CyberPeace
Foundation

ONLINE GAMING

Opportunities, Challenges
and Recommendations for Stakeholders

Online gaming creates a global business market promoting economic growth of countries globally for decades now. However, the booming market of online games also holds safety and security challenges. This whitepaper examines the opportunities, challenges, and recommendations related to it at depth.

PREFACE

From tabletops to virtual reality, how we play online games is changing with the times. As the number of players continues to grow, it is clear that the technological possibilities of online gaming are endless. With industry leaders announcing cheaper headset options, blurring the lines between fantasy and reality is becoming more accessible for mass markets, and the pace is anticipated in future.

Cloud gaming takes advantage of faster, more reliable internet connections by giving gamers the ability to stream games rather than playing on a console. In the future, games could automatically generate game content that is customized to fit each player's personality and playstyle, based on their player data. As these technologies develop, they alter the way users experience games, and provide new opportunities for brands and advertisers to tap into enhanced viewer engagement.

Many industry players will thrive in this new environment, while others will fall by the wayside. Who will emerge victorious, and lead us into the future of entertainment?

Unfortunately, flipping the coin will also bring the individuals of the 21st century, who has been in touch with modern gaming culture knows that it contains several elements that can only be described as harmful, if awareness and attention is not given.

The present white paper is derived with the objective to provide deeper insights towards children, adolescents, adults and concerned guardians alike about uncontrolled gaming's real dangers. It highlights eye-opening statistics and horrific real-life incidents and prescribes what precautions must be taken to keep young gamers safe.

By following the preventive and protective measures detailed in the white paper, end-users and parents can take appropriate action to prevent crime and psychological issues like addiction from ever occurring. More importantly, they can help themselves or their wards lead healthy, happy, and productive lives. Finally, the whitepaper shows the critical role government regulators play in dealing with emerging issues and challenges. The scope for improvement and remedies to make gaming a less risky activity are also elaborated.

CyberPeace | Foundation

Today online gaming continues to have become a sky-rocketing business market. It is by no means a small industry. Perhaps, by the last quarter of 2021 approximately about 2.7 billion people globally is believed to be engaged into the segment of playing online games. This is accounting almost one-third of the total population across countries. The generated revenue structure for digital games during the year 2019, is emphasized as below.
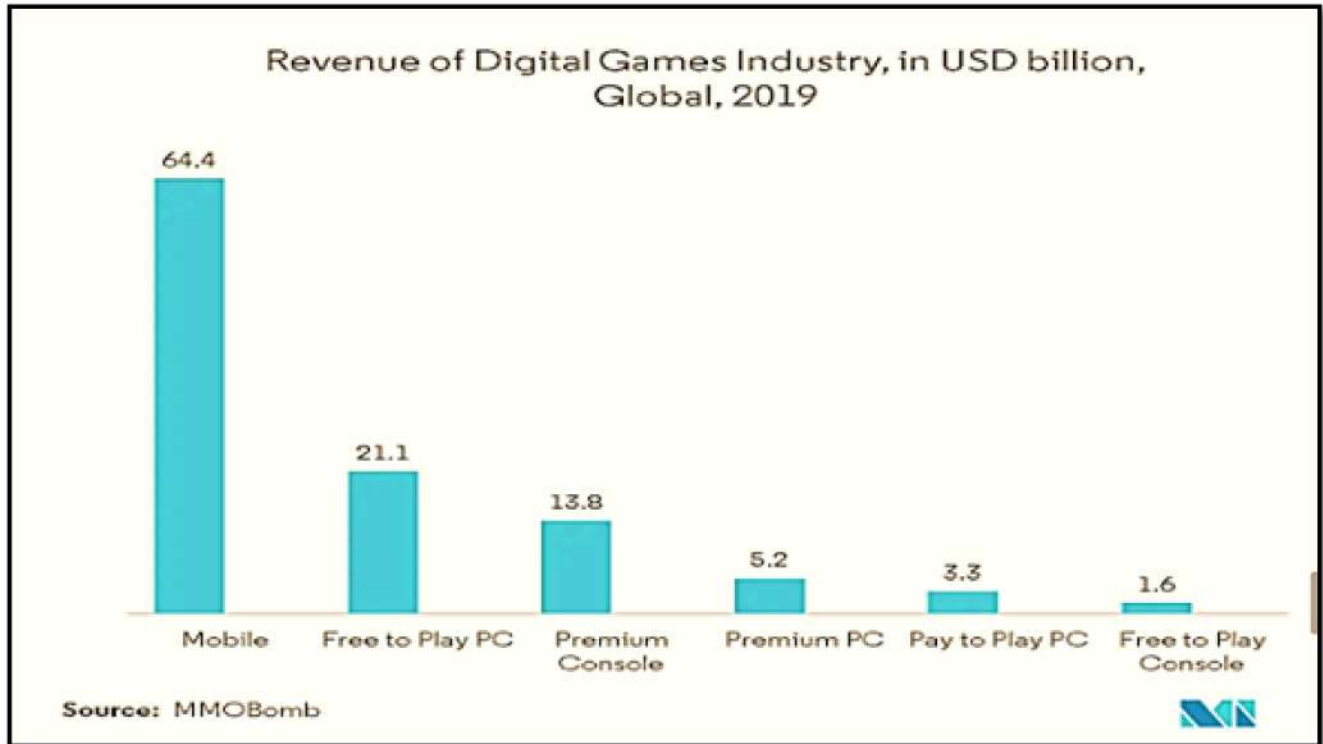
(The above Figure are marked in USD$, Billion)

It has been observed that, during 2019, the global gaming market within the United States were valued at $151.55 billion. The industry expects it to grow to $256.97 billion by 2025, thereby registering a CAGR of 9.17% over the forecast period. **The online gaming segment in India is projected to grow at a CAGR of 21 per cent over FY21-FY25 to reach a size of INR 29,000 Crore.** Of the total size, online casual gaming sub-segment is the most significant one and stands at INR 6,000 Crore accounting for 44 per cent of the total online gaming revenues.

Nonetheless, the segment is significantly under indexed on monetization with lower aver-age revenue per user (ARPU) as compared to gaming markets like - Indonesia, Malaysia and South Africa which are comparable in terms of the per capita GDPs. Factors like increasing smartphone penetration, internet penetration, young population and adoption of digital payments adoption has been determined as major growth drivers for such booming gaming industry.

Smartphone gaming is witnessing tremendous growth, and smartphones have made online games the most popular activity among young people. The release of 5G and unlimited data plans will further drive cloud gaming across the globe. Growth in digital consumption sophistication has helped online gaming become a mainstream entertainment option. Besides, there are supply side factors like increase in supply of world class titles, games with localized content, new features such as multiplayer and social elements added to games, and an increase in investor interest at large.

Online gaming is hugely popular among children and adolescents mostly, though adults also find it as a source of leisure, entertainment and escapism from everyday world. In otherwords, it has become a societal realism of 21st century to continuously be with the quest of attaching self-identity with the innovations of internet and social media, surpassing reality. Online games give children the chance to learn to, collaborate with others, connect with friends around the world, learn new things, and simply have fun.

While online gaming is an excellent entertainment outlet, it contains several risks that must be acknowledged and addressed by parents, gamers, and the government. Cybercriminal activity, for example, is something that needs to be contained. Aspects like addiction, cyberbullying, and indecent exposure also need a look. There are many ways for users to play games online. This includes free games found on the internet, games on mobile phones and handheld consoles, as well as downloadable and boxed games on PCs and consoles such as the PlayStation, Nintendo Wii or Xbox. Some of the most common devices on which online games are played includes :

01 **PC Games**

Basically played on a PC, similar to software programmes, can be bought offline or online. Many PC games make use of the internet, and many 'Massively Multiplayer Online' (MMO) games, where gamers interact together in virtual spaces, are PC games.

02 **Web Games and Application Apps**

These are accessed from unique websites that hosts a platform for varying games together. Many of these games are free of charge online, although some may have paid-for components.

03 **Consoles**

These are purchased boxed products from shops consisting of game discs with manuals. And can be played via connection to internet on home network just like other computers. Gamers can download expansions and renew subsriptions online.

04 **Mobile Games**

They can be free or either chargeable. There are opportunities to purchase added functionality such as 'in-app' purchases. These functions however can be deactivated, usually through the phone settings. .

This white paper discusses such risks and suggests the precautions that must be taken to prevent from becoming a victim of harmful activities.

The unique integration of an online space, has created a distinctive, and highly accommodating, social environment among users. On one-hand while it promotes range of social accommodators associated with all mediated social outlets (i.e., visual anonymity, asynchronicity), online games provide a shared, playful activity. The presence of a shared activity helps to facilitate the development and maintenance of social relationships as well as further socially accommodate its users, as social communication can become intertwined with the activity itself, reducing the pressure to maintain and guide direct socialization.

On the other-hand they have several risks associated with them. Excerpts from the Report by CyberPeace Foundation (published in IndiaTv) points that Children are more highly vulnerable to cybercrimes and cybercriminals pursue magnifying tricks in accessing personal information, location, financial data, etc by fraudulent means through the mode of these games online. Knowing about these risks will help the user remain safe and enjoy a positive gaming experience.

2.1 Risks

Some risks of online gaming include the following.

2.1.1 Gaming Addictions

The World Health Organization added the term 'gaming disorder' to its medical reference book "International Classification of Diseases" in 2018. It was classified under the section that deals with "Disorders due to Addictive Behaviours (Category 6)." This category also deals with addictive behaviours related to alcohol, gambling, and drugs. Some experts believe that it is harmful to label people enthusiastic about gaming, but everyone agrees that the percentage of people who meet the proposed criteria for addiction to video games is around 1-9%.

(Image courtesy: Pexels)

A user must have five or more of the following signs in one year to be considered to have a problem, according to the proposed criteria in the DSM-5.

- Thinks about gaming all the time or a lot of the time.

- Feels terrible when access to gaming is denied

- Needs to spend more time playing to feel good

- Is unable to quit or play less

- Does not want to do things they liked earlier

- Has problems with work or school due to gaming

- Plays despite problems

- Lies to people close to them about the amount of time spent gaming.

- Uses gaming to cope with negative moods or feelings

2.1.2 Sexual Grooming and Inappropriate Content

A significant risk of online gaming is that it may expose children to sexual predators. Sexu-al predators often carry out grooming online to meet with children in real life or receive explicit photographs. Children become vulnerable during their interaction with strangers in chat rooms or inside the game environment itself.

Discord, a popular gaming app, has often been used for grooming. In a glaring example, two underaged boys were lured using Discord with false promises of a better life. They were held captive in a filthy trailer, and one was sexually abused for over a year. Seven people were arrested in St. Petersburg over the incident.

Gaming can also be a "gateway drug" into online pornography. For example, several Twitch streamers do activities that border on indecent. The incident where many people wanted to buy Gamer girl bathwater for $30 should be an appropriate insight. The same girl charges $2,500 a month for access to "lewd" Snapchat content. Games like GTA or even Roblox can contain inappropriate content.

2.1.3 Cyber Bullying in Online Gaming

Suicide is ranked third among causes of death in young people aged 15 to 24. Online gaming can expose children to cyberbullying, leading to other severe problems like depression or even suicide. Children often make avatars of themselves and use these to play online games. However, the Internet's anonymity leaves them open to other players harassing, bullying, or ganging up on them. Curse words and hurtful messages are often sent over the Internet if a child does not perform well, and other children may resort to excluding them from playing altogether. Such situations can be stressful for a child.

The danger is compounded by the fact that strangers may find the child's location in real life and put them at risk. The child or streamers can also misuse live-streaming apps.

2.1.4 Poor Physical Health

Games like Pokémon Go encourage players to go outside, roam and look out for Pokémon characters. However, most online games like Clash of Clans or PUBG require that you remain seated for long hours. Besides causing mental strain, sitting in one place increases the risk of deep vein thrombosis, cancer, heart disease, liver disease, carpal tunnel, and other significant problems.

Some of these are life-threatening problems, while cancer and heart disease are among the world's top three killers today. Continuous exposure to the blue rays from a monitor or smartphone can also increase the risk of damage to the eyes and harm people's sleep schedules.

2.1.5 Exploitative DLCs And In-App Purchases

The UK recently banned misleading advertising for mobile games for a reason.

Parents should become aware that there are facilities for making in-app and in-game pur-chases in several games, most notably addictive mobile multiplayer gamers. These so-called "Gacha games" sell loot boxes with a low chance of containing an item the player wants. Such games are essentially gambling and have a pay-to-win mechanism leading to children spending hundreds if not thousands to be "good" at their game.

Children often do not understand the significance of using their parents' debit/credit cards for making these purchas-es. Moreover, there is a question of cybersecurity and compromise of financial data. Some games are also exploit-ative in the sense that they offer limited "free trials" but overcharge at an annual rate once the trial expires. There have even been instances of children emptying their parents' bank accounts for making in-game purchases.

(Image courtesy: Pexels)

2.1.6 Risk of downloading Malware

One of the most significant risks involved in online gaming is the risk of downloading malware. Cybercriminals take advantage of the fact the people prefer to go for free downloads of pirated game versions instead of purchasing them. Pirated gaming copies often come bundled with malware that gets introduced into their systems with ease. Cracked copies of games also require children to shut down firewalls and anti-virus protections and quickly lead to malware infections.

Even older adults fall victim to such tactics, thereby putting their confidential financial information at risk.

2.2 Some Eye-opening Statistics

The amelioration of technology has further influenced online gaming, to the point that certain gamers have blurred the boundaries between reality and fiction. This industry is driven profusely by mobile gaming technology, and in recent years, the advancement of innovations such as machine learning (ML), artificial intelligence (AI), virtual reality (VR), and augmented reality (AR), among others, has intensified. The following statistics concerning online gaming show us a disturbing picture of the industry.

01 More than half a billion online gamers worldwide have compromised their data over the last five years.

02 The FBI has warned parents to be wary of sexual predators using games such as Fortnite to target underage children.

03 The average online gamer has experienced five cyberattacks due to their activities.

04 55% of gamers reuse passwords in different accounts. A practice that introduces significantsecurity risks.

05 A report from the eSafety Commissioner's Office has found that around 24% of children aged 8-17 met up with people in real life after encountering them online.

2.3 Horrific Real-Life Incidents

Online gaming can lead to various alarming incidents. Here are a couple of incidents that show hidden dangers with gaming.

Pedophile Government Officials

A New Jersey police officer was among 24 criminals arrested for luring underage children for sex in 2018. A serving NJ police officer, along with a nurse, firefighter, and others, set up an appointment with an online gamer expecting to find a 15-year-old boy or girl. Instead, they were trapped by law enforcement officers and charged with second-degree luring. This case became famous as "Operation Open House."

Death By Swatting

"Swatting" is a practice used by some gamers to settle scores where gamers falsely report other gamers to the police for being criminals or terrorists. In one such incident, California resident Tyler R Barriss made a false emergency call to the authorities to get a SWAT team to target a rival gamer in Wichita. The address was an old one. When the SWAT team arrived, the door was answered by an innocent person named An-drew Finch, who was ultimately shot dead by the team.

Empty Bank Accounts

A teenager from Punjab's state in India spent nearly Rs 1.6 million from his parents' bank accounts for making in-app purchases on PUBG mobile. The 17-year old's parents had saved the money for medical expenses. The boy's father was a Government servant posted elsewhere and could not supervise him.

Death due to Suicide

A child by a 13-year-old boy died of suicide in Madhya Pradesh's Chhatarpur district after losing Rs 40,000 in an online game. The minor, who lived with his family in Chhatarpur's Shanti Nagar, took the extreme step as unbeknownst to his parents, he had spent Rs 40,000 into the online battle royale game called Free Fire.

The boy and his sister were alone at home at the time of the incident. According to the police, their mother, who was at work, received a message notifying that Rs 1,500 had been debited from her bank account. She called up her son and inquired about the deduction, at which he admitted to having spent the money on an online game. She reprimanded her son, following which he went to his room and hanged himself from the ceiling fan.

2.4 Cybercrime Related to Gaming

The United Nations Department on Drugs and Crime has stated that games and virtual economies such as World of Warcraft Gold are often used for money laundering. The gaming industry suffered 12 billion cyberattacks in 2019, showing they are genuine cybercrime victims and criminals are interested in the industry. Cybercriminals want valuable personal information and financial data that gamers often leave on forums or accounts.

For instance, people might be reusing passwords and thus compromise their accounts on other sites because they have the same passwords as those in a hacked gaming account. What's even more worrying is that several young gamers turn into hackers to commit cybercrimes. Almost 82% of teens recruited by online criminals got their hacking skills while learning to hack video games.

Having discussed risks, statistics, and incidents involving online gaming, we move on to what can be done to protect users from the various pitfalls.

3.1 Regular/Basic Self-Preventive Practices

Online users can use these tips to enjoy a safer and enjoyable gaming experience.

• Create a family e-Mail address for signing up for online games.

• Screenshots: If anything, bad happens while playing online games, stop immediately and take a screenshot (using the "print screen" button on the keyboard) and report it — using the screenshot as evidence.

• Use antivirus and anti-spyware programs.

• Be cautious about opening files attached to e-Mail messages or instant messages. Verify the authenticity and security of downloaded files and new software.

• Configure your web browsers securely. Use a firewall.

• Set up your user profile to include appropriate language and game content.

• Set time limits for children.

• Never download software and games from unknown websites.

• Beware of clicking links, images and pop-ups in the websites as they may contain a virus and harm the computer.

• Never give personal information over the Internet while downloading games.

• Some free games may contain a virus, so be cautious and refer while downloading them.

• Create and use strong passwords.

• Patch and update your application software.

3.2 Steps Parents Can Take

Parents play a very critical role in preventing children from becoming victims of cybercriminals, bullies, or perverts. They can take the following steps to safeguard their children.

• The foremost responsibility being a parent, one must pursue is to encourage their child/Children is to open up about ANY online activity that is disturbing them.

• Parents should understand what their child is playing and for how long. Keeping a time-table prevents addiction. They can apply time limits as a way to control bad habits. It is also a good idea to encourage children to take frequent breaks of 45 to 60 minutes.

• Playing games with children helps parents review said games and check if the community is a toxic one. They can also set up better privacy protection.

• Parents should set up online interaction settings in the Parental Control option on video game consoles. It helps restrict children from accessing dangerous websites.

• Keeping devices in shared family spaces discourages children from interacting with strangers or conducting inappropriate activities.

• Discourage children from using headsets when playing online games. Switching on the speakers will enable parents to know the kind of language used by strangers on the Internet and take appropriate action.

• They can turn on notifications in their accounts when installing consoles like Xbox or PlayStation to get direct messages.

• Parents should review their child's diet to ensure that it gets the right food. They should keenly watch out for symptoms such as light-headedness, altered vision, eye twitching, etc., and consult a medical professional immediately. If they find their children suffering from health issues, it is better to consult a GP.

• One should consider the ongoing costs of playing a game before purchasing it online. Setting up email on the devices helps to flag purchases. Parents should not allow children to use their debit/credit cards for making in-app purchases. Instead, you can use gift cards.

• It is advisable to create a lobby of friends the children know. Such lobbies prevent strangers from gaining access to the closed group.

• Keep an eye out for signs that third parties are manipulating the child.

Gaming is fun, but we have seen the dangers associated with online gaming. Besides addiction, gaming can cause mental disorders, especially in children who are of the impressionable age. Though parents have the responsibility to regulate gaming timings and other aspects, one must concede that children today are far smarter than their parents. They always seem to find a way out.

Online gaming has a dark side to it as it encourages online gambling. The dividing line between gaming and gambling is thin. It requires tremendous self-control not to breach the line, and you cannot expect children to be mature enough to take care. It is here that the Governments should step in and regulate the gaming app ecosystem. DSM-5 of the American Psychiatric Association recognizes Internet Gaming Disorder. Governments can act and stipulate strict regulations to control and prevent the younger generation from falling prey to vices like online gambling.

3.3 What Role Schools/Teachers Can Play

Teachers represent faculty and staff who are responsible for using a variety of instructional strategies to address individual students' strengths and needs, thereby ensuring each student has an opportunity to learn and succeed.

As teachers interact with their students while providing instruction, they play a very important role in establishing a safe, supportive learning environment. Positive teacher–student relationships can have long-lasting effects on the social, emotional, and academic development of youth. Teachers can improve the school's environment by actively seeking to prevent physical violence, bullying, and emotional abuse faced by students in the school by building relationships with students and staff.

3.3.1 Teachers can develop culturally responsive classrooms to foster a collaborative environment

Creating a culturally responsive classroom allows teachers to understand the differences among the cultures in the classroom, while still recognizing and valuing individual student needs. Understanding the diverse needs of students can assist teachers with creating relationships with students that are built upon collaboration. In turn, students will feel more empowered to speak out, ask questions, and give input to classroom procedures.

3.3.2 Getting Parents Involved

Schools are an important place to connect with parents and disseminate information about online safety. Invite parents to workshops about cyberbullying, and cyber safety practices and share the school's policy.

3.3.3 Preparing for Online Threats to Students

Schools together with teachers and special instructors/ counselors can implement several cyber policies and procedures to help keep their students safe from online threats. Create clear processes and practices to manage classroom and online behaviour and respond to any incidents that may arise such - the creation and implementation of responsible use policies to ensure that students are aware of appropriate online behavior, the use of filtering and blocking software's at school and at home (PCs) to prevent access to inappropriate content, and education about the risks of being online and how to stay safe.

3.3.4 Digital Citizenship in Schools and in nearby local communities

Digital citizenship is the ability to use technology in safe and appropriate ways. Teachers can encourage students what it means to be a responsible digital citizen as part of a broader strategy of promoting a positive school climate. A digital citizenship curriculum can include topics such as privacy and security, relationships and communication, cyberbullying and digital drama, digital footprints and reputation, self-image and identity, information literacy, and creative credit and copyright.

3.4 Regulatory Mechanisms by Government

As technological change has accelerated the business industry of Online gaming, the mechanisms attached to governance in regulating the landscape have failed to keep up with the pace. Divergent approaches and ad hoc responses while continue to threaten and fragment the interconnectedness that defines the digital age, leading to competing standards and approaches, lessening trust and discouraging cooperation.

3.4.1 Regulatory Mechanisms by Government of India

Government of India holds strict regulations towards minimalizing the above challenges however it is seemingly inadequate and must be ensured that the implementation is effectively channelized without negotiations. The key focused pointers that needs attention includes:

• A single self-regulatory body with membership of online fantasy games operators should be set up and receive government recognition.

• The games offered by online fantasy sports operators should continue to be skill-reliant, and in the event that any operator wishes to deviate from the recognized format of online fantasy sports, they will have to receive permission from the self-regulatory body. Operators will be required to keep collections of data to track player performance and the same would have to be supplied to the regulatory body periodically.

• Necessary safeguards to protect minors must be implemented, and pay to play formats should not be offered by operators to minors below 18 years of age.

• Operators should not advertise games of chance or gambling on their platforms. All advertisements of such games should be in compliance with the ASCI guidelines.

• A grievance redressal mechanism should be set up by the operators for dealing with disputes that arise as part of the games.

3.4.2 Here is how different countries around the world assign ratings. The chart also includes ratings stipulated by online gaming stores.

Europe and Asia – PEGI Ratings	PEGI 3 – Suitable for all ages
	PEGI 7 – Suitable for young children
	PEGI 12 – Suitable for children 12 years and older
	PEGI 16 – Suitable for children 16 and above
	PEGI 18 – Only suitable for adults

Entertainment Software Ratings Board – ESRB – the US only	RP – Rating Pending EC – Early Childhood E – Everyone E 10+ - Everyone above ten years T – Teen M – Mature A – Adult
App Store Ratings	4+ - Does not contain any objectionable material 9+ - Might have unsuitable content for children below nine years of age 12+ - Can contain inappropriate content for children below 12 17+ - Contains content inappropriate for children below 17 years
Google PlayStore	Google displays age-based ratings as determined by the IARC (International Age Rating Coalition). Thus, you will see the relevant rating, depending on the country in which you reside.
Australian Classification Board	G – General PG – Parental Guidance M – Mature R18+ - Restricted MA15+ - Restricted

CyberPeace | Foundation

Brazil	L – For all ages
	10 – Rated 10+
	12 – Rated 12+
	14 – Rated 14+
	16 – Rated 16+
	18 – Rated 18+

Companies comprising of the Online business world, are far from being alone in bearing responsibilities towards the end users that consists of individuals from varying age groups, however they do have specific accountabilities to ensure that the gaming experience is not causing detrimental effects to the psychosocial, economic landscape of these individuals. Hence, some measures must be followed by the online business industry strongly. These can be maintained under the broader mentioned 2 categories :

4.1 The Game Developers

• Ensure games are inclusive environments, representing the diversity of the players, providing positive role models, avoiding stereotyping and overtly sexualized representations, and providing characters that all genders from diverse backgrounds can relate to.

• Address challenges to flagging mechanisms in the game, intended to report inappropriate behaviour, to ensure these are not misused. These mechanisms should be easily available and always visible to the player and should go beyond flagging hacks or cheating.

• While designing games, consider how some features might be restricted if required for underage players. This could be related specifically to monetization features, such as loot boxes or turning off in-game purchasing and setting spending limits. It could also apply to regulating communication features or being able to play games in offline mode.

• Review use of techniques that are explicitly designed to hold attention and prevent users from logging off, which may make it more difficult for children to manage their game time.

• Investment and attention must be given on R & D by the developers of games in creating age specific games. Cautiously design and decide, varying demographics, words, sound note, etc introduced in a game.

• Attention must be given on age-verification techniques that do not infringe children's rights to privacy or collect unnecessary personal data.

4.2 For Game Publishers

• Ensure all games have clear community guidelines on what behaviour is and is not acceptable. Promote and enforce these guidelines by actively managing potentially toxic environments and inappropriate behaviour during in-game communication and on streaming services. This includes provision of monitoring and flagging mechanisms, and giving prompt responses to reports from players including outcomes of investigations and ability to appeal decisions, and taking action against players who do not respect the rules.

• Make information about community guidelines, privacy policies, and terms and condi-tions easily accessible and visible to all age group users.

• Provide information to parents to help them be more in control of their child's gaming experience. Explain how the games work, how interaction in the game works, how purchases in the game work and how they can teach children about safe online behaviour and also restrict access to certain games.

• Marketing of games with in-game purchasing options should take into account that they are not consisting of any message involving any form of extremism.

Online gaming is expected to rise in the future, and along it will come problems like cybercrime, increasing addiction, and abuse. Users should equip themselves accordingly to tackle emerging risks posed by these cyber criminals worldwide. While some countries like the UK have banned misleading advertising and other countries like Japan have taken steps to control the gambling aspect of Gacha gaming, it is not enough.

Young children regularly play games not meant to be played by children their age and are exposed to indecent material. Moreover, some games ban nudity while allowing players to dismember or murder other players or NPCs violently. **Such loopholes and obvious logic flaws need in-depth research to counter**.

Governmental regulation is essential to provide a better environment for gamers. It is especially vital since gaming deals with children's activity but is being overrun by trolls, cybercriminals, racists, pedophiles, and worse. There are many steps a government must take to protect the interests of children and parents.

The rating system is one such measure. Governments globally have assigned specific ratings for gaming, depending on the gamer's age. The regulations stipulate that organizations strictly follow the rules. **Governments worldwide find it easy to ban online games. However, that is not the ideal solution to the problem. The trick lies in regulating gaming rather than having a blanket ban. Here's how governments can step in and control online gaming.**

The Licensing Regime   Approval for Apps   Provide Room for Self-Regulation

The Licensing Regime

Licensing online games is an excellent way of regulating it. Governments can make it mandatory for gaming service providers to obtain a license before offering it to subscribers. Governments can exclude games involving skill from the licensing requirement. Thus, it leaves the games that depend on chance or the luck factor. In this way, it can control online gambling, while allowing legitimate online gaming to continue.

Approval for Apps

Gamers download gaming apps from either App Store or Google PlayStore, depending on which OS they use. Governments can be strict on these online marketing resources and stipulate that they should seek prior approval of the Government before allowing the gaming app to be made available for downloading on the internet.

Provide Room for Self-Regulation

While licensing and insisting on approval for gaming apps could sound hyper-regulative, one can relax the rules a bit and allow gamers/app-downloaders to exercise their discretion before downloading any gaming app. It provides room for self-regulation. However, cynics can argue that it would not serve any purpose because self-regulation depends on the specific individual.

We hereby also propose that if further actions as such the underlined below can be considered by the Governments as a regulatory protocol in controlling illegal or undesirable actions for the online gaming communities.

- Ensure that the data collected from gamers in a particular country is stored in servers located in the same region and not shared elsewhere.

- Assign ratings for online games, depending on the gamer's age.

- Ban games that can prove addictive or do not subscribe to Governmental guidelines. India has already banned games like PUBG, not because they are addictive but because they violated Government regulations regarding maintaining player data confidentiality.

- Regulate gambling sites and ensure there is no monopoly of a specific company/entity.

- Enforce gaming laws and impose disciplinary sanctions for violations. It should include fines and penalties, leading to complete bans.

- Grant licenses for participating in gaming operations.

- Ban misleading ads, and provide larger gambling warnings on games with a Gacha system.

- Maintain effective controls over the financial records of Registered Gaming Compa-nies, including establishment of stringent checks on the procedures for internal fiscal affairs and the safeguarding of assets and revenues.

- Create special Legal-Tech teams similar to nature of special Task Force with Cyber-law Division of Governments who would be liable on ensuring that periodic reports with gaming companies are filed.

- Maintain strict compliance with various laws, regulations and required minimum internal controls pertaining to new games being launched in the market.

- Enforce gaming laws and impose disciplinary sanctions for violations, including fines and penalties for users as well as gaming companies.

- Review the character and fitness of participants in gaming operations and make determinations regarding their suitability or qualification for licensure

It can be concluded that while those online games, just like social media accounts have both merits and demerits, however it has become crucial as breathing space in the process of globalisation. Whether the economic costs of these games are expensive for many customers or are purchasable at zero or with minimal costing, the initiative of cloud computing has bestowed individuals to break down this impediment, giving anybody with a secure internet network access to gaming.

With this comes, the concern towards maintaining a regulated online gaming industry. The series of problems existing on the current stage of online games, leading to malicious tampering of virtual data, account theft, server maintenance, etc., are not seemingly unsolvable easily. Therein, preventive counter walls by parents, academic educations, online game industry and the state are thus seen as proactive antidots in protecting children, adolescents and adults.

We at CyberPeace believes that Government mandates and legal regulations are one of the significant strategies of controlling online gaming, however it should not be a case of excessive regulation where serious gamers would find it impossible to download and play online games. As the prevention chain revolves, it is utmost important to realise safeguarding principles to be implemented and followed by the game industry- whether it is the game developers, publishers alongwith marketing teams, etc needs to take seriously into concern the wellbeing of its clients or end users.

But what is most significant among all the guidelines or any other attempt of safeguarding policy is – **SELF AWARENESS OF ONLINE ACTIVITIES**. Our foremost task here, as CyberPeace Foundation, hence is to put across sound guidance for all age-groups to have a safer experience of online gaming through the present piece.

1. India TV. CyberPeace Foundation Report View. Cybercriminals using online gaming to tar-get kids. https://www.indiatvnews.com/technology/news-cybercriminals-using-online-gaming-to-target-kids-694878

2. LeVar Battle. Online Gaming Risks and Kids: What to Know and How to Protect Them. Webroot. October 10, 2019. https://www.webroot.com/blog/2019/10/10/online-gaming-risks-and-kids-what-to-know-and-how-to-protect-them/

3. Associated Press. California man sentenced to twenty years in fatal 'swatting.' Los Angeles Times. March 29, 2019. https://www.latimes.com/nation/la-na-tyler-barriss-swatting-sentencing-20190329-story.html

4. Internet Safety 101. https://internetsafety101.org/onlinegaming

5. Branka Vuleta. Thirty-nine worrying cybercrime statistics (Updated for 2020). Legal Job Site, February 13, 2020. https://legaljobsite.net/cyber-crime-statistics/

6. Online Gaming – The Risks. https://www.internetmatters.org/resources/online-gaming-advice/online-gaming-the-risks/#strangers

7. GoldPhish. Online Gaming and Cybercrime – You playing or being played? Goldfish Cyberse-curity Awareness. February 11, 2020. https://www.goldphish.com/post/online-gaming-and-cyber-crime-are-you-playing-or-being-played

8. Nicholas Pugliese, Trenton Bureau. NJ police officer among 24 arrested on charges of luring underage children for sex. NorthJersey.com September 18, 2018. https://www.northjersey.com/story/news/new-jersey/2018/09/18/nj-police-officer-among-24-arrested-child-luring-sting/1346054002/

9. Deepankar Sharda. Tribune News Service. Punjab teenager spends Rs 16 lakh on PUBG. The Tribune. July 02, 2020. https://www.tribuneindia.com/news/chandigarh/teenager-spends-rs16-lakh-on-pubg-107717

10. Safe gaming – how gamers can protect themselves and their PCs when playing online. October 06, 2017. https://www.eset.com/au/about/newsroom/press-releases1/eset-blog/safe-gaming-how-gamers-can-protect-themselves-and-their-pcs-while-playing-online/

11. Gaming Regulatory Overview. Exhibit 99.3. https://www.sec.gov/Archives/edgar/data/858339/000119312512115625/d268435dex993.htm

12. Game age ratings explained. Internet matters. https://www.internetmatters.org/resources/video-games-age-ratings-explained/

13. Gaming Market – Growth, Trends, Forecasts (2020 – 2025) https://www.mordorintelligence.com/industry-reports/global-games-market

14. Is Video Game Addiction Real? WebMD https://www.webmd.com/mental-health/addiction/video-game-addiction#1

15. Online Gaming: Regulate, Don't Ban, Experts Sat. Bloomberg, Quint. https://www.bloombergquint.com/law-and-policy/online-gaming-regulate-dont-ban-experts-say

16. Business Standards. Online gaming industry to worth Rs 29,000 crore by FY25, says KPMG. https://www.business-standard.com/article/economy-policy/online-gaming-industry-to-worth-rs-29-000-crore-by-fy25-says-kpmg-121061700714_1.html

17. Roland Landers. How technological advancement can be a game-changer for the online gaming industry. https://yourstory.com/2021/05/technological-advancement-game-changer-online-gaming-industry/amp

18. Rachel Kowert. Et. al. The Relationship Between Online Video Game Involvement and Gaming-Related Friendships Among Emotionally Sensitive Individuals. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4080869/

19. Childnet International. Online Gaming: An introduction for parents and carers. https://www.childnet.com/u-files/online-gaming.pdf

20. Eric J. Hayes. Playing it Safe: Avoiding Online Gaming Risks. https://us-cert.cisa.gov/sites/default/files/publications/gaming.pdf

21. Otelco. Online Gaming Security: Don't Ignore the Risks – 13 Tips to Safety. https://www.otelco.com/online-gaming-security/

22. Guidelines regulating Online Gaming in India. https://www.helplinelaw.com/business-law/GROG/guidelines-regulating-online-gaming-in-india.html

23. Gaming and Regulatory Overview. https://www.sec.gov/Archives/edgar/-data/858339/000119312512115625/d268435dex993.htm

24. India Today. 13-year-old spends Rs 40,000 on online game, hangs self after mother scolds him. https://www.indiatoday.in/cities/story/13-year-old-suicide-spent-rs-40000-on-online-game-1835056-2021-07-31

25. Katie Jones. Visual Capitalist. Online Gaming: The Rise of a Multi-Billion Dollar Industry. https://www.visual-capitalist.com/online-gaming-the-rise-of-a-multi-billion-dollar-industry/

26. Childnet International. Online Grooming. https://www.childnet.com/parents-and-carers/hot-topics/online-grooming

27. Discussion Paper Series Child Rights and Business in a Digital World: Child Rights and Online Gaming Opportunities and Challenges for Children and the Industry. https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf

28. 5 Benefits of Serious Games and Simulations. https://www.designingdigitally.com/blog/2017/09/5-benefits-serious-games-and-simulations

29. 15 Surprising Benefits of Playing Video Games. https://www.mentalfloss.com/article/65008/15-surprising-benefits-playing-video-games

30. Caralee Adams. Cyberbullying: What Teachers and Schools Can Do. https://www.scholastic.com/teachers/articles/teaching-content/cyberbullying-what-teachers-and-schools-can-do/

31. Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center. https://rems.ed.gov/docs/Cyber_Safety_K-12_Fact_Sheet_508C.pdf

32. Dr. Lauren Hayes. How to Promote Digital Citizenship in the School Library. https://ideas.demco.com/blog/how-to-promote-digital-citizenship-in-the-school-library/

CyberPeace
Foundation

www.cyberpeace.org | secretariat@cyberpeace.net

/cyberpeacefoundation   /cyberpeacengo   /cyberpeacefoundation