ✦ Operators are not permitted to offer functionality designed to allow players to play multiple slots at the same time

- **Informed choice** – Prohibitory measures often fail the test of constitutionality, as they violate individual freedoms. For example, in 2011 the US Supreme Court in *Brown v. Entertainment Merchants Association* struck down a California law banning the sale of violent video games as it violated free speech laws. To mitigate harms without violating individual autonomy, many jurisdictions rely on the principle of informed choice instead. The idea is to supply consumers with all the relevant information to ensure that they make an informed decision. A prime example is the information obligation prescribed by Sweden’s gambling law. It requires all licensed gambling providers to make all relevant information about the game, including its rules and the likelihood of winning, easily accessible to players as well as authorities.
- **Use of technology as a regulatory tool** – In many jurisdictions, gambling operators are required to observe patterns in player behaviour to look for traits of problem gambling. This requires the use of cutting-edge technologies like artificial intelligence. In the UK, the gambling industry has voluntarily focussed on ensuring that the games they offer are low-risk by design. For example, Camelot Lotteries Ltd, one of the largest lottery services in the UK, ensures that all games offered by them go through ‘Gamgard’, an online tool that assesses a game’s structural risk levels, including jackpot sizes and the speed of play.³³
- **Responsible business conduct** – In most jurisdictions, instead of heavy handed regulations, governments require gaming businesses to adhere to ethical standards of business conduct. For example, chapter 14 of the Swedish Gambling Act prescribes a legal duty of care for licensed gambling providers. To do so the law relies on a principles-based approach. It requires licensed operators to ensure that social and health protection considerations are considered in gambling operations in order to protect players from excessive gambling and to help them reduce their gambling habits. In the UK, research, education, and treatment to help people struggling with gambling problems are funded by the gambling industry. All licensed gambling businesses are required to contribute.

These standards include responsible advertising, transparency and disclosure, and referral services. For example, under Denmark’s gambling law, platforms must spread awareness around responsible gambling and the ill effects of gambling. They are also mandated to advise at-risk and problematic gamblers to seek clinical help. Similarly, in Sweden, gambling licence holders are required to provide an online tool that lets players assess their gambling behaviour.

VI. Recommendations for India: The Case for Self-Regulation

Gaming disorder is a key policy concern in India, with the issue often being debated in Parliament. In December 2021, the Union Ministry of Education released an advisory for parents and teachers aimed at addressing the “downsides of online gaming”. It highlighted the risks of gaming addiction and prescribed a list of dos and don’ts for a safer experience. Many states including Telangana³⁴ and Tamil Nadu³⁵ have enacted blanket prohibitions on games involving monetary stakes, citing ‘addiction’ as one of the regulatory triggers. However, the skill gaming industry is protected under the right to freedom of trade and commerce under Article 19(1)(g) of the Constitution of India. This position has been upheld by the judiciary, including the Supreme Court, on several occasions.³⁶ Game content is also a form of protected speech under Article 19(1)(a) of the Constitution. Thus, the existing prohibitory approach is not only ineffective but constitutionally suspect.

Policymakers will have to ensure that regulatory interventions do not violate constitutionally guaranteed freedoms. Otherwise, they will be subject to tedious litigation and run the risk of being struck down. Policymakers will also have to consider the potential unintended consequences of regulation. The online gaming industry is a vital part of India’s digital economy, and by 2025 is expected to be worth USD 7 billion. It is also expected to generate more than one million job opportunities by 2030.³⁷ Heavy-handed regulation risks derailing the growth curve of this industry, leading to potential loss of employment opportunities, public revenue, and foreign investment.

From the discussion above it is evident that a harm-reduction approach is best suited to address the behavioural issues associated with gaming. It is also clear that across most jurisdictions, the industry is inextricably involved in the process of redressing these issues. In fact, most of the principles identified above are best implemented by industry. There are many reasons for this. To begin with, traditional regulatory approaches suffer from pacing issues. Gaming has always been an early adopter of frontier technologies, and each innovation throws up new challenges. In such a scenario, the traditional ‘regulate and forget’ approach becomes unviable, as technology outpaces the speed of regulatory fine-tuning. For example, the advent of the ‘Metaverse’ is expected to exacerbate issues of cybercrime in the virtual world. Criminal offences like assault and voyeurism will find new dimensions in an augmented or virtual reality. Yet the definitions of these offences in existing criminal laws are not fluid enough and will need amending.

Another issue is the lack of state capacity. Gaming is a huge market, with close to 4.5 lakh games available on the Google Play Store³⁸ and over a million games on the iOS App Store.³⁹ There are thousands of games available on other marketplaces like Steam and the PlayStation Store, and many games are available in grey markets which operate in complete legal vacuum. Regulating such a vast and fast-paced market will need technological sophistication and manpower of a sort seldom at the disposal of governments. In this backdrop, principles based self-regulation emerges as the most viable solution. It allows policy objectives to be achieved using minimal state capacity, while balancing economic and constitutional imperatives.

Historically, transparent and representative self-regulatory regimes have been instrumental in driving the growth of sunrise industries in a responsible and consumer-friendly manner. Courts have also weighed in favour of self-regulation administered by well-organised industry bodies to enhance consumer welfare. In its decision in *Ravindra Singh Chaudhary v. Union of India*, the Rajasthan High Court acknowledged the role played by the Federation of Indian Fantasy Sports (FIFS) in developing the fantasy sports industry and appreciated the best practices established by FIFS including an ombudsman and a charter.

There are many self-regulatory organisations (SROs) operating in the online gaming industry besides FIFS. These include the All-India Gaming Federation (AIGF), the industry body for online skill gaming in India, and the E-Gaming Federation of India (EGF) which regulates the Indian e-gaming industry. These SROs have their own charters, which lay down standards of business conduct and allow consumers access to a fair and transparent grievance redressal mechanism. In this backdrop it will be prudent for the Ministry of Electronics and Information Technology (MeitY) to legitimise existing SROs through rules made under the IT Act, 2000.

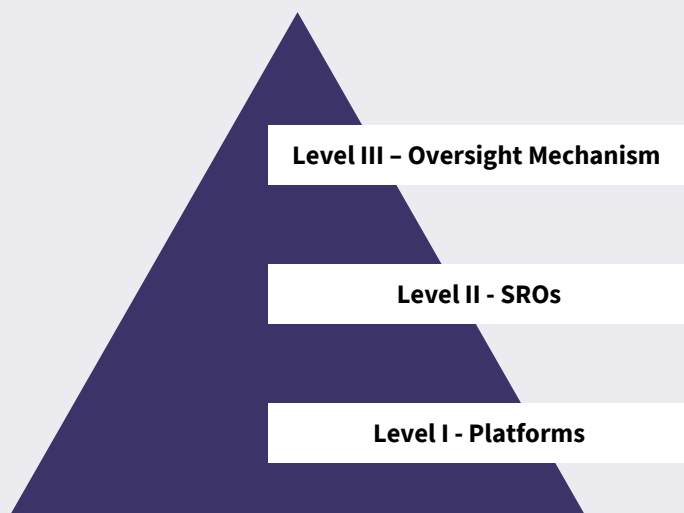
MeitY can lay down the minimum standards of conduct for every platform to abide by. Since online gaming platforms are intermediaries⁴⁰, the ministry may prescribe minimum standards such as additional due diligence requirements for gaming platforms. From the principles identified above, the following table suggests what these standards could be.

First Principles	Due diligence
Informed choice	<ul style="list-style-type: none"> • Age-rating – MeitY may prescribe a graded age rating system based on globally recognised frameworks like the ESRB and Pan-European Game Information (PEGI) game ratings. Every publisher should be mandated to prominently display the applicable ratings on their websites and applications. • Content descriptors – Content descriptors inform users that a certain game may contain themes of concern. Examples include violence, language, nudity, sexual references etc. Descriptors can also inform users if a game involves interactive elements like in-app purchases and real or simulated gambling. Besides age ratings, MeitY should also mandate the use of content descriptors. • Parental Controls - Dedicated gaming consoles have parental controls built in to allow parents or guardians to restrict access to games based on age suitability, to control spending, set time-limits or restrict communication in interactive games. Such measures should be uniform across all platforms. To ensure a uniform level of protection, the rules should mandate that all gaming platforms must mandatorily provide robust parental controls. Further, information regarding such controls must be easily accessible and easy to use.
Responsible game design	<ul style="list-style-type: none"> • MeitY may lay down first principles for ethical game design. These may be in the form of non-binding guidelines that help the industry design games in an ethical and non-exploitative manner. • The guidelines should discourage the use of unethical tools like ‘dark game design patterns’ to hook gamers. They may also direct the concerned personal data protection authority to issue detailed guidelines on the use of children’s data, which should be made mandatory for all gaming platforms. • The guidelines should also encourage game designers and publishers to ensure that best practices like privacy by design and security by design are at the centre of the design concept. • Based on these guidelines, the industry should come up with minimum standards of responsible game design.

<p>Responsible business conduct</p>	<ul style="list-style-type: none"> • Responsible Advertising – Businesses should be mandated to be more ethical in their marketing practices. Towards this, the Advertising Standards Council of India (ASCI) may lay down content standards for gaming advertisements. These standards may include the following: <ul style="list-style-type: none"> ◦ Advertisements should contain factually correct information and should not be false or misleading, particularly about the odds of winning ◦ Advertisements should not be designed to entice minors and should not be displayed in media that is clearly intended for minors ◦ Advertisements should not encourage users to chase their losses or re-invest their winnings ◦ Advertisements should not suggest that gaming is a means of solving financial difficulties. <p>It is important to point out that ASCI has issued similar guidelines for gaming advertisements in the past. On November 24, 2020, it issued guidelines for online real money games that went into effect on December 15, 2020.</p> <ul style="list-style-type: none"> • Transparency and Disclosure – Platforms should provide all relevant information to the users including terms and conditions and other policies that accurately and clearly specify the mechanics and rules of the contests, the terms and conditions of each contest, the points calculation mechanism and the manner of determining winners, and prizes and the distribution of the prizes. In the interest of proportionality, exceptions may be carved out for games which are in the development stage or have rolled out beta versions of their products for testing. • Referral Services – Businesses should identify gamers exhibiting patterns of problematic behaviour and should refer them to specialised centres for counselling and treatment. A dedicated helpline may also be established to allow gamers to seek help voluntarily.
<p>Use of technological tools</p>	<p>Businesses may be encouraged to use the available technological tools to monitor gaming behaviour and look for patterns of problematic gaming behaviour. Users exhibiting such patterns should be informed of the same as well as the physical and mental harms associated with gaming disorder.</p>

Enforcement Mechanism

The rules can be enforced by creating a three-tier consumer grievance redressal mechanism similar to that created for digital media under the IT Rules.



At the first tier, platforms can appoint a grievance officer based in India. The grievance officer will receive complaints against violations of the aforesaid standards and dispose of them within a fixed time.

SROs can be the second tier. They should supervise gaming platforms and guide them in complying with the standards of due diligence prescribed under the rules. SROs may act as an appellate forum to hear appeals emanating from the first tier. The bylaws of SROs should vest them with powers to take corrective measures against platforms which violate the provisions of the rule.

At the third tier, there can be an oversight committee constituted by the Central Government (similar to the Inter Departmental Committee under the IT Rules, 2021). The Committee can act as the final appellate forum and hear appeals arising out of the platforms and SROs. It should also be empowered to take suo moto cognizance of violations and enforce the rules through guidelines and advisories.

Chapter II: Addressing Financial Issues

Introduction

The online gaming ecosystem is fraught with financial challenges that are becoming more widespread and harder to detect. The trans-jurisdictional nature of online gaming makes it difficult to track game related transactions as they quickly change hands from country to country. When combined with technological innovations such as the use of crypto (for buying and selling in-game items) these anonymous digital transactions can be used to launder dirty money.⁴¹ Additionally, new game features have emerged that make it difficult to discern chance-based elements embedded in games of skill, causing uncertainty about the extent of liability that ought to be imposed on game developers and operators. Chance based elements, such as loot boxes, contain many items that players covet and tend to buy from secondary markets. Often these items are purchased from unverified sellers who use criminal proceeds to source them and sell them on to unsuspecting players. Many countries have evolved a principled approach in their regulatory responses to such financial fraud. For instance, Malta focuses on balancing innovation with financial safeguards. In 2019 the country adopted a sandbox approach to develop user safeguards while using virtual financial assets in gaming. In another instance the USA's approach to gaming regulation is guided by its public policy priorities of maximizing revenue, taxation, and licensing, enhancing economic development and tourism.

There are also user-facing concerns associated with online gaming. These involve financial propriety: ensuring that gaming companies adhere to ethical conduct such as eliminating conflicts of interest between them and the players and preventing misuse of the money that users deposit with them. Game company federations have developed responsible gaming codes of conduct for a greater duty of care towards users.

The following sections contain an overview of the principles and solutions developed by countries and international organisations to address the financial challenges associated with 1) the financial integrity of gaming operators, 2) the use of virtual currencies, and 3) micro-transactions.

I. Financial Integrity

Monetisation strategies for gaming companies hinge on user engagement and their willingness to spend. Users typically spend money on in-app purchases or on deposits made with the expectation of winning rewards. As online games become more popular, the amount of money users spend on average is increasing too. According to an EY-FICCI report, in 2020 the revenue for transaction-based games like fantasy sports and pay-to-play rummy grew by 21%.⁴² In the same period, the revenue earned from in-app purchases for casual games grew by 15%.⁴³ The high volume of money involved invariably puts a very high responsibility on gaming companies to ensure that user money is handled in accordance with the highest standards of financial propriety. Yet there are many instances where users have been victims of financial impropriety. For example, users have experienced situations where the in-game rewards disappeared, or they did not receive their prize money on time. In 2020 the FIFS Ombudsman received several complaints against 'Playing 11' which stated the platform had not credited the winning amount due to the players in their accounts despite repeated written reminders.⁴⁴

For the gaming industry to grow sustainably it is imperative to build user trust. And as seen with banking and the stock markets, trust can only be established through strong grievance redressal systems, fiduciary practices and regulation – either self or external. The following sections discuss these practices and outline how such systems can be built to enhance user trust.

Current Practices

a. Financial propriety in user accounts through self-regulation charters

Gaming federations like the All India Gaming Federation (AIGF)⁴⁵ and the Federation of Indian Fantasy Sports (FIFS)⁴⁶ have laid down self-regulation codes for all games of skill offered in pay to play formats. AIGF regulates fantasy sports, online rummy, casual games, and online poker games within India. FIFS solely governs online fantasy sports. These federations provide responsible gaming standards to ensure that user funds are not misused and in the event of any dispute the grievance is resolved quickly through an established dispute resolution mechanism. On financial integrity the charters are similar and stipulate basic conditions for securing user funds. For instance, they require user funds to be maintained in a non-interest earning escrow account and to be segregated from operational expenses. Companies are also required to perform user verification for accurate payment processing and to prevent the diversion of funds. Other measures prescribed by the charters include:

- Accept only digital payments and ensure that the digital wallets and accounts of the user are KYC compliant
- Implement controls and preventive measures to detect and prevent the use of platforms for money laundering or terror financing
- Conduct an annual assessment of the risks of the platform being used for money laundering or terror financing.

A notable difference is while both the AIGF and FIFS have established redressal systems, the AIGF charter clearly mentions consumer dispute redressal, unlike the FIFS charter. Clearly a uniform charter of fiduciary responsibilities for pay-to-play games of skill providers will offer users a more predictable gaming landscape.

A better organised approach to self-regulation can be seen in the standards developed by the European Gaming and Betting Association (EGBA).⁴⁷ Although the standards are aimed at gambling operators, they provide insights into responsible consumer protection measures. The EGBA standards are based on 9 principles incorporating 134 practical measures for remote responsible gambling established by the European Committee for Standardization (CEN), a private regulator.⁴⁸ Similar principles are insufficiently spelt out in the AIGF and FIFS charters. For example, the principle of prompt and accurate customer payments in the EGBA charter lays down a strict time limit of 7 days within which all payments to customers must be completed. It also requires separately identifying members' liability for customer balance and guaranteed prizes and demonstrating that member organisations have sufficient cash to pay what they owe. The EGBA standard specifically lists⁴⁹ ISO/IEC 17025 certified independent accredited testing agencies and player protection and standards organisations for a mandatory annual audit of compliance with the charter. A similar approach could be followed by gaming federations in India.

b. Lessons from International Best Practices

Prescriptive regulations for non-gambling companies are rare and are mostly directed at domestic and offshore gambling and betting websites. They aim to enhance financial integrity and some of their provisions could be borrowed for non-gambling operators as well. The principles underlying them are discussed below

- **Financial responsibility and stability:** Fiduciary responsibility may be built into the regulation as a mandatory condition. This could resemble the conditions imposed on gambling operators to obtain a licence. The UK's licensing Condition and Codes of Practice⁵⁰ requires gambling operators to segregate customer funds in a separate bank account and implement the prescribed internal control and accounting systems to enhance financial accountability towards customers. Typically, the financial stability of the operator safeguards consumer deposits. One of the conditions for granting a licence in the United States is the applicant's ability to maintain adequate insurance levels and the history of the applicant.⁵¹
- **Transparency:** Providing more transparency to customers and giving them the ability to control their accounts is found to promote financial discipline and reduce the chances of misuse. For example, the EU's Responsible Remote Gambling Measures require operators to give customers remote access to their account balance and history for the past 60 days and offline access for a minimum of 6 months. Sharing a meaningful activity statement for consumers to track and monitor online wagering spending and behaviour enhances consumer awareness and control over their deposit and transactions.
- **Conflict of interest:** Operators' offering lines of credit to consumers for money to wager can induce players to wager more than they can afford. A 2015 baseline study by Financial Counselling Australia⁵² established that betting companies were luring gamblers to place bets on their websites by offering credit to users. In response, the Interactive Gambling Amendment Act, 2017 and Australia's National Consumer Protection Framework (National Framework)⁵³ for Online Wagering prohibit online wagering service providers from offering or providing credit to users who gamble.⁵⁴ Online wagering service operators are also prohibited from advertising payday loans, and customer information cannot be given to payday lenders. Such provisions aim to discourage conflicts of interest between users and operators. Similarly, the UK's licensing Condition and Codes of Practice⁵⁵ prohibit licensees from providing credit or participating in arranging credit in connection with gambling.

II. Virtual Currencies

Online gaming companies such as Nexon America,^{56 57} and Wargaming⁵⁸ accept virtual currencies like Bitcoin, Ethereum and Dogecoin for in-game purchases. Traditional games have likewise yielded to formats where players can own virtual in-game items. Ownership gives users the ability to go beyond pure gaming and monetise the in-game items by exchanging them for virtual currency. The presence of a large community of gamers spread across countries creates opportunities to trade such items across jurisdictions. Virtual currencies are the preferred means of buying or selling in-game items because they enable fast transactions and eliminate the hassle of currency conversions.

Definition of Virtual Currency



For the purpose of this report, we rely on the FATF's definition of virtual currencies.⁵⁹ A virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; (2) a unit of account; and/or (3) a store of value but does not have legal tender status in any jurisdiction.

Virtual currencies are of two sorts – open or closed. Open or convertible virtual currencies (CVCs) like Bitcoin (cryptocurrency) or Linden Dollars (from the Second Life game) are widely used to perform microtransactions in online games.⁶⁰ Their convertibility means that they can be exchanged for fiat currency because a market exists for them. CVCs are not backed by law and their convertibility solely depends on the value they hold for the community

of users who agree to buy or sell them. They can also be exchanged for other virtual currencies on a virtual currency exchange. For law enforcement purposes, convertible currencies are subject to Anti-Money Laundering (AML)/ Combating the Financing of Terrorism (CFT) laws as they can be used to move money from one source to another.

Linden Dollars



Linden Dollars are a virtual currency used on the online multimedia platform/game Second Life. They are pegged to and convertible to the US Dollar. In 2013 the Financial Crimes Enforcement Network (FinCEN), the US Department of Treasury's AML and financial crimes monitoring and prevention unit, classified them as a convertible centralized virtual currency for the purpose of taxation and AML regulations.⁶¹ It classed the company that had created the game, Linden Labs, as a "money service business" / money transmitter.^{62 63} Users are now required to provide their personal information and verification details while transmitting Linden Dollars.

On the other hand, non-convertible currencies, such as QCoins or World of Warcraft Gold, cannot be exchanged for fiat currency. They are called closed currencies, being restricted to use in a specific virtual world. In practice, however, even closed virtual currencies are often exchanged for fiat or open virtual currencies in secondary markets.⁶⁴ In such cases, they can be considered open currencies and therefore attract AML/CFT regulations. Massively Multiplayer Online Role-Playing Games (MMORPGs) such as World of Warcraft involve millions of players spread across several jurisdictions, making it easier to covertly move money around the world. Both convertible and non-convertible virtual currencies can be used in online games to commit financial frauds.^{65 66} The frauds associated with non-convertible currencies are explained in the section on micro transactions.

Money Laundering through virtual currencies and in-game items?

Money Laundering involves three steps:

1. **Placement:** *Putting the dirty money into the financial system* | Criminals use illicit funds to obtain virtual currency through a specific exchanger and purchase in-game items - or - criminals create user accounts using stolen credit cards or hack into accounts and purchase in game items
2. **Layering:** *Creating complex layers to hide ownership and source* | In game items are then sold to players across the world for convertible virtual currencies, by routing transactions through mule or multiple accounts or mixing and tumbling on crypto exchanges
3. **Integration:** *Putting the proceeds of laundering back into the economy* | The money is then exchanged for fiat and withdrawn as legitimate money - or - the proceeds are reinvested into the virtual currency market.

Although bank accounts are subjected to strict regulations, criminals transfer funds through P2P transactions using several intermediaries or mules across jurisdictions to evade supervision.⁶⁷ The anonymity offered by peer to peer (P2P) transactions makes them attractive for criminals to launder money. Such transactions take place between unique wallet addresses that are difficult to trace. When combined with mule accounts and the involvement of multiple financial institutions, it becomes difficult to work out money laundering responsibilities. Tumble/mixing services also facilitate transaction anonymity, where tainted cryptocurrency is swapped with other cryptocurrency owners' streams to obscure the trail back to the original source.⁶⁸ Criminals also use unregulated cryptocurrency exchanges to swap illicit funds with other virtual currencies and send them to anonymous accounts.

Current Practices

To address AML/CFT fraud, various countries and international organisations have crafted regulation to address certain specific uses of CVCs. Some key actions are discussed below.

a. Activity based regulation

The US Financial Crimes Enforcement Network (FinCEN) subjects certain uses of CVCs to AML regulations. FinCEN requires the application of AML/BSA rules to people who accept or transmit any value substituting for currency (such as CVCs⁶⁹) from one person to another or to another location.⁷⁰ Such persons are known as money transmitters. All of them must abide by AML norms such as collecting and identifying information from users, regularly monitoring and reporting suspicious transactions and registering with FinCEN. For gaming companies this means that if the company issues virtual currency (puts it in circulation) and has the authority to redeem it (withdrawing it from circulation) it will be considered an exchanger or administrator and the virtual currency transaction will be treated as money transmission.⁷¹ For instance, a gaming platform may put CVCs into circulation by providing them to users as a reward, in exchange for fiat or even as a promotion, and exchange it for in-game / in-app items or features, real currencies etc.⁷² Applying this principle to Linden Dollars, in 2013 the FinCEN classified Linden Labs as a money transmitter.

b. Risk-based approach

Gaming companies can mitigate AML/CFT threats by monitoring high risk users and tailoring rules according to their risk profiles. For example, as per the recommendations of the Financial Action Task Force (FATF), low value limits could be imposed for customers with low due diligence requirements and high value limits for those with high due diligence requirements.⁷³ Value limits may mean account balance, transaction value or transaction frequency restrictions. They will also require continuous and close monitoring of high-volume suspicious transactions. Users from high-risk countries could be subjected to enhanced assessment criteria. Companies may include additional safeguards for transactions to and from high-risk countries.

c. Regulatory sandbox

Regulatory sandboxes offer the chance to test innovations in a controlled environment. The aim is to encourage innovative business models in a way that protects the consumer interest. A sandbox provides a platform to experiment and the opportunity to identify gaps in regulation and to build legal certainty before the model is mainstreamed. A noteworthy case is Malta, which has seen potential in promoting innovations in the gaming industry, especially in the use of Digital Ledger Technology (DLT) and Virtual Financial Assets (VFAs). Malta launched the sandbox approach in 2018 to address AML/CFT obligations. The sandbox ecosystem requires operators to implement conditions including wallet ownership verification systems, player identification and verification procedures and limits on wallet values. To track the money, operators must verify the ownership of every player's wallet by ensuring that it belongs to the registered player within a short span of time, set at 30 days. The sandbox also aims to address the challenges associated with diversion of funds by stipulating that any withdrawals from a wallet other than the one used for deposits will require customer due diligence (CDD), explanations and proof of control over the wallet.

d. Value based regulation

In 2018, the Malta Gaming Authority (MGA) launched a regulatory sandbox to create a controlled environment in which licensed operators can use Virtual Financial Assets (VFAs) as a valid consideration. As mentioned above, only licensed VFAs are allowed into the environment, and they are covered by AML provisions. To determine the licensability of the VFA, gaming operators must conduct a Financial Instrument Test⁷⁴ to assess whether the DLT technology falls under the VFA Act or any existing EU legislation.⁷⁵ Only VFAs that pass the financial instrument test can be licensed under the sandbox and are supervised under anti-money laundering laws. The tests evaluate criteria such as the financial value, technological value, scalability, market conditions among others.

e. Customer due diligence

Customer due diligence (CDD) is an integral part of monitoring and tracking funds. Game companies are expected to lay down due diligence practices to verify customers' identity and only allow transactions through verified accounts. CDD requirements aren't always required for all accounts and may only kick in after a monetary threshold is crossed.⁷⁶ This allows operators to monitor specified transactions by keeping logs of wallet addresses, transaction amounts and time stamps. The MGA rules also require withdrawals to be made from the same wallet as used for the deposit and unverified funds to be sent back to the originating wallets. Such conditions help ensure that all withdrawals conform to the relevant AML/CFT obligations.⁷⁷

III. Microtransactions

Microtransactions have revolutionised revenue streams in the video game industry. They are low-value transactions users can make to buy virtual in-game items. The business models of several online games, especially those that are free to play, rely on such microtransactions. Currently, in-app/ in-game purchases are a significant income source for non-RMG games.⁷⁸ In 2021, global consumer spending on mobile gaming apps reached \$133 billion,⁷⁹ and in India by 2025 the gaming market is expected to value \$7 billion with in-app purchases being the fastest growing segment.⁸⁰ Players have the incentive to buy in-game items as they offer significant gameplay advantages – the items could include virtual weapons, vehicles, mission or quest packs, extra playtime or aesthetic items like interface skins. Some games also offer in-game currencies⁸¹ to buy such items, while others require players to purchase lootboxes⁸² the contents of which become known to the user only after they have purchased the boxes.

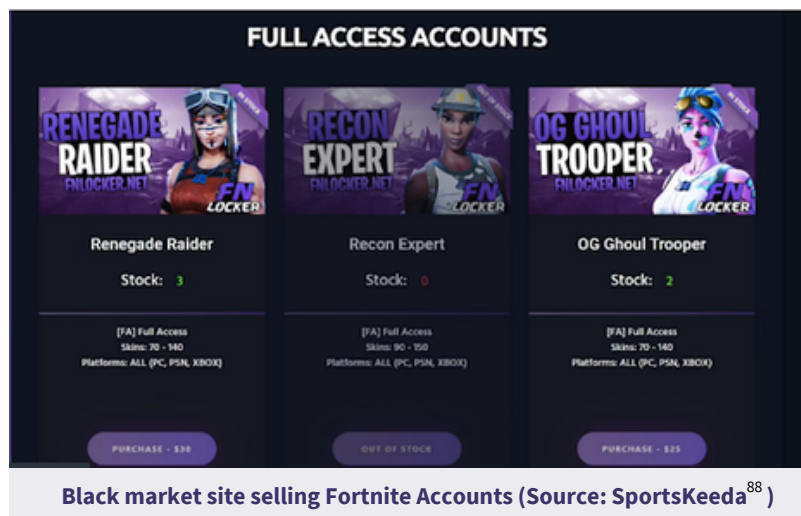
Conversion of microtransactions into illicit income

Third party trading of in-game items or currencies: In-game artefacts and currencies can be used to store value and offer ways to convert illicit income or move criminal proceeds. This is done by trading in-game currencies or virtual items unofficially through online marketplaces extraneous to the game. The practice of laundering money through microtransactions is not new and was highlighted in a 2013 United Nations Office on Drugs and Crime (UNODC) report. It revealed that criminals have exploited massively multiplayer online role-playing games (MMORPGs) to launder money by transferring illicit funds to other accounts and using them to buy or exchange in-game currency for real currency.⁸³ For example, criminals stole bank card details to buy V-Bucks from the Fortnite store and sold them at a discounted rate to other players on the dark web and social media platforms.⁸⁴

Money Laundering through V-bucks on Fortnite

In 2019, an investigation by *The Independent* newspaper and the cybersecurity firm Sixgill found that criminals had used V-bucks, Fortnite's in-game currency, and other in-game items to launder money in five countries.⁸⁵ These were purchased using stolen credit cards and sold on the dark web in exchange for bitcoins or bitcoin cash. With over 200 million players worldwide, there is high demand for in-game currencies with some game items costing more than \$250,000 on eBay.⁸⁶

Fortnite has taken several steps to discourage the purchase of V-bucks from third parties. Its policy prevents third parties from purchasing V-bucks or in-game items. If such purchases are detected, the game can revoke them, remove the virtual items or impose a permanent account ban if the player continues to buy V-bucks despite repeated warnings. Critics however say these steps are not enough and that the game should monitor suspicious accounts and report them to the authorities.



Using chance-based elements to clean money: Regulators are also facing challenges as the lines blur between gaming and gambling. This is made possible by the introduction of chance-based elements such as lootboxes into online games of skill, which may expose users to gambling related harms.⁸⁹ According to estimates, by 2025 the revenue from loot boxes is projected to cross \$20 billion.⁹⁰

Elements of gambling in lootboxes

The lootbox works as a kind of microtransaction, i.e., an in-game purchase is made to unlock certain content – cosmetic items like costumes or skins for a player's avatar, special items, skills or abilities, or any other content that is not available to everyone. Essentially, a lootbox is a mystery box that players can purchase without knowing its contents, which can vary in terms of rarity or in-game value. For instance, some first-person shooter games offer players the option of purchasing a weapons crate which contains a randomized weapon. While a lootbox can be acquired by players through their in-game performance, regulatory concerns usually emerge when these are offered for purchase for real money.

Lootboxes have come under scrutiny from some policymakers for containing elements of gambling, especially in a context easily accessed by children. Most legal definitions of gambling or wagering include three elements - i) the wagering of money ii) on the unknowable outcome of a chance event iii) for a valuable prize. Lootboxes, which are purchased for real money (or in-game currency, which can itself be purchased for real money) and which contain an element of chance along with the promise of potentially valuable prizes thus fall under this definition.

Laundering money through lootboxes

The Netherlands Gaming Authority found that 4 of 10 lootboxes contained items that could have been traded outside of a game because the prizes had market value.⁹¹ Investigations have shown that criminals use illegally obtained money to purchase lootboxes and collect rare items valued by players.⁹² These are sold on to players on third-party platforms for money or convertible virtual currencies.

The fact that virtual assets have financial value outside of the gaming ecosystem provides an opportunity for criminals to transfer illegally obtained funds. In 2019, Counter Strike discontinued the trade of container keys on the Steam Community Market after it was observed that nearly all key purchases were traded to convert illicit money. Steam Community Market is an online marketplace used to buy and sell in-game items with the approval and support of the game to which they belong.

Current Practices

There are no certain solutions for regulating in-game items. Third-party misuse of microtransactions is still being investigated and companies typically self-regulate to discourage players from buying in-game items from unauthorised platforms. The discourse around applying AML obligations under gambling laws to lootboxes is still nascent. These aspects are discussed below.

a. Regulating closed virtual currencies as CVCs

In 2014, the Financial Action Task Force (FATF) published a report on virtual currencies.⁹³ It classifies in-game virtual currencies (such as V-bucks) as non-convertible or closed virtual currencies as they are meant for use within the gaming platform and cannot be exchanged for fiat or another virtual currency outside. Yet the report notes that these currencies may have value outside the game and could be exchanged in the black market for fiat or another virtual currency, and several investigations have established such third-party transactions.⁹⁴ Closed virtual currencies may attract AML/CFT and other financial regulations in such cases. In other words, enhanced liability may apply to gaming companies that offer such items and they may be required to carry out KYC and CDD processes, monitor suspicious transactions etc.

b. Regulating chance-based elements in online games (lootboxes)

Many countries are considering whether to class lootboxes as gambling activity or as part of games of skill.⁹⁵ Parliamentary committees in the UK⁹⁶ and Australia⁹⁷ have recommended that microtransactions for chance-based items such as lootboxes should be covered by gambling laws. If microtransactions qualify as gambling, gaming companies that offer such features are required to fulfil AML responsibilities and undergo enhanced scrutiny.

c. Value-based approach

The Netherlands and Belgium have taken a value-based approach to regulate certain microtransactions as gambling. The Danish Gambling Authority considers certain lootboxes as gambling under the Dutch Betting and Gaming Act. Under this law, if chance-based items have an economic value, i.e., they can be converted into money, they will be regulated as gambling activity. The Act does not apply to items that cannot be sold or otherwise converted to money. According to the Authority, a game will fall under the Dutch Betting and Gaming Act if it satisfies the following criteria: there must be a deposit; there must be an element of coincidence; and there must be a prize. Where the prize is a virtual item, it must be able to be translated into monetary value.⁹⁸ According to the Authority, the Gambling Act would apply, for example, when items are sold on third-party websites as they have been converted into money.⁹⁹ On the other hand, in Belgium, lootbox items needn't possess monetary value; it is sufficient if the items are of value to the player. In other words, they can be money's worth due to their subjective value to the players.¹⁰⁰ Belgium regulates lootboxes as games of chance under the Act of 7 May 1999. According to the Belgium Gambling Commission, all lootboxes are considered gambling regardless of whether the items can be exchanged for real money. Lootboxes bought for real money constitute a game of chance and are therefore illegal.¹⁰¹ The Belgian Gaming Commission also investigated four games – FIFA 18, Overwatch, Counter Strike: Global Offensive and Star Wars Battlefront 2 – and found that the lootbox mechanic in all of them except Battlefront 2 (which was removed from stores after some controversy at the game launch) constituted illegal gambling under the Belgian Gaming Act, as it was similar to betting on a game of chance. This contrasts with the UK and the USA, where lootboxes do not fall under gambling regulations as yet.

d. Legal clarity

Regulators have taken varying approaches to regulating in game, chance based microtransactions. In September 2019, the Digital, Culture, Media and Sports (DCMS) Committee in the UK released a report on immersive and addictive technologies, where it called for the Gambling Act, 2005 to be extended to cover lootboxes. A July 2020 report by the House of Lords Select Committee on the Social and Economic Impact of Gambling arrived at the same conclusion, calling for explicit regulations declaring lootboxes to be games of chance and saying it was required ‘immediately’. Both committees recommended that lootboxes should be regulated as a game of chance for prize under Section 6(1) of the Gambling Act, 2005.¹⁰² The Gambling Commission, however, has so far maintained that lootboxes do not fall under the legal definition of gambling.¹⁰³ As long as in-game items obtained through lootboxes are ‘confined for use within the game and cannot be cashed out’ it is unlikely to be considered a licensable gambling activity, according to the Commission.^{104 105} In June 2020, as part of its response to the DCMS Committee report, the British government announced it would launch a call for evidence into the impact of lootboxes on gambling-like behaviour.¹⁰⁶ The call for evidence forms part of the government’s wider Review of the Gambling Act.

In Singapore the Ministry of Home Affairs put the Remote Gambling Act under review in 2021, with the aim of making the law technology-agnostic, which could mean new regulations for lootboxes and other kinds of non-traditional gambling products.¹⁰⁷ Japan on the other hand has chosen to permit lootboxes while prohibiting a subcategory considered the most egregious and has focused on protecting consumers from deceitful practices instead of fitting lootboxes into gambling laws.

In the Netherlands, the Danish Gambling Authority has adopted a case-by-case approach to determine if a lootbox qualifies as gambling. In one such case the games publisher Electronic Arts challenged the Authority’s decision to hold FIFA lootboxes as gambling in the Hague District Court, and in 2020 the court ruled¹⁰⁸ that lootboxes, albeit played within games of skill, would be regarded as a separate game.¹⁰⁹ It also held that even if some of the items inside the FIFA lootboxes were already known to the user, it did not take away the element of chance from lootboxes. In March 2022, however, the highest administrative court overruled the district court’s decision and held that FIFA packs (lootboxes) were an integral part of the game which is predominantly a game of skill. The press release on the case further explained that “the tradability of the packs on the black market is relative. The black market mainly focuses on trading complete accounts rather than individual packs or their contents. Since the packs are not a standalone game, they are not a game of chance and do not require a licence.”¹¹⁰

e. Self-regulation

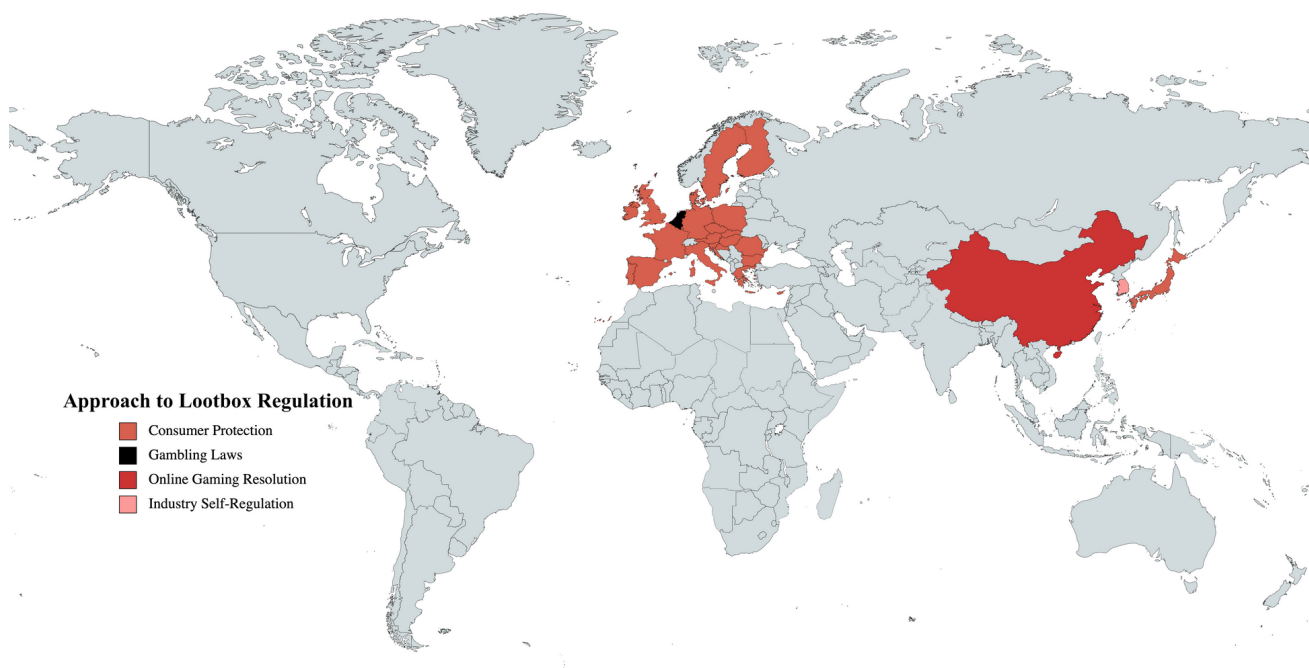
In 2019, leading game console manufacturers like Sony, Microsoft and Nintendo made changes to their policy stating that publishers’ games would be released on the console only if they disclosed the probability of receiving “rare” items.¹¹¹

Lootboxes offer a unique case of behavioural and financial implications for consumers

Lootbox regulation provides an interesting example of an issue that blends behavioural and financial concerns. The element of chance associated with lootboxes along with the promise of potentially valuable prizes raises concerns about children being drawn into gambling, especially as lootboxes are presented using visual design elements (such as visual effects, sounds and colours) that heighten the excitement of opening them.

The UK’s Advertising Standards Authority (ASA) issued guidance on mobile games in September 2021 on how such games advertise their in-game premium currency.¹¹² Among these factors, the ASA’s guidance states that games which include lootboxes must disclose this information on store pages and any advertising. While the ASA cannot penalise companies for failing to follow its standards, being named by the Authority for violating guidelines can be seen as a deterrent.

The Internal Market and Consumer Protection committee of the European Parliament published a comprehensive study in July 2020 examining lootboxes from a consumer protection perspective, especially the protection of children.¹¹³ While going into the design elements of lootboxes that promote addictive behaviour, the study recommends the consumer protection approach to tackle problematic game design as opposed to gambling legislation. While gambling is a matter of national competence, risking a fragmented market for video games in the EU, a wider consumer protection perspective, which focuses on psychological and financial harm to the consumer, would enable action on a transnational level. The study examined lootbox features such as near-miss experiences (which signal to a player that they almost won big), visual and audio effects, and casino-like features along with social components that together create strong psychological reward structures which could promote addiction. The study recommends that protective measures be introduced ‘at multiple points throughout the consumer journey’, through consumer information and transparency measures (such as displaying the odds of winning certain items in a loot box) and age and parental controls. While encouraging self-regulatory initiatives by industry, such as Apple and Google’s requiring games listed on their stores to display the probabilities of winning various items when they offer lootboxes, the report goes on to state that if voluntary practices are found inadequate to protect players, lootboxes may be regulated at the EU level through consumer protection regulations.



Approaches taken by jurisdictions to deal with issues relating to lootboxes

IV. Recommendations for India

a. Financial integrity of gaming platforms

As a consequence of new monetisation models, users are spending unprecedented sums of money on gaming platforms. Given the high volumes of money and the large number of users involved, fiduciary responsibilities towards consumers are a need of the hour. Traditionally, the gambling industry has been strictly regulated and presents a good example to ensure that safeguards are put in place to protect consumer money. Therefore, some provisions from gambling laws could be borrowed to create a responsible gaming mechanism for users. For example, to maintain effective control over financial practices, gambling laws prescribe accounting procedures, and require operators to keep transaction records and file periodic reports with the regulators. Similar provisions could be applied to games of skill to protect the user interest. In India, MeitY may incorporate some of the practices discussed as part of its guidance for gaming intermediaries. Alternatively, SROs may stipulate these in the self-regulation charters of pay-to-play games of skill.

Principles	Implementation
Conflict of interest	SROs can include these in their charters to ensure that members abide by the conditions. MeitY may issue regulations or guidelines incorporating these as due diligence while SROs monitor their implementation.
Financial responsibility and stability	
Control to customers	

b. Recommendations for the use of CVCs

India's gaming industry has been reluctant to accept CVCs as payment because the Government's stand on cryptocurrency regulation remains unclear. Whether or not it is permitted in payment transactions, while crypto continues to be traded on the internet it will be possible to circumvent restrictions using offshore routes. With the introduction of new games that give gamers total ownership of their items, the tradability of such items is likely to witness explosive growth.¹¹⁴ For example, NFTs represent the right to ownership in a particular asset. NFT based play-to-earn games like Axie Infinity, which is extremely popular in India,¹¹⁵ allow players to trade NFT items against crypto.¹¹⁶ Analyses by Chainalysis reveal that money laundering through NFT based cryptocurrency is worth \$1 million and convey the need for KYC and AML safeguards.¹¹⁷

India does not so far have a regulation to monitor CVCs in online gaming for AML/CFTs. Although the Supreme Court in *Internet and Mobile Assn. of India v. RBI*¹¹⁸ acknowledged that the RBI could regulate CVCs provided they are defined as currency as per the Foreign Exchange Management Act, 1999, the appropriate way to regulate the use of CVCs in online gaming would be to amend the Prevention of Money Laundering Act, 1999. The measures taken by the countries discussed in the section above would be helpful in developing suitable regulations.

Principles	Implementation
Activity based regulation	Amend PMLA to regulate entities that perform functions to put CVCs in circulation or redeem them. While the Ministry of Finance has the overall responsibility for enforcement and monitoring of AML/CFT regulations,

	MeitY is the concerned Union ministry for gaming regulation. ¹¹⁹ Therefore, mitigating AML/CFT will require close collaboration between MeitY and the Ministry of Finance where MeitY can require gaming companies using CVCs to register with it. Additionally, SROs can advise members on game features that may subject members to AML regulations.
Value based approach	MeitY can lay down licensing conditions for VFA based gaming operators. This will require close coordination with the Ministry of Finance, which can introduce regulations defining VFAs and clarifying the scope of AML provisions.
Risk based approach	SROs can recommend a risk-based approach to CDD and impose value limits. CDD norms in PMLA may also need to be amended depending on the risk profile of the customer.
Regulatory sandbox	Instead of banning a new business model outright or regulating it through legacy laws, use a sandbox-based approach to test innovations. MeitY can keep these principles in mind while updating the IT Act or issuing new guidelines.
Customer due diligence	MeitY can issue guidelines on CDD for wallet address where it involves CVCs. SROs can include these in their charter.

c. Recommendations for micro-transactions

India's gaming ecosystem is developing rapidly, supported by brisk growth in the purchase of in-game items. In 2020, in-app purchases of games on the Google Play Store and Apple App Store grew by 51% and 30% approximately, according to a report by Sensor Tower. Keeping in mind the foregoing discussion and developments in other countries, India can take the following steps to address the AML challenges associated with microtransactions.

Principles	Implementation
Value based approach	The Centre (MeitY) in collaboration with Self-Regulatory Organisations (SROs) and the States can determine whether chance-based items in games of skill should be treated as a separate game or an extension of the game of skill. For this it is necessary to ascertain at what point a particular item should be considered to have economic value such that it is covered as prize under the gambling laws.
Legal clarity	
Self-regulation	SROs can choose to issue suitable guidance on chance-based items embedded in a game of skill. These may include transparency by members to disclose in-game chance-based items, the probability of winning rare items, and the value of some of these items before users purchase the game.

Chapter III: The Metaverse and Future Issues in Gaming

METaverse

Introduction

The term ‘metaverse’ refers to a simulated digital environment, created through the use of technologies such as virtual reality (VR) and augmented reality (AR). It mimics a shared physical environment that users can inhabit through avatars, and focuses on social connection, allowing people to communicate, create and play games together. The metaverse has been positioned as successor to today’s internet, which is referred to as web 2.0, and is itself considered a big component of web 3.0 along with decentralization through technologies such as blockchain. The key traits of the metaverse are its immersiveness (users perceive the sensation of actually being in the simulated environment), persistence (the simulated world continues to exist even when not being actively used by a particular user) and interoperability (given the need to create digital assets that can be used across different ‘realms’ of the metaverse).¹²⁰ Metaverses are inherently linked to gaming, as many of their core concepts and technologies (such as shared virtual worlds in games like World of Warcraft or Second Life) were first developed in the context of games.

The metaverse is an exciting opportunity for the Indian technology community, and a number of Indian companies have started work with the aim of contributing to this space in its early stages. For instance, Bolly Heroes¹²¹ aims to create a parallel world of Bollywood in the metaverse, complete with NFT collections, in collaboration with production houses, music studios, celebrities, gaming and animation companies. Loka, a New Delhi based initiative offers 3D recreations of iconic Indian locations such as Connaught Place in Delhi and Marine Drive in Mumbai that can be accessed through a mobile app.¹²² Meanwhile, large companies like Tata Consultancy Services (TCS) have signalled that they are making large investments in the metaverse.¹²³ Other software exporters such as Infosys and HCL are also following suit.¹²⁴

In the metaverse, India has the opportunity not only to participate but actually build the next generation of the internet, giving a massive boost to domestic IT industries, and to content creation in the media and entertainment industry as it creates next generation experiences in India for the world. Thus it is important to take an early view on some of the pressing issues being raised about the metaverse. The recently constituted Animation, Visual Effects, Gaming and Comics (AVGC) Task Force has been created with a view to capturing 5% of the global market share in these industries by 2025, creating 1,60,000 new jobs every year.¹²⁵ As part of its National AVGC Policy, the Task Force can set out a vision for India’s metaverse industries, and create an enabling ecosystem to make India an early leader in this nascent space. The following sections discuss some of the early issues that regulators and policymakers will have to consider.

Issues in the Metaverse

Digital metaverses present two sets of issues. The first consists of problems that apply to existing (web 2.0) online platforms but are extended or amplified by the nature of the metaverse. The immersiveness of the metaverse increases the impact of any problem, its persistent nature increases the velocity with which the problem spreads, and its interoperability makes content moderation more difficult across platforms. Besides amplifying existing concerns, the metaverse also poses unique challenges, many of which will emerge as the technology is more widely deployed.

To study the metaverse from the perspective of games, we can categorize the issues into two baskets. First, those relating to user protection from harms, including bullying and harassment, deceptive advertising and excessive tracking and profiling. Second, those relating to property rights (including but not limited to intellectual property rights) over virtual assets in the metaverse.

I. User Protection

As mentioned above, the metaverse amplifies some of the issues users already face in the realm of online gaming. These are essential to address right from the nascent stage that the metaverse is in today, to ensure that the growth of this technology is beneficial to users and society. This section examines some user safety concerns that come with games in the metaverse.

a. Online harassment

Most online gamers have, at one point or another, encountered toxic behaviours in online gaming communities. These may range from cyberbullying and verbal abuse to more serious cases of the grooming of underage players or sexual harassment. These behaviours can lead to significant psychological harms, especially for children and vulnerable groups. The scope of this harm is further heightened in the metaverse, where players are more immersed and can therefore experience harassment in more visceral ways, approximating real world harassment. According to Katherine Cross, who researches online harassment at the University of Washington, since virtual reality is designed to trick the user into thinking that they are physically in a certain space, emotional reactions in this space can be much stronger, as they trigger the same nervous system and psychological response as encountering danger in real life.¹²⁶

Unfortunately, there have already been instances of sexual harassment in the metaverse even before the technology has achieved commercial scale. As far back as 2016, a user wrote an open letter after being groped on Quivr, a VR archery game.¹²⁷ More recently, a beta tester reported being groped by a stranger on Horizon Worlds, Meta's virtual reality social media platform.¹²⁸ Still more instances of sexual harassment in the metaverse have been reported in recent years.¹²⁹

Early Solutions

Given the nascency of the metaverse, discussions around regulation are in their earliest stages. While most jurisdictions have not initiated such discussions, some like South Korea have taken first steps. Self-regulatory initiatives have also been seeded, by individual companies as well as by larger groups or associations. At present there are two primary solutions to deal with the threat of harassment in the metaverse. The first involves putting the onus on the platform to provide redressal for such incidents after they occur. This includes proactive moderation, penalizing offending users by suspending or banning their accounts, and ensuring they cannot create additional accounts in future. The creation of an offenders' registry has also been suggested, to ensure that users banned for abuse in one virtual world cannot simply hop into another and replicate their behaviour. These steps require creating industry-wide reporting systems, including record keeping and coordination mechanisms along with checks and balances like hearings and/or a chance to appeal.

Besides limiting offending users' access, offline redressal can be pursued through existing provisions of the Indian Penal Code. While the IPC does not directly address online harassment, the language of its provisions suggests that they can be applied to harassment in the metaverse. For instance, Section 354 of the IPC focuses on assault or criminal force with intent of 'outraging the modesty of a woman' through physical acts, gestures, or sexually coloured remarks. Voyeurism and stalking are also specifically addressed. Further, Section 509 criminalises words, gestures and acts intended to 'insult the modesty of a woman'. And the Information Technology Act specifically deals with online harassment through Section 67 and 67A, which makes sharing obscene or pornographic content

or conduct a punishable offence. However, Section 354A of the IPC, which punishes sexual harassment, explicitly mentions physical advances, and would not in its current form cover an incident of groping in the metaverse. Further, cyberstalking as defined under Section 354D only contemplates a male offender and a female victim, which does not account for the spectrum of harassment as well as the veil of anonymity in the metaverse that might obscure the offender's gender, age or other characteristics. These will need to be broadened to account for harassment in the metaverse.

It is essential also to train and sensitise law enforcement officials to identify and deal with cases of online harassment in the metaverse. Such capacity building will enable them to understand the technology, its applications and the potential offences that can be committed. It will also be important to foster some degree of cooperation between law enforcement and metaverse operators, for instance to familiarise the police with the user protection measures available on a particular platform, or to identify offenders.

Besides these remedial solutions, a preventive solution would be to equip users with the technological tools to protect themselves from attempted harassment. After the 2016 incident on Quivr, its founders immediately responded with an apology and an in-game fix: a gesture users could use to immediately push other users away from their avatar, immediately getting away from the harassing parties.¹³⁰ Meta provides the option of a Safe Zone, which can be used to access a private space where nobody can see or talk to the user. It is worth noting however that the Meta groping victim was unable to effectively use this feature to protect themselves.¹³¹ In practice, user protection requires a balance between tools to empower users as well as hold platforms accountable. A mixture of these two solutions is the most likely outcome to address the issue: universalizing gestures or features across platforms within the metaverse that can protect users and prevent harassment, and instituted mechanisms for moderation and redressal of offences that work across platforms and prevent repeat offences from the same users.

b. Data collection and Manipulative advertising

The metaverse will be accompanied by an unprecedented level of data collection, including physiological data through wearable devices. This may enable the creation of comprehensive psychological profiles of individual users, which can then be used to target advertising that is far more effective than its current form, which calls for limits and safeguards. For instance, a game seeking to sell a user a virtual good or service may employ AI characters indistinguishable from another real user, and customize the gender, looks and other characteristics of the AI character based on the target user's psychological profile. By tracking data points such as eye movements, breathing, heart rate etc, 'promotional conversations' can be adjusted in real time to be most persuasive to a particular user.¹³² This extensive tracking combined with the artificial intelligence behind targeted advertising could lead to a situation where the user is highly prone to being manipulated and their individual agency is reduced.

Regulation is necessary to ensure that this level of manipulative advertising does not take place in the metaverse. Without regulatory interventions, it is almost certain that today's targeted advertising practices will evolve in the manner described above. Users must always be informed when a particular interaction within the metaverse is a targeted or sponsored event, making it clear to them that they are being advertised to. Illustratively, AI bots should be clearly labelled as such, to prevent users mistaking them for other humans. Policymakers should also consider a total ban on using certain physiological metrics for advertising algorithms, as it can be considered a form of psychological manipulation, even when the user has been nominally informed that the interaction they are in is a promotional one.

Future Data Protection Authority and the Metaverse

While there is currently no agency specifically tasked with administering a data protection framework, the proposed Data Protection Bill envisages the setting up of a Data Protection Authority for the purpose. It will be advisable for this DPA to closely examine the data collection and processing practices prevalent in the metaverse, with a special focus on physiological or biometric data, which has been designated as sensitive personal data in the Bill. From its findings the DPA could decide whether specific regulations are required to govern the collection and processing of data in the metaverse, over and above the applicable provisions of the Bill. For instance, limits may be set on the use of factors such as heart rate, breathing etc. to determine the advertising content presented to users of metaverse applications. Such regulations should be backed by evidence and expertise across business, technology and psychology to ensure a balance between protecting user rights and enabling the growth of innovative technologies and business models.

II. Ownership and Competition in the Metaverse

The metaverse will also challenge existing perspectives on intellectual property rights in gaming. For instance, existing protections will need to be extended to the metaverse, such as the use of trademarked logos or a copyrighted piece of art within a particular virtual space. Further, an uptick in user created content is also expected, raising important questions about the nature of protections applicable to content built on top of an existing game. The competition issues that have emerged out of technology markets in recent times are also likely to carry forward into the metaverse.

a. Mods, User created content and Intellectual property

Games, as software, are protected as ‘literary works’ under copyright legislation in India. Various elements of a particular game may further have their own protections – for example, a piece of music used in the background of a game, or the design of a popular cartoon character used within a game, are protected works in themselves. Courts in the United States have held that modifications (also known as ‘mods’) built on top of existing games are ‘derivative works’ in relation to the original game, and the rights in the original game extend to such derivative works.¹³³ In other words, a video game modification cannot be protected as an independent work, and the creator of the mod can be sued for infringement by the creators of the original.

While a number of user-created mods are regularly created and distributed and enhance the popularity of the base game on which they are built, commercializing them is a challenge for their creators. Currently, the terms on which users can create and distribute mods rely largely on the End User Licensing Agreement (EULA) of the original video game. While some EULAs may allow for a degree of monetization (usually by giving a small share of revenue) for user generated content, others, such as Blizzard’s recently updated EULA, claim ownership over all mods created by game players. It remains to be seen whether new jurisprudence is developed for the same in the metaverse, or if mods will continue to be treated as derivative works.

The argument can be made for offering protection to such user created content, as it plays an important role in the development of video games and often involves significant creativity and work on the part of the modder. Further, the current position as set out by the *Micro Star* case was evolved in 1998, over two decades ago, and developments in the intervening period may call for greater rights for modders.¹³⁴ As the metaverse leads to an uptick in user created content built on top of existing games, legal questions of ownership and rights in mods may once again come to the fore.

It must be noted here that the question whether video game mods deserve protection has never been raised in front of Indian courts, and thus there is no Indian jurisprudence on the matter. Thus, EULA terms continue to be the deciding factor in whether and to what extent content created by users on top of existing video games can be monetized by the user-creator.

b. Virtual items, NFTs and Ownership

Another key technology for the metaverse is blockchain. This refers to a distributed ledger of transactions stored across multiple computers linked in a peer-to-peer network. Essentially, it can verify transactions and track assets online, as seen in the cryptocurrency use case. An emerging use case for blockchains is the creation and trade in non-fungible tokens (NFTs). This refers to a unique, non-interchangeable unit of data stored on a blockchain ledger that can be sold and traded, often in the form of an image, video or audio clip. It is important to note that in most cases, NFTs represent the right to ownership in a particular asset, and not the intellectual property rights behind it (unless specifically provided for in the accompanying smart contract).

In the context of metaverse gaming, NFTs are likely to have a significant impact. Virtual objects (such as costumes, works of art and even virtual plots of land) are an essential part of the metaverse experience, allowing users to customize their avatar and surroundings. NFTs supply a way to track the authenticity and ownership of a particular virtual object, enabling the creation and sale of entirely unique objects (for instance, a collectors' edition t-shirt for a metaverse avatar to wear) that only one person can own and use at a time. It will also likely lead to the creation of secondary markets for reselling virtual objects. As mentioned in the section on lootboxes, if virtual objects capable of being resold for monetary value are obtained through a randomized process, offering such randomized boxes/items may attract gambling regulations in some jurisdictions. Another important use case for NFTs is taking virtual objects from one metaverse universe to another, thus enabling interoperability and extending the user's experience with that virtual object.

At present there is no specific law addressing NFTs in India, which are governed under the general law of contract. Given the growing interest in NFTs as a speculative investment, it remains to be seen if the government will impose any restrictions or taxes on NFTs such as the tax on income generated from cryptocurrencies.

c. Competition law, Gatekeeping and the Metaverse

Technology-enabled digital economies pose novel regulatory challenges, one of the most visible manifestations of which is in the worldwide movements in competition law. Governments and regulators are increasingly concerned about concentration in technology markets and its implications for online commerce and communication. Further, the prevalence of platform-based economies has raised concerns about the gatekeeping role played by the Big Tech companies running these platforms, and its impact on innovation and competition in the market. South Korea has already passed a law addressing the issue in the context of mobile app stores.¹³⁵ Other countries such as the United States have seen similar legislative proposals come up, such as the Open App Markets Bill, which seeks to restrict the gatekeeping power of companies running these stores.¹³⁶ India too has seen significant discussions on gatekeeping, with both Google¹³⁷ and Apple¹³⁸ facing complaints in the Competition Commission of India on the matter.

Such concerns, no matter their validity, might be reflected in the metaverse as well. With digital delivery quickly overtaking physical media in the way most people purchase and access games,¹³⁹ companies running such stores (such as Steam or Epic for PCs) are increasingly likely to face questions about their business practices and impact on the larger market. Here it is important to note the existence of multiple distribution models across the wide expanse of gaming. Besides mobile distribution (through app stores) and PC storefronts like Epic or Steam, there is also the console ecosystem, where hardware manufacturers like Microsoft (Xbox) and Sony (PlayStation) control digital distribution on their respective platforms through native storefronts.

Each of these markets have their own distinct dynamics. For instance, console makers often sell their hardware at a loss, aiming to recoup this through the sale of games and services, making these usually more closed off as a market than the PC or mobile game markets. These, too, are seeing some shakeups, as Sony faced a class action complaint¹⁴⁰ for monopolising the PlayStation Store last year, and Microsoft has adopted an ‘open app store approach’ across its various digital stores, including the Xbox store.¹⁴¹ Microsoft’s statement of intent to promote competition comes shortly after concerns were raised about concentration in the video game industry after Microsoft’s acquisition of Activision Blizzard for USD 68.7 billion in January 2022¹⁴² in what was seen as a massive move towards consolidation. Sony, too, bought Bungie studios shortly thereafter for USD 3.6 billion.¹⁴³

The challenges inherent in this intersection of competition law and digital economies will likely be reproduced in the metaverse, with a few businesses occupying key positions. How this plays out and its impacts will depend on several factors, but we predict a few trends. As with the console gaming market, users are likely to need specialised hardware to access the metaverse. This means that hardware manufacturers will play a central role and may even choose to subsidise the cost of hardware hoping to increase the volume of content consumption.

Second, the existing Big Tech companies will likely have a leg up in building the infrastructure of the metaverse, from hosting, advertising, creating hardware ecosystems to licensing and producing content. Mark Zuckerberg’s Meta, for instance, has already signalled an intent to become a key player in the metaverse through its rebranding, and has pivoted from being a social media company, leveraging its acquisition of the hardware company Oculus to help create an early infrastructure for the metaverse.

Thus, regulators and policymakers will likely pay more attention to existing competition issues in technology markets that play out in the metaverse. It will be important to balance these existing concerns and any new competition concerns that arise from the unique nature of the metaverse, to maximise user welfare while promoting innovation and competition in the market. Gatekeeping is at odds with the decentralised, interoperable vision of the metaverse that would transform it into a hub of communication, trade and creativity, and it is important to ensure that no entity exercises undue control or influence over the design, infrastructure or business practices prevalent in the metaverse.

III. Contemporary Regulatory Responses

Given the nascent stage of development of the metaverse, regulatory initiatives around it are few and far between. As the technology grows in scope and scale in the coming years, the regulatory issues are likely to grow in number and complexity. This section examines some of the steps that have already been taken in this regard, by governments and self-regulatory organisations.

a. South Korea

South Korea has long been a leading nation in promoting and regulating creative content markets, including online gaming. It proactively encouraged the development of gaming and its offshoots such as eSports, and today is one of the world’s leading gaming economies. So it is no surprise that it is also an early mover when it comes to regulating metaverses. In January 2022, South Korea unveiled a long-term road map to foster its metaverse related industries, with the aim of becoming the fifth largest metaverse market in the world. This includes plans for an online Korean language institute on metaverse platforms, the creation of a metaverse academy to train 40,000 local experts,¹⁴⁴ as well as making metaverse avatars for government officials, with the city of Seoul taking the lead in developing a ‘Metaverse Seoul’.¹⁴⁵

Besides preparing to foster the industry, South Korea has also taken cognizance of the problems discussed above. The South Korean Communications Commission (KCC) has set up a committee to look into user safety in the metaverse, with a particular focus on the safety of children. The 30-member committee will consist of experts from media, law, technology and industrial management, and will discuss issues in the metaverse including violence, sexual crime and exclusion.¹⁴⁶ The committee will study emerging issues in the metaverse and come up with recommendations for future rules and regulations. At the same time, some lawmakers have been working to draft amendments to South Korea's minor protection law, to impose greater accountability on online platforms for cases of grooming or sexual exploitation of children.

AVGC Task Force: Lessons from South Korea

South Korea's example offers some useful cues to the AVGC Task Force in the development of India's metaverse related industries.

- **Capacity building:** Skill development in areas such as animation, coding etc. is essential to create a base for metaverse development in India. The demographic advantages of a young population and a robust IT/ITeS sector should be leveraged to create opportunities for Indian metaverse businesses by providing training, grants, and support communities.
- **Holistic user safety:** Beyond building capacity, it will be necessary to address user safety aspects from a holistic, multidisciplinary lens. This can be accomplished by a set of guiding principles for India's metaverse industries, developed through collaborations between government, industries, and other relevant experts.
- **Dynamic solutions based on research:** The consistent study of issues emerging in and around the metaverse by interdisciplinary groups of experts will also enable the development of dynamic solutions to new challenges.

b. Case study for standard-setting: The OASIS Consortium

The OASIS Consortium was founded in 2021 and pulls together leaders deeply invested in the metaverse: from gaming, dating apps and immersive tech platforms like Roblox, Riot Games and Wildlife Studios to addressing safety and privacy in web 3.0.¹⁴⁷ Founded by Tiffany Wang, chief strategy and marketing officer of the AI company Spectrum Labs, the think-tank seeks to solve metaverse challenges not through government intervention, but by working with metaverse builders to self-regulate and inculcate a safety-first approach to design.¹⁴⁸ OASIS stands for Openness, Accountability, Security, Innovation and Sustainability, and the organization seeks to advance ethical standards around three core pillars: safe online communities, data privacy, and diversity and inclusion.

OASIS User Safety Standards

In January 2022 the OASIS Consortium published its first User Safety Standards.¹⁴⁹ This framework is based on 5 Ps: priority, people, partnership, product and process.

- **Priority** establishes that trust and safety are mission-critical for member companies, and covers accountable leadership, dedicated resources and a roadmap for the development of user safety, and cross-functional collaboration on trust and safety between departments or verticals.
- **People** focuses on ensuring policies are based on representation, learning and wellness, and includes diversity and inclusion, creating a 'learning organization' that gathers best practices from the broader industry, and promoting employee wellness, especially for those in high-stress roles such as content moderation.

- Partnership focuses on gaining expertise and objectivity by collaborating with a variety of stakeholders, including industry alliances, the media, law enforcement and government agencies. This tenet also recommends the establishment of an independent Advisory Board to give feedback on the trust and safety aspects of product updates etc.
- Product refers to applying current technology and design solutions, and includes clear community guidelines, visibility for data on how well trust and safety measures are working, proactive detection and moderation tools for the platform, and user reporting tools.
- Process emphasises the need to institute consistent enforcement of policies, regular and effective audits, clear systems for user appeals and escalation, regular reviews and updates of policies, bias prevention to ensure moderation is objective, data security frameworks, and transparency reports.

146

These standards also open the door for OASIS to preside over a grading system for platforms, similar to how buildings are graded for energy efficiency, or companies can be certified as B Corporations—signalling a commitment to social responsibility. Wang envisions the think tank as taking a multi-stakeholder approach to continually tweak its rules and says it is crucial for the safety standards to be reviewed biannually. This is due to the dynamic nature of this field, and the pace at which new challenges emerge. Illustratively, Wang has indicated that OASIS will collaborate with non-profits for specific advice in certain areas like deep fakes, or video files that are manipulated or falsified.

IV. Recommendations for India

Given the nascency of the metaverse, the AVGC Task Force should take the lead in articulating recommendations on how to resolve the issues identified above. Beyond building capacity through skilling, it will need to address user safety aspects from a holistic, multidisciplinary lens. This can be accomplished through a set of guiding principles for India's metaverse industries, developed through collaborations between government, industries, and other relevant experts. The Task Force can convene or assume stewardship of such an initiative. The consistent study of issues emerging in and around the metaverse by an interdisciplinary group of experts will also permit the development of dynamic solutions to emerging challenges. This will enable calibrated regulatory responses that balance between innovation and welfare, allowing for the optimum growth of India's metaverse industries.

From the initiatives and principles discussed above, the following actions can be taken by government agencies to prepare legal frameworks and regulatory mechanisms to suitably deal with the metaverse.

Principles	Recommended Actions
User Safety	<ul style="list-style-type: none"> • Curbing harassment: The application of existing laws against harassment (e.g., Sec. 354 IPC) to the metaverse should be clarified, and amendments brought where necessary. Law enforcement officials should be trained to deal with new forms of harassment and technologies. • Hardware safety standards: Safety and security standards for new devices such as VR headsets etc. should be created or adapted from existing international standard organizations such as the <u>IEEE</u> which are working on creating metaverse related standards. Indian standard setting organizations such as the Bureau of Indian Standards (BIS) and STQC should increase participation in international standard setting bodies to help create standards instead of merely adopting them

Data and Advertising Transparency	<ul style="list-style-type: none"> • Advertising guidelines: Advertising guidelines for the metaverse should be co-created with industry through ASCI along with a government committee with representation from the MIB, MeitY, Ministry of Women and Child Development, Ministry of Health etc. Users should always be informed when a particular interaction within the metaverse is a targeted or sponsored event, so it is clear to them that they are being advertised to. Illustratively, AI bots should be clearly labelled as such, to prevent users from mistaking them for other human users. • Limits on use of physiological data: Any future DPA should closely examine the data collection and processing practices that become prevalent in the metaverse, with a special focus on physiological or biometric data, which is designated as sensitive personal data in the Data Protection Bill. From its findings the DPA can determine whether specific regulations are needed to govern data collection and processing in the metaverse, over and above the applicable provisions of the Bill. For instance, limits may be set on the use of factors such as heart rate, breathing etc. to determine the advertising content presented to users of metaverse applications. Any such regulations should be backed by evidence and expertise across business, technology and psychology to ensure they achieve a balance between protecting user rights and allowing the growth of innovative technologies and business models.
Enabling Ecosystem	<ul style="list-style-type: none"> • Future-proof regulation: The next iteration of the IT Act and IT Policy are likely to deal with questions of gaming regulation. Any framework created hereunder should be flexible, technology-agnostic and principle-based in order to be future proof for the metaverse and its gaming applications. • Ethical principles for the metaverse: Similar to its work on ethical principles for responsible AI, the NITI Aayog should create a framework encouraging principles such as security by design, data hygiene, user empowerment through information etc. for metaverse products. • Industry promotion: Besides leveraging the existing skilling clusters, incubators, exhibitions and expos for the Indian metaverse, products and projects can be hosted/promoted by the NITI Aayog and/or the AVGC Task Force. • Intellectual property: The Department for Promotion of Industry and Internal Trade (DPIIT) should closely examine intellectual property issues in the space – mainly the rights in user created mods or items in a particular metaverse ‘world’ – and should clarify Indian law around the same. Use review of IPR Policy 2016 as an opportunity to ideate.

NOTES

- 1 Netflix's letter to the shareholders dated January 17, 2019. Available at - https://s22.q4cdn.com/959853165/files/doc_financials/quarterly_reports/2018/q4/FINAL-Q418-Shareholder-Letter.pdf
- 2 Fortune Business Insights, Global gaming market overview, Market Research Report, August 2021. Available at - <https://www.fortunebusinessinsights.com/gaming-market-105730#:~:text=The%20global%20gaming%20market%20size,growth%20of%2038.24%25%20in%202020.>
- 3 *Ibid.*
- 4 Mike Verdu, Let the Games Begin: A New Way to Experience Entertainment on Mobile. Dated November 02, 2021. Available at - <https://about.netflix.com/en/news/let-the-games-begin-a-new-way-to-experience-entertainment-on-mobile>
- 5 FICCI-EY, Playing by new rules: India's Media & Entertainment sector reboots in 2020, March 2021. Available at - https://assets.ey.com/content/dam/ey-sites/ey-com/en_in/topics/media-and-entertainment/2021/ey-india-media-and-entertainment-sector-reboots.pdf
- 6 PM Modi addressed the toy and gaming market, The News Minute, July 07, 2021. Available at - <https://www.thenewsminute.com/article/pm-modi-addressed-toy-and-gaming-market-151893#:~:text=Speaking%20recently%20about%20the%20video,are%20not%20Indian%20in%20concepts%E2%80%9D.>
- 7 Written evidence submitted by Ukie, the Association for UK Interactive Entertainment. Available at - <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/immersive-and-addictive-technologies/written/94958.pdf>
- 8 Written evidence submitted by Dr Paul Cairns and Dr Christopher Power. Available at - <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/immersive-and-addictive-technologies/written/94832.pdf>
- 9 Gaming Disorder, International Classification of Diseases, 11th Revision, World Health Organization. Available at - <https://icd.who.int/browse11/l-m/en#/http://id.who.int/icd/entity/1448597234>
- 10 *Ibid*
- 11 A weak scientific basis for gaming disorder: Let us err on the side of caution; Antonius J. van Rooij, Christopher J. Ferguson, Michelle Colder, Carras Daniel, Kardefelt-Winther, Jing Shi, Andrew K Przybylski. Available at - <https://psyarxiv.com/kc7r9>
- 12 American Psychiatric Association, Internet Gaming. Available at - <https://www.psychiatry.org/patients-families/internet-gaming>
- 13 Hazardous gaming, International Classification of Diseases, 11th Revision, World Health Organization. Available at - <https://icd.who.int/browse11/l-m/en#/http://id.who.int/icd/entity/1586542716>
- 14 Douglas A. Gentile, Edward L. Swing, Choon Guan Lim, and Angeline Khoo; Video Game Playing, Attention Problems, and Impulsiveness: Evidence of Bidirectional Causality; Psychology of Popular Media Culture, 2012, Vol. 1, No. 1, 62–70, American Psychological Association.
- 15 'Sexually violent' GTA 5 banned from Australian stores, December 04, 2014, BBC News. Available at - <https://www.bbc.com/news/technology-30328314>
- 16 Maria Fernanda Santos, Aline F. Bastos, Jose M. Oliveira, Ivan Figueira, Sonia Gleiser, Mirtes G. Pereira, Eliane Volchan, and Fátima S. Erthal; Hands Up! Atypical Defensive Reactions in Heavy Players of Violent Video Games When Exposed to Gun-Attack Pictures; Frontiers in Psychology. Available at - <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6370668/>
- 17 Kevin Draper, Video Games Aren't Why Shootings Happen. Politicians Still Blame Them, New York Times, August 05, 2019. Available at - <https://www.nytimes.com/2019/08/05/sports/trump-violent-video-games-studies.html>

- 18 Claire McCarthy, MD, Protecting children from the dangers of virtual violence, Harvard Health Blog, Harvard Medical School. Dated October 06, 2021. Available at - <https://www.health.harvard.edu/blog/protecting-children-dangers-virtual-violence-2016080210036>
- 19 Aysu Burak, More than 50,000 games have been added to Google Play Store in Q1 2021, Mobidictum. Dated June 14, 2021. Available at - <https://mobidictum.biz/google-play-store-50000-games-added-q1-2021/#:~:text=More%20than%2050%2C000%20games%20were,with%20more%20than%2050%2C000%20games.>
- 20 Written evidence submitted by the British Esports Association for DCMS Committee looking at the growth of immersive and addictive technologies. Available at - <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/immersive-and-addictive-technologies/written/94859.pdf>
- 21 Digital Grooming Tactics on Video Gaming & Video Gaming Adjacent Platforms: Threats and Opportunities, Radicalization Awareness Network, March 2021. Available at - https://ec.europa.eu/home-affairs/system/files/2021-05/ran_cn_conclusion_paper_grooming_through_gaming_15-16032021_en.pdf
- 22 The dark side of online gaming, The Children's Society. Dated February 09, 2021. Available at - <https://www.childrenssociety.org.uk/what-we-do/blogs/gaming-and-grooming#:~:text=Online%20grooming%20is%20when%20someone,moving%20money%20between%20bank%20accounts>
- 23 Yoonmo Sang, Sora Park, and Hogeun Seo. Mobile Game Regulation in South Korea: A Case Study of the Shutdown Law. Available at - https://link.springer.com/chapter/10.1007/2F978-94-024-0826-3_4
- 24 Sabrina Barr, Children With Gaming Addiction to be Offered Treatment by NHS, The Independent. Dated October 07, 2019. Available at - <https://www.independent.co.uk/life-style/health-and-families/gaming-addiction-nhs-treatment-children-video-games-health-a9146136.html>
- 25 Margot James, former Minister for Digital and the Creative Industries, Government of UK, said it as a part of her evidence to the Digital, Culture, Media and Sport Committee. Available at - <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmds/1846/1846.pdf>
- 26 Verbatim Debates, 255th Session of the Rajya Sabha. Dated December 03, 2021. Available at - <https://cms.rajyasabha.nic.in/UploadedFiles/Debates/VerbatimDebates/255/3122021/Full%20Day//FullDay.pdf> (See pages 52 - 56)
- 27 Vamsi Krishna Undavalli, Gobburu Sudha Rani, Jonnalagadda Ravi Kumar, Prevalence of internet gaming disorder in India: a technological hazard among adolescents, The International Journal Of Community Medicine And Public Health, Vol 7 No. 2(2020). Available at - <http://dx.doi.org/10.18203/2394-6040.ijcmph20200450>
- 28 Written evidence submitted by UK Research and Innovation towards the Digital, Culture, Media & Sport Committee's 'Immersive and addictive technologies' inquiry. Available at - <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/immersive-and-addictive-technologies/written/95558.pdf>
- 29 Written evidence submitted by the International Gaming Research Unit, Nottingham Trent University towards the Digital, Culture, Media & Sport Committee's 'Immersive and addictive technologies' inquiry. Available at - <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/immersive-and-addictive-technologies/written/94799.pdf>
- 30 Defined as *a pattern used intentionally by a game creator to cause negative experiences for players that are against their best interests and happen without their consent.*
- 31 José P. Zagal, Staffan Björk, Chris Lewis, "Dark Patterns in the Design of Games", Foundations of Digital Games Conference (14–17 May 2013). Available at - <https://core.ac.uk/download/pdf/301007767.pdf>
- 32 UK Gambling Commission, Remote gambling and software technical standards under section 89 and section 97 of the Gambling Act 2005. Available at - <https://www.gamblingcommission.gov.uk/standards/remote-gambling-and-software-technical-standards/rts-14-responsible-product-design>
- 33 Written evidence submitted by Camelot UK Lotteries Ltd to the Digital, Culture, Media & Sport Committee's 'Immersive and addictive technologies' inquiry. Available at - <https://committees.parliament.uk/writtenevidence/118/pdf/>
- 34 Telangana Ordinance No. 6 Of 2017, The Telangana Gazette, Part Iv-B, Extraordinary. Dated July 08, 2017. Accessed from - http://aigf.in/wp-content/uploads/2018/06/Eng_Ordi-No-6-of-2017-E.pdf

- 35 The Tamil Nadu Gaming and Police Laws (Amendment) Act, 2021, Tamil Nadu Government Gazette, Extraordinary. Dated February 04, 2021. Available at - http://www.stationeryprinting.tn.gov.in/extraordinary/2021/63_Ex_IV_1_E.pdf
- 36 Dr. K.R. Lakshmanan vs. State of Tamil Nadu [1996 SCC (2) 226]
- 37 FICCI-EY, Playing by New Rules: India's Media and Entertainment Sector Reboots in 2020. March 2021
- 38 J. Clement, Number of available gaming apps in the Google Play Store from 1st quarter 2015 to 1st quarter 2022, Statista. Dated April 25, 2022. Available at - <https://www.statista.com/statistics/780229/number-of-available-gaming-apps-in-the-google-play-store-quarter/>
- 39 L. Ceci, Number of available apps in the Apple App Store from 2008 to 2022, Statista. Dated May 17, 2022. Available at - <https://www.statista.com/statistics/268251/number-of-apps-in-the-itunes-app-store-since-2008/>
- 40 While responding to a Parliamentary question dated 02.02.2022, MeitY said that all gaming platforms are intermediaries. Response of the ministry is available at - <http://164.100.24.220/loksabhaquestions/annex/178/AU2.pdf>
- 41 Help Net Security, Cybercriminals launder money through mansions, private islands and crypto currency. Dated March 16, 2018. Available at - <https://www.helpnetsecurity.com/2018/03/16/cybercriminals-launder-money/>
- 42 Playing by new rules, India's Media & Entertainment sector reboots in 2020, March 2021, https://assets.ey.com/content/dam/ey-sites/ey-com/en_in/topics/media-and-entertainment/2021/ey-india-media-and-entertainment-sector-reboots.pdf
- 43 Playing by new rules, India's Media & Entertainment sector reboots in 2020, March 2021, https://assets.ey.com/content/dam/ey-sites/ey-com/en_in/topics/media-and-entertainment/2021/ey-india-media-and-entertainment-sector-reboots.pdf
- 44 Re: Complaints against Playing 11, Order dated 3 December 2020, <https://fifs.in/ombudsman/orders/>
- 45 Online games of Skill Charter, General Principles, AIGF, <https://www.aigf.in/wp-content/uploads/2021/04/3-AIGF-online-skill-games-charter-for-self-regulation-01.pdf>
- 46 Charter for Online Fantasy Sports Platform, FIFS, <https://fifs.in/wp-content/uploads/2021/02/FIFS.Charter.wef-01Sep20201.pdf>
- 47 The Framework, Principles and Standard to which EGBA Member Operations Annually Subscribe, Commit and Adhere to, EGBA Standards, 2011, <https://www.egba.eu/uploads/2018/11/EGBA-Standards-October-2011.pdf>
- 48 Summary of the Initiative, European Committee for Standardization (CEN), <https://www.eesc.europa.eu/en/policies/policy-areas/enterprise/database-self-and-co-regulation-initiatives/143>; Making standards for Europe, CENLEC, <https://www.cencenelec.eu/>; As agreed in the European Committee for standardisation (CWA 16259 : 2011) – 'Responsible Remote Gambling Measures'; <https://www.eesc.europa.eu/en/policies/policy-areas/enterprise/database-self-and-co-regulation-initiatives/143>
- 49 EGBA Standards, <https://www.egba.eu/responsibility/egba-standards/>
- 50 License Conditions and Code of Practice, 2020, Operating License Conditions, <https://www.gamblingcommission.gov.uk/licensees-and-businesses/lccp/print>
- 51 Securities exchange commission gaming and regulatory overview, <https://www.sec.gov/Archives/edgar/data/858339/000119312512115625/d268435dex993.htm>
- 52 National Consumer Protection Framework for Online Wagering: Baseline Study, Final report 2019, https://www.dss.gov.au/sites/default/files/documents/11_2019/d19_887121_final_baseline_study_-_national_consumer.pdf
- 53 National Consumer Protection Framework (National Framework), http://docreader.readspeaker.com/docreader/?jsmode=1&cid=brrmu&lang=en_au&url=https%3A%2F%2Fwww.dss.gov.au%2Fsites%2Fdefault%2Ffiles%2Fdocuments%2F08_2020%2Fncpow-fact-sheet28-august-2020.pdf
- 54 According to Black's Law Dictionary, gambling is defined as the act of risking something of value for the chance to win a prize. Gambling consists of a consideration, an element of chance and a reward. Wagering is a broader term that includes betting and gambling. Sourced from the report: Distinction between wagering, gambling, and betting, Chapter III, Legal Framework: Gambling and Sports Betting Including in Cricket in India, Law Commission of India, Report No. 276

- 55 License Conditions and Code of Practice, 2020, Operating License Conditions, <https://www.gamblingcommission.gov.uk/licensees-and-businesses/lccp/print>
- 56 Gaming Giant Nexon America Starts Accepting Bitcoin, Ethereum for In Game Purchases <https://cryptonews.com/news/gaming-giant-nexon-america-starts-accepting-bitcoin-ethereum-for-game-purchases.htm>
- 57 Nexon America Accepts Cryptocurrencies for Purchase of In-Game Items. <https://www.businesswire.com/news/home/20211214005561/en/Nexon-America-Accepts-Cryptocurrencies-for-Purchase-of-In-Game-Items>
- 58 Gaming Giant Wargaming Starts Accepting Bitcoin in BitPay Integration, <https://www.newsbtc.com/news/bitcoin/bitpay-enables-gaming-giant-wargaming-to-accept-bitcoin/>
- 59 <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>
- 60 Guidance For Risk based approach to Virtual Currencies, FATF, 2015, <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>
- 61 Virtual world Second Life to enforce anti-money laundering regs, 2019, <https://www.itnews.com.au/news/virtual-world-second-life-to-enforce-anti-money-laundering-regs-527558>
- 62 Money transmitting business have to be licensed
- 63 Linden Dollars Resellers Must Register With US Gov't, Says Analyst. Available at – <https://nwn.blogs.com/nwn/2013/05/linden-dollar-regulation.html>
- 64 Virtual Currencies Key Definitions and Potential AML/CFT Risks, Financial Action Task Force Report. Dated June 2014. Available at - <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>
- 65 Guidance For Risk based approach to Virtual Currencies, FATF, 2015, <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>
- 66 Help Net Security, Cybercriminals launder money through mansions, private islands and crypto currency. Dated March 16, 2018. Available at - <https://www.helpnetsecurity.com/2018/03/16/cybercriminals-launder-money/>
- 67 Those who are mules are clueless that they have been recruited for the purpose, and are exploited to receive criminal proceeds into their accounts before these are wired to another. In 2016 over 90 percent of money mule transactions were linked to cybercrime, according to Europol.
- 68 Usman W. Chohan, UNSW Business School; Critical Blockchain Research Initiative (CBRI); International Association of Hyperpolyglots (HYPIA); Centre for Aerospace & Security Studies (CASS) The Cryptocurrency Tumblers: Risks, Legality and Oversight, November 2017. Available at - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080361
- 69 CVC is a currency that has an equivalent value in real currency or acts as a substitute for real currency.
- 70 Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FinCen Guidance. Dated May 09, 2019. Available at - <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>
- 71 Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. Dated March 18, 2013. Available at - <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>
- 72 Regulatory Risks of In Game and In App Virtual Currency, <https://www.venable.com/insights/publications/2017/05/regulatory-risks-of-ingame-and-inapp-virtual-curre>
- 73 Money Laundering Using New payment Methods, FATF Report, 2010.
- 74 Guidance Note to financial Instrument Test, Malta Financial Services Authority. Available at - https://www.mfsa.mt/wp-content/uploads/2019/04/20190405_GuidanceFITest.pdf
- 75 Understanding the VFA Framework, Malta Financial Services Authority. Available at - <https://www.mfsa.mt/our-work/virtual-financial-assets/>

- 76 Malta requires CDD to kick in if the threshold of Euro 150 is crossed.
- 77 Understanding the VFA Framework, Malta Financial Services Authority. Available at - <https://www.mfsa.mt/our-work/virtual-financial-assets/>
- 78 Levelling Up India's Gaming Market 2021, Inside Digital Entertainment's Fastest Growing Sector, Redseer, Lumokai. Available at - <https://www.lumikai.com/post/leveling-up-india-s-gaming-market-2021>
- 79 The State of Mobile Gaming 2021, Sensor Tower. Available at - <https://sensortower.com/blog/app-revenue-and-downloads-2021>, <https://go.sensortower.com/state-of-mobile-gaming-2021>
- 80 Levelling Up India's Gaming Market 2021, Inside Digital Entertainment's Fastest Growing Sector, Redseer, Lumokai. Available at - <https://www.lumikai.com/post/leveling-up-india-s-gaming-market-2021>
- 81 World of Warcraft gold or Fortnite V-bucks
- 82 Also known as loot crates, mystery boxes, prize crates
- 83 Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, UNODC. Available at - https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf
- 84 Threat Intelligence Report, Underground Financial Fraud Report H2 2019, Cyber Sixgill. Dated January 27, 2020 Available at - https://info.cybersixgill.com/h219undergroundfraud-lp?hs_preview=lvGnkCHY-24886820745 and reported here
- 85 Anthony Cuthbertson, How children playing Fortnite are helping to fuel organized crime, The Independent. Dated January 13, 2019. Available at - <https://www.independent.co.uk/news/fortnite-v-bucks-discount-price-money-dark-web-money-laundering-crime-a8717941.html>
- 86 Alexandra Norton, Gaming the System: Money Laundering through Microtransactions and In-Game Currencies, JLIA Blog, PennState Law, Pennsylvania State University. Dated February 28, 2020. Available at - <https://sites.psu.edu/jlia/gaming-the-system-money-laundering-through-microtransactions-and-in-game-currencies/#:~:text=Another%20way%20that%20criminals%20could,online%20for%20real%2C%20clean%20cash>
- 87 Rishabh Sabarwal, The Fortnite V-Bucks black market that sells in game cosmetics for pennies, Sportskeeda. Dated January 10, 2022. Available at - <https://www.sportskeeda.com/fortnite/news-fortnite-v-bucks-black-market-sells-in-game-cosmetics-pennies>
- 88 *Ibid*
- 89 Gaming micro-transactions for chance-based items, Environment and Communications References Committee, The Senate, Parliament of Australia. Dated November 27, 2018. Available at - https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/Gamingmicro-transactions/~media/Committees/ec_ctte/Gamingmicro-transactions/report.pdf l-cft-risks.pdf
- 90 The New Trends Shaping the Loot Box landscape, Juniper Research, <https://www.juniperresearch.com/resources/analystxpress/march-2021/the-new-trends-shaping-the-loot-box-landscape>
- 91 Netherlands Gaming Authority- Study into loot boxes A treasure or a burden, Oliver Oosterbaan, 2018, <https://www.slideshare.net/OlivierOosterbaan/netherlands-gaming-authority-study-into-loot-boxes-a-treasure-or-a-burden>
- 92 Matthew Gault, 'Nearly All' Counter-Strike Microtransactions Are Being Used for Money Laundering, Vice News. Dated October 29, 2019. Available at - <https://www.vice.com/en/article/8xw7nx/nearly-all-counter-strike-microtransactions-are-being-used-for-money-laundering>
- 93 Virtual Currencies, Key Definitions and Potential AML/CFT Risks, <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-am>
- 94 Anthony Cuthbertson, How children playing Fortnite are helping to fuel organized crime, The Independent. Dated January 13, 2019. Available at -, <https://www.independent.co.uk/news/fortnite-v-bucks-discount-price-money-dark-web-money-laundering-crime-a8717941.html>; Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, UNODC, https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf
- 95 Gaming micro-transactions for chance-based items, Environment and Communications References Committee, The Senate, Parliament of Australia. Dated November 27, 2018. Available at - https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/Gamingmicro-transactions/~media/Committees/ec_ctte/Gamingmicro-transactions/report.pdf

- 96 Loot boxes in video games, March 2022, House of Commons Library, UK Parliament. Available at - <https://commonslibrary.parliament.uk/research-briefings/cbp-8498/>
- 97 Gaming micro-transactions for chance-based items, Environment and Communications References Committee, The Senate, Parliament of Australia. Dated November 27, 2018. Available at - https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/Gamingmicro-transactions/~media/Committees/ec_ctte/Gamingmicro-transactions/report.pdf
- 98 Statement about lootboxes/loot crates, Danish Gambling Authority. Dated November 29, 2017. Available at - <https://www.spillemyndigheden.dk/en/news/statement-about-loot-boxes-loot-crates>
- 99 Gaming micro-transactions for chance-based items, Environment and Communications References Committee, The Senate, Parliament of Australia. Dated November 27, 2018. Available at - https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/Gamingmicro-transactions/~media/Committees/ec_ctte/Gamingmicro-transactions/report.pdf
- 100 Cerulli-Harms, A. et al., Loot boxes in online games and their effect on consumers, in particular young consumers, Publication for the committee on the Internal Market and Consumer Protection (IMCO), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020. Available at - [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652727/IPOL_STU\(2020\)652727_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652727/IPOL_STU(2020)652727_EN.pdf)
- 101 Philippe Vlaemminck and Robbe Verbeke, The Gambling Law Review: Belgium, The Law Reviews. Dated May 09, 2022. Available at - <https://thelawreviews.co.uk/title/the-gambling-law-review/belgium#:~:text=A%20loot%20box%20must%20be,his%20or%20her%20game%20character.&text=A%20player%20who%20pays%20for,in%20gambling%20under%20Belgian%20law.>
- 102 John Woodhouse, Loot boxes in video games, Commons Library Research Briefing, House of Commons Library. Dated May 25, 2022. Available at - <https://commonslibrary.parliament.uk/research-briefings/cbp-8498/>
- 103 *Ibid*
- 104 Loot boxes within video games, UK Gambling Commission, 2017, <https://www.gamblingcommission.gov.uk/news/article/loot-boxes-within-video-games>
- 105 Section 6 of the Gambling Act, 2005 which regulates gambling defines gaming as “playing a game of chance for a prize”. Under section 6(5), a prize in relation to gaming (except in the context of gaming machines): (a) means money or money's worth, and (b) includes both a prize provided by a person organising gaming and winnings of money staked.
- 106 Government launches call for evidence on video game loot boxes, Press Release, Department for Digital, Culture, Media & Sport, Government of UK. Available at - <https://www.gov.uk/government/news/government-launches-call-for-evidence-on-video-game-loot-boxes>
- 107 Gambling Control Bill and Gambling Regulatory Authority of Singapore Bill - Wrap-Up Speech by Mr Desmond Tan, Minister of State, Ministry of Home Affairs and Ministry of Sustainability and the Environment, Parliamentary Speeches, Ministry of Home Affairs. Available at - <https://www.mha.gov.sg/mediaroom/parliamentary/gambling-control-bill-and-gambling-regulatory-authority-of-singapore-bill-wrap-up-speech/>
- 108 *Electronic Arts Incorporated, at Redwood Shores Parkwood (United States) vs. The Board of Directors of the Gaming Authority*, Court of The Hague, <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:10428>
- 109 Chris Scullion, Dutch court overrules decision to fine EA €10 million for FIFA loot boxes, VGC news. Dated March 10, 2022. Available at - <https://www.videogameschronicle.com/news/dutch-court-overrules-decision-to-fine-ea-e10-million-for-fifa-loot-boxes/>
- 110 Judgment of the Division Of Administrative Jurisdiction in EA v. The Board of Directors of the Gaming Authority. Dated March 09, 2022. Available at - <https://www.raadvanstate.nl/actueel/nieuws/@130150/202005769-1-a3/>
- 111 Charlie Hall, Microsoft, Nintendo, and Sony to require loot box odds disclosure, Polygon. Dated August 7, 2019. Available at - <https://www.polygon.com/2019/8/7/20758617/ftc-loot-boxes-policy-ps4-xbox-one-nintendo-switch>
- 112 Consulting on new guidance on ads for 'loot boxes' and other in-game purchases, Advertising Standards Authority Ltd. and The Committee of Advertising Practice Ltd. Dated November 05, 2020. Available at - <https://www.asa.org.uk/news/consulting-on-new-guidance-on-ads-for-loot-boxes-and-other-in-game-purchases.html>

- 113 Loot boxes in online games and their effect on consumers, in particular young consumers, Project for the European Parliament, ConPolicy - The Institute for Consumer Policy. Available at – <https://www.conpolicy.de/en/project/loot-boxes-in-online-games-and-their-effect-on-consumers-in-particular-young-consumers/>
- 114 Inside the Virtual Item economy: True Ownership of In-Game Digital Items is the Future of the \$100 Billion Video Game Industry, Wax io. Dated December 08, 2018. Available at – <https://legacy.wax.io/ja/blog/inside-the-virtual-item-economy-true-ownership-of-in-game-digital-items-is-the-future-of-the-100-billion-video-game-industry>
- 115 NFT Games India: The New Way to earn a Living, Deccan Herald. Dated December 09, 2021. Available at – <https://www.deccanherald.com/brandspot/pr-spot/nft-games-india-the-new-way-to-earn-a-living-1059171.html>
- 116 Simon Chandler, Money Laundering Might Taint NFTs Too, Prepare for Tighter Controls, Crypto News. Dated March 27, 2021. Available at – <https://cryptonews.com/exclusives/money-laundering-might-taint-nfts-too-prepare-for-tighter-co-9689.htm>
- 117 Tala Michel Issa, NFT fraud: Money laundering and wash trading on the rise, expert warns, Alarabiya News. Dated April 06, 2022. Available at – <https://english.alarabiya.net/features/2022/04/06/NFT-fraud-Money-laundering-and-wash-trading-on-the-rise-expert-warns>
- 118 (2020) 10 SCC 274
- 119 While responding to a Parliamentary question dated 02.02.2022, MeitY said that all gaming platforms are intermediaries. Response of the ministry is available at - <http://164.100.24.220/loksabhaquestions/annex/178/AU2.pdf>.
- 120 Matthew Ball, Framework for the Metaverse, MatthewBall.vc. Dated June 29, 2021. Available at - <https://www.matthewball.vc/all/forwardtothemetaverseprimer>
- 121 <https://bollyheroes.com/>
- 122 <https://www.lokaworld.app/>
- 123 Swathi Moorthy, TCS starts taking small virtual steps towards metaverse, Money Control. Dated February 23, 2022. Available at - <https://www.moneycontrol.com/news/business/tcs-starts-taking-small-virtual-steps-towards-metaverse-8152321.html>
- 124 Bismah Malik, How Indian software exporters are tapping the \$8 trillion Metaverse opportunity, Business Today. Dated January 25, 2022. Available at - <https://www.businesstoday.in/latest/corporate/story/how-indian-software-exporters-are-tapping-the-8-trillion-metaverse-opportunity-320337-2022-01-25>
- 125 Devesh K. Pandey, Centre sets up AVGC promotion task force for animation, visual effects, gaming and comic sector, The Hindu. Dated April 08, 2022. Available at - <https://www.thehindu.com/news/national/centre-sets-up-task-force-to-promote-animation-visual-effects-gaming-and-comics/article65302265.ece>
- 126 Tanya Basu, The metaverse has a groping problem already, MIT Technology Review. Dated December 16, 2021. Available at – <https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/>
- 127 Jordan Belamire, My First Virtual Reality Groping, Medium. Dated October 21, 2016. Available at - <https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee>
- 128 Tanya Basu, The metaverse has a groping problem already, MIT Technology Review. Dated December 16, 2021. Available at – <https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/>
- 129 Nina Jane Patel, Reality or Fiction?, Medium. Dated December 21, 2021. Available at - <https://medium.com/kabuni/fiction-vs-non-fiction-98aa0098f3b0>
- 130 Aaron Stanton, Dealing With Harassment in VR, Upload. Dated October 25, 2016. Available at - <https://uploadvr.com/dealing-with-harassment-in-vr/>
- 131 Tanya Basu, The metaverse has a groping problem already, MIT Technology Review. Dated December 16, 2021. Available at – <https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/>
- 132 Louis Rosenberg, The metaverse needs aggressive regulation, Venture Beat. Dated December 04, 2021. Available at - <https://venturebeat.com/2021/12/04/the-metaverse-needs-aggressive-regulation/>
- 133 *Micro Star v Formgen*, US Court of Appeals for the Ninth Circuit

- 134 Carl "Ott" Lindstrom, Mod Money, Mod Problems: A Critique of Copyright Restrictions on Video Game Modifications and an Evaluation of Associated Monetization Regimes, 11 Wm. & Mary Bus. L. Rev. 811 (2020), <https://scholarship.law.wm.edu/wmblr/vol11/iss3/6>
- 135 Kate Park, South Korea passes 'Anti-Google law' bill to curb Google, Apple in-app payment commission, Tech Crunch. Dated August 31, 2021. Available at - <https://techcrunch.com/2021/08/31/south-korea-passes-anti-google-law-bill-to-curb-google-apple-in-app-payment-commission/>
- 136 Adi Robertson, Everything you need to know about the bill that could blow up the app store, The Verge. Dated February 29, 2022. Available at - <https://www.theverge.com/22914479/open-app-markets-act-legislation-senate-committee-markup-explained>
- 137 Tarush Bhalla, CCI probe finds Google's Play Store billing guidelines 'unfair' and 'discriminatory', The Economic Times. Dated March 31, 2022. Available at - <https://economictimes.indiatimes.com/tech/technology/cci-probe-finds-googles-play-store-billing-guidelines-unfair-and-discriminatory/articleshow/90550596.cms>
- 138 Reuters, CCI orders investigation into Apple's business practices in India, Mint. Dated January 01, 2022. Available at - <https://www.livemint.com/industry/infrastructure/india-antitrust-body-orders-investigation-into-apple-s-business-practices-in-india-11640955821370.html>
- 139 Kyle Orland, Physical console games are quickly becoming a relatively niche market, Ars Technica. Dated February 18, 2022. Available at - <https://arstechnica.com/gaming/2022/02/fewer-and-fewer-console-games-are-seeing-a-physical-release/>
- 140 Kirsten Errick, Sony Sued for Monopolization of PlayStation Store, Law Street Media. Dated May 06, 2021. Available at - <https://lawstreetmedia.com/news/tech/sony-sued-for-monopolization-of-playstation-store/>
- 141 Ian Sherr, Microsoft vows Windows, Xbox app stores will promote competition, CNET. Dated February 9, 2022. Available at - <https://www.cnet.com/tech/mobile/microsoft-promises-better-competition-in-its-windows-and-xbox-app-stores-ahead-of-regulation/>
- 142 Carrie Mihalcik, FTC to review Microsoft's \$68.7B deal to buy Activision Blizzard, report says, CNET. Dated February 1, 2022. Available at - <https://www.cnet.com/tech/gaming/ftc-to-review-microsofts-68-7b-deal-to-buy-activision-blizzard-report-says/>
- 143 Matt Kim, Sony Buys Bungie for \$3.6 Billion, IGN India. Dated January 31, 2022. Available at - <https://in.ign.com/destiny/170090/news/sony-buys-bungie-for-36-billion>
- 144 S.Korea aims to become world's 5th-biggest metaverse market by 2026, Daijiworld. Dated January 20, 2022. Available at - <https://www.daijiworld.com/news/newsDisplay?newsID=917343>
- 145 Julie Gaubert, Seoul to become the first city to enter the metaverse. What will it look like?, EuroNews. Dated November 11, 2021. Available at - <https://www.euronews.com/next/2021/11/10/seoul-to-become-the-first-city-to-enter-the-metaverse-what-will-it-look-like>
- 146 DANNY PARK, Sexual harassment in metaverse triggers S.Korean government response, Forkast. Dated January 27, 2022. Available at - <https://forkast.news/headlines/sexual-harassment-metaverse-government/>
- 147 <https://www.oasisconsortium.com/>
- 148 ANDREW R. CHOW, An Industry-Backed Group Thinks the Metaverse Can Avoid the Ills of Social Media. Here's How, Time. Dated January 06, 2022. Available at - <https://time.com/6133271/oasis-safety-metaverse/>
- 149 User Safety Standards, OASIS Consortium. Available at <https://www.oasisconsortium.com/usersafetystandards>



©2022 Koan Advisory Group

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from Koan Advisory Group

contactus@koanadvisory.com | www.koanadvisory.com