The Role Of Consent In Protecting Children's Personal Data In Online Games: Evaluating The Effectiveness Of Consent Mechanisms

Manvee[1] & Mukund Ranjan[2]

Abstract

With the increasing availability of smartphones and tablets, the gaming business has grown rapidly along with the proliferation of gadgets. The gaming industry generated over $200 billion in revenue globally in 2023, with mobile gaming emerging as the leading segment. This increase is explained by the ease of use and low cost of mobile devices, which have made gaming possible for an estimated 2.7 billion people globally, most of whom use mobile platforms. The democratization of online gaming has resulted in a transformation of the business and the emergence of a new gaming culture. The affordable and speedy internet connectivity and the accessibility of mobile devices have facilitated this. According to UNICEF, this change has completely changed how players interact, discuss, buy, and play digital games. Online gaming is defined as playing commercial digital games via internet-connected devices. However, worries over the security of children's personal information have been highlighted by this increased accessibility. Given that a large percentage of players are young people, parents who frequently give their kids' gaming gadgets run the risk of being harmed by gaming businesses' data extraction practices. Thus, it becomes essential to put in place parental control methods to protect the privacy of parents' and children's data.

In this paper, we have explored the complexities of parental consent with regard to children's personal information in online gaming in this article. Further, we have examined the efficacy and ramifications of the current consent procedures. Furthermore, we have done a comparative study of international legislative standards pertaining to data privacy in online gambling, concentrating on India. In the end, this paper highlights the significance of parental participation in guaranteeing the confidentiality and safety of kids' personal information, offering valuable perspectives for legislators, gaming corporations, and guardians alike.

Keywords

Consent, Children's Data, Consent Mechanism, Parental Consent, Online Gaming

[1] University Affiliation: Chanakya National Law University, Patna
[2] National University of Study and Research in Law
✉ Manvee (manvee.nlu.patna@gmail.com) & Mukund Ranjan (mukund.ranjan@nusrlranchi.ac.in)

1. Introduction

The gaming industry has become an ever-growing industry since the advent of gadgets publicly. In 2023, the video gaming industry approximately generated a revenue of around 200 billion USD worldwide. These numbers include the sales of physical video games and home consoles, but the largest of them is mobile gaming. The estimates suggest that there are around 2.7 billion gamers worldwide, out of which 2.6 billion gamers play on mobile devices such as smartphones and tablets.[3] Mobile gaming devices are famous as they allow gamers to play without using expensive gaming consoles or personal computers. This is because it has become popular among children.[4] Further, the availability of fast and cheap internet in remote locations and affordable mobile devices are other reasons for the rise of the online gaming industry.

This increased accessibility has "revolutionized the industry and opened doors to a new generation of gamers – changing the way they communicate and interact with other gamers and as spectators, how they buy and play games, and how the games they play interact with other digital services"[5] the same has been outlined by the UNICEF. This report also defines online gaming as "playing any type of single- or multiplayer commercial digital game via any Internet-connected device, including dedicated consoles, desktop computers, laptops, tablets, and mobile phones." Children, being the major focus in the industry of online gaming, are increasingly adopting digital devices that have smoothly become an integral part of their everyday lives.

However, this access to online games has posed significant problems in protecting the personal data of children. The engagement of so many children in online games makes it easier for companies to extract data from children. In most cases, the children do not have their smartphones or tablets rather they use their parent's smartphones or tablets and thereby, it imposes a threat to their parent's data which are extracted by these online gaming companies.

[3] Oehlenschlager (2021).
[4] Russell et al. (2018).
[5] UNICEF (2019).

Therefore, it becomes necessary to obtain consent from the parents when children log on to any online games. This consent mechanism will help in protecting not only the children's data but their parents' data as well.

Herein, in the present paper, we will discuss consent in the context of Children's personal data in online games and the role of parents in providing such consent to protect the data. Further, we will analyze the consent mechanisms already in place and we will find out the implications of such consent mechanisms. In the end, we will analyze out the legal regulations globally and compare that with India and we will conclude by suggesting the appropriate mechanism for our country to protect children's data.

1.1. Developing A Jurisprudence For A Consent-Based Framework In Online Gaming For Children

1.1.1. Safeguarding Children from Harassment in Esports

Davis vs Monroe County Board of Education[6] is one of the landmark cases which laid down a roadmap for dealing with sexual harassment. In this case, the U.S. Supreme Court addresses whether a school board can be held liable under Title IX of the Education Amendments of 1972 for indifference to student-on-student sexual harassment deliberately. In this case, a 5th-grade student 'LaShonda' was sexually harassed by her classmate for several months which included vulgar comments, attempts to touch her physically, and sexually aggressive behavior. Despite the repeated complaints by the victim and her mother to the teachers of the school, the superintendent, and the principal, no meaningful disciplinary action was taken. The school failed to separate the students and it also lacked a policy to address sexual harassment. The sexual harassment caused a decline in the victim's grades and badly affected her mental health which eventually led to a suicide note. The Supreme Court reversed the holding of the Eleventh Circuit and held that[7] Title IX damage claim could be sustained when it is found that the school acted

[6] *Davis v. Monroe County Bd. Of Ed.*, 526 U.S. 629 (1999).
[7] Manke (2000).

with deliberate indifference to harassment which was so severe, offensive, and pervasive that it denied the victim all the access to educational benefits. The court also clarified that the liability is limited to the situations where the school has sustained substantial control over the harasser as well as the environment in which the harassment occurs, the court emphasized the fact that liability requires actual knowledge and deliberate indifference.

Vice President[8] Joe Biden back in 2010 strengthened the Title IX policy by aligning the principles established in *Davis vs Monroe County Board of Education*. The administration updated the guidance via a 'Dear Colleague' Letter which reinforces this by rejecting inadequate compliance methods like solely relying on surveys to assess interest in athletics and advocating for comprehensive procedures to address discrimination. Thus, by ensuring robust evaluations and responses, these updates aim to prevent the systemic neglect seen in *Davis's* case, safeguarding the educational rights Title IX was designed to protect.

It can be inferred from this case that gaming entities need to establish clear boundaries and potential consequences for the misconduct related to the children in the esports and online gaming setup, hence here getting informed consent from children which includes a verifiable parental consent becomes crucial before collection of the data. A robust consent mechanism will ensure that the child understands what data they are giving up and how it can be used.

1.1.2. Real Instances of Virtual Harassment

1.1.2.1. Nina Jane Patel Virtual Harassment in Metaverse

The case of Nina Jane[9] Patel raised alarming concerns over virtual harassment in the metaverse, Nina designed her avatar a cartoon-like version of herself and entered the Meta's Horizon venue using a VR headset. Within less than a minute her avatar was gang

[8] The White House, Office of the Vice President (2010).
[9] Patel (2021).

raped virtually, the 3-4 men groped her, touched her, and eventually she froze there. She says *"It happened so fast and before I could even think about putting the safety barrier in place,"* and when she tried to get away from there the men yelled *"Don't pretend you didn't love it"* and *"Go rub yourself off to the photo".* After this incident, Meta added a 'Personal Boundary' feature that creates a 4-foot invisible[10] bubble around the avatars in the Horizon Worlds. Now people can use it to block everyone or even just strangers from getting too close. They can also disable it as per their wish and needs. The personal Boundary bubble is a strong example of how VR has the potential to engage and interact with people comfortably.

This incident has however raised ethical and moral concerns for the developers in addressing the virtual sexual harassment and online misconduct. This was the first of its kind incident that was under police scrutiny and investigation in the UK highlighting the psychological trauma victims can experience in such an environment. This blurs the line between real-life assault and virtual assault, especially for children who often struggle to distinguish between the two

1.1.2.2. British Teenage Rape Case in Metaverse (2024)

A case came up before the British police in January 2024 where a 16-year-old teenager was attacked in the VR gameplay model. The girl has been left traumatized[11] after her avatar; her digital character was gang raped by online strangers. However, she didn't suffer any physical harm as there was no physical attack. But the officers stated that she is suffering psychological and emotional trauma as someone who has been raped in the real world as the 'VR' experience is designed to be completely immersive.

For addressing virtual harassment, personal bubble concepts[12] can help as VR developers can immersive VR applications, like *TooCloseVR*, to address cyberbullying through personal space invasion (PSI) simulations. such applications should incorporate phases

[10] Hoover (2022).
[11] Cluley (2024)
[12] Wienrich (2024).

of engagement: setup for familiarization, conflict to simulate personal space invasions using impactful elements like mean text phrases, large non-removable message boxes, sound effects, and abstract profile pictures within a 0.5-meter proximity, and resolution for reflection and decision-making. This structured approach enables users to experience and reflect on cyberbullying scenarios, fostering empathy and equipping them with actionable strategies as victims or bystanders.

1.2. Gender Representation in Esports

Historically the gaming industry has depicted women mostly as victims of any of the objectified roles such as in the *GTA* series or in *Max Payne.* However, this has changed with time significantly and now female characters are making a significant impact on the industry as one of the leading icons in the game. This has made a significant departure from the earlier depictions that often reduced the women's roles in the games as mere objects of desire or characters who only required rescue in the game. Notable examples include Princess Zelda from[13] *The Legend of Zelda* who constantly portrays herself as a powerful and selfless ruler by her incarnations, she defends her people against the evil forces, particularly in Breath of Wild where her powers alone keep Ganon at Bay. In *The Last of Us,* Ellie emerges as the resourceful survivor navigating the zombie apocalypse, growing from a fearless 14-year-old teenager to a powerful adult in the sequel. She explores the themes of resilience and identity. Faith Connors from *Mirror's Edge*, an Asian-descended parkour expert, rebels against a dystopian regime using agility, strength, and resilience, showcasing the power of resistance and revenge in the face of personal loss. Hence their characters are redefining representation in gaming thereby offering complex and diverse role models who inspire within the virtual worlds and in real life.

1.3. Critical Review of IESF Articles 5 and 7

Article 5[14] of the International Esports Federation (IESF) Regulations demonstrates a commitment to players' mental and physical health highlighting the importance of stress management and mental well-being. However, it lacks clarity as to what would constitute harassment, particularly in the unique contexts of online gaming and esports such as hate

[13] Almeida (2019).
[14] World ESports IESF (n.d.).

speech, cyberbullying, and targeted trolling. Article 7 provides for Conflict resolution and Reporting violations in Esports and Online Gaming; however, it doesn't elaborate on the reporting process like does the reporting mechanism has to be anonymous, or whether are there any safeguards to protect reporters from retaliation, this could make the potential whistleblowers hesitant to report the incidents thereby undermining the effectiveness of the provisions. Article 7 lists down potential disciplinary actions but doesn't outline the criteria for determining the severity of offenses and this ambiguity may lead to inconsistency enforcement and perceptions of bias.

2. Understanding Consent In The Context Of Children's Personal Data

Data processing by companies leads to a lot of money and at the same time brings threats to the people whose data is processed. However, processing personal data is usually prohibited under the laws, unless expressly allowed.[15] Consent is one of the bases by way of which processing the personal data of individuals may be allowed. The conditions of valid and effective consent are provided under Article 7 of the General Data Protection Regulation and further specified in Recital 32 of the same. Consent must be freely given, specific, informed, and unambiguous. In order to obtain freely given consent, it must be given on a voluntary basis. The term "free" signifies that the data subject must have a real, genuine, and unrestricted choice. If any form of undue pressure or influence is present, impacting the decision-making process, the consent becomes void.

Online gaming enables children to participate in shared activities, promoting collaboration and the development of essential learning skills like strategizing and problem-solving. However, it's crucial to strike a balance between these potential benefits and the inherent risks that come with children engaging in online gaming. Game developers and marketers catering to children must be aware of the potential impact on children's rights and should establish policies and procedures that prioritize supporting and respecting those rights.[16] Herein, one of the key areas for consideration is the consent

[15] General Data Protection Regulation, art. 6(1).
[16] UNICEF (2019).

of both the children and their parents and the collection of the personal data of children. Online gaming platforms may get away with these things stating that the consent which was given was free, specific, informed, and unambiguous. However, the reality has so much to do with it. Usually, the 'Agree' or 'Accept' button is highlighted so that children press those buttons and they have no information about the consent they are giving about their personal data.

Furthermore, any person under the age of 18 is a child unless otherwise stated under the law applicable to the child.[17] UNICEF recommends companies to provide special consideration and protection to every child in line with international norms and standards, regardless of any regulatory regimes. This is because of two reasons,

(i) there may not be regulatory regimes in place in every jurisdiction, and

(ii) the guidelines concerning the online gaming industry mandates it.

When it comes to the collection, sharing, or reselling of the personal information of children, these activities must not be undertaken unless specific and valid consent has been obtained.[18] The companies must also consider the fact that the present age verification process may be ineffective and the games which are targeted to adults may be played by the children. At this juncture, the companies must consider the implications of the rights of children who play these games and how their data is processed because of the ineffectiveness of the age verification or non-implementation of proper consent mechanisms.

UNICEF recommends[19] all gaming companies should carefully process the player data they gather and its intended purpose. Data aimed at enhancing the gaming experience is likely less detrimental than data gathered for targeted advertising or resale, which also includes personal data. To promote transparency and informed consent, companies should actively disclose the kinds of personal data they collect and its intended use, ensuring that users comprehend the implications and can provide full consent.[20] As such,

[17] Convention on the Rights of the Child (1989), art. 1.
[18] UNICEF (2020).
[19] Ibid.
[20] Ibid.

companies should provide different options for consent and not ask for consent for all the data together.[21] Obtaining meaningful consent is key to ensuring that the rights of children are protected in respect of data collection.

Under the European Union's (EU) General Data Protection Regulation (GDPR) children get special protection in relation to the collection and use of their personal data.[22] This additional layer of protection is provided as it is expected that children are less aware of their rights and the risks inherent in sharing personal data online. We can't expect children to be aware of all of these and therefore, the role of parents also arises in these circumstances. The European Commission has recommended that "any information addressed specifically to a child should be adapted to be easily accessible, using clear and plain language."[23] Further, the consent of parents/guardians is required to process the personal data of the children.

In the United States, the Children's Online Privacy Protection Rule (COPPA) is a federal law that requires the operators of websites or online services to obtain parental consent before collecting the personal data of children under the age of 13 years.[24] Thus, in the US, children under the age of 13 years cannot give their consent on their own in any manner and this law applies to all games and applications played on smartphones and tablets which are internet-enabled or can connect to the Internet. Furthermore, these laws apply to all games and applications that collect data from children in the United States or are directed to users in the United States.

In Canada, the Office of the Privacy Commissioner has released guidance[25] that specifically concerns gaming and data collection. It states that the companies must obtain meaningful consent from players if personal data is collected, used, or disclosed.[26] Nevertheless, monitoring children who engage in online gaming poses a significant challenge. Similar to other guidelines addressing children's online privacy, it is

[21] Ibid.
[22] General Data Protection Regulation (2018), recital 38.
[23] European Commission (n.d.); General Data Protection Regulation (2018), art. 8, recitals 38 and 58.
[24] Children's Online Privacy Protection Rule (1998), s. 312.2.
[25] Convention on the Rights of the Child (1989), art. 1.
[26] Office of the Privacy Commissioner of Canada (2019).

unrealistic to expect children to fully comprehend the extent of their personal data collection and usage online. Consequently, special measures must be taken to safeguard their personal information. Further, similar to the US, this guidance provides that gaming services must request parental consent for children under the age of 13 years.

Consent is very important for companies while processing or collecting personal data but the consent is not always limited to the children and it extends to the informed consent from the parents/guardians therefore, the consent holds a great significance in the context of processing of personal data of the children.

3. The Role Of Parents And Guardians In Consent Management

In this revolutionized world, mobile games and online games have become one of the most prominent forms of entertainment for children. These games can be educational at times and fun, most of the time. However, most of the games process personal data to show them Ads based on their recent search or personalize their user experience. The consent is obtained by these online gaming platforms as the children merely click on the buttons without looking at or understanding the terms. This makes the role of parents/guardians essential in consent management as the personal data might include personal data of them and not merely of the children.

Firstly, the role of parents becomes crucial as there are certain age-appropriate games but few children might log into such games even when they are not appropriate for their ages. In this regard, the role of parents is mandatory and the parents/guardians should look into the online games their children are playing and thereby, not allow their children to play the games inappropriate for their ages.

Secondly, online safety measures are often at stake when children get into playing these games. The consent management is not restricted only to giving consent to the online gaming companies but often, it goes on to the online players who interact with the children, not always with the best intentions. Those players can also take out the personal data after getting consent and process it accordingly which might be threatful.

Apart from these, there are several other roles of parents/guardians while their children engage in playing online games. One, the parents/guardians should always give informed consent about in-game purchases and set boundaries for their children. Additionally, the parents/guardians might consider setting up parental controls or password protection to prevent unauthorized purchases. However, herein we also need to analyse how parents can be a part of the consent mechanism and control the informed consent.

As per EU's GDPR, the consent of a parent or guardian is required in order to process the personal data of a child. In the EU the age threshold for requiring consent is set by each EU member state and ranges between the ages of 13 and 16 years old.

In the United States, COPPA is the law governing the processing of online data. Under the law, parental consent for the collection of personal data of children under the age of 13 years is mandatory. Further, the companies must provide direct notice to parents and obtain verifiable consent before collecting any personal data. Gaming companies are required to offer parents the choice to consent to the collection and internal usage of their child's personal data, while strictly prohibiting the disclosure of such data to third parties. If any disclosure is made, it must be transparent and clearly communicated to parents. Furthermore, parents must be granted access to their child's personal data to verify its accuracy or request its deletion. They should also have the option to prevent any further use or online collection of their child's personal data. A child's participation in online activities must not be contingent upon providing more personal data than is reasonably required for the activity in question.[27] It is clear that in order to ensure compliance with the requirements set out under COPPA, covered companies must employ thorough data security, retention, and destruction practices.

In Canada too, consent from the parents/guardians is necessary for the collection of personal data of children under the age of 13 years. Additionally, parents and guardians should be able to control their child's access to content, ability to chat with other account

[27] Federal Trade Commission (2020).

holders, and how personal data will be shared.[28] In relation to the retention of personal data for inactive accounts, companies must apply an appropriate retention schedule for inactive accounts as this data should be destroyed after a defined period of inactivity.[29] Companies must also provide a "true deletion" option that allows users to request that their accounts be entirely deleted.[30]

These discussions make it clear that the role of the parents/guardians is not limited to them giving consent for collection of the personal data of children in games but is much more than that and therefore, it is an important aspect in the context of consent management. Further, we need to strengthen the effectiveness of parental consent as this is not verifiable most of the time.

4. Challenges-Limitations With Consent Mechanisms & Proposed Solutions

When it comes to obtaining consent from children while they are playing the game it possesses a certain set of challenges followed by the limitations for the same. Some of the prominent challenges related to the Data Protection and privacy of children in Online Gaming include Age Verification, Complex Privacy Policies, Manipulative and Persuasive Design of the Game, Data Sharing with third parties & Informed Consent.

4.1. Age – Verification Manipulation GE-Verification Manipulation

While we can agree upon the fact that, verifying the age of the users in Online Games especially children can be extremely challenging. During the account registration process, many online games rely on self-reported age while providing[31] access to their users. However, for all the users this self-reported age cannot be accurate, children often dupe while feeding their age in the verification process. Since the users including the children easily manipulate their age during the account creation, it renders the verification process

[28] Office of the Privacy Commissioner of Canada (2019).
[29] Office of the Privacy Commissioner of Canada (2015).
[30] Ibid.
[31] Future of Privacy Forum (2021).

ineffective. This manipulation in the age verification process raises doubts about the efficacy of age-based restrictions and the integrity of consent obtained by the gaming company to process the data of its users.

4.1.1. Solution

While children can manipulate their age easily during the age verification process, some of the proposed solutions the companies can implement to tackle this issue is by having a Multi-layered Verification approach where these companies instead of relying solely on a self-reported age, can involve a combination of methods such as 'Age-verification check' by partnering with third-party services that verify user age against the publicly available database with parental consent or by using the credit/debit card information of the parent for allowing the consent. Companies can also partner with companies providing AI-based-age verification by scanning the face to ensure control, where the children will be required to scan their face by the camera and the tool will tell the age of the child. Video Game companies can also offer 'Parental Control Tools' where they will offer robust control features that will allow parents to manage their children's sign-in activities, in-app purchases, content filtering, and even playtime restrictions. Game developers while designing the game can focus on developing the UI-UX of the game in 'Age-Appropriation Content Tiers' where children will be allowed age-restricted features and content only after a successful age verification.

4.2. Complex Privacy Policies

Terms of Service and Privacy Policies[32] are usually the most important and compulsory documents for governing the data collection of users. However, the challenge about it is its complexity. The use of legal jargon and terminologies usually confuses most of the users and children are no exception to it. Children usually struggle to interpret[33] and comprehend the implications of giving consent to the data collection and its usage in the privacy policy. Not only children but their parents too due to the complexity of the jargon

[32] The Danish Society of Engineers (2021).
[33] Denham CBE and Wood (2022).

used often find difficulty in making an informed decision about data sharing. The use of technical and intricate legal language can complicate the true implications of Data sharing leading to uninformed consent of the user. The only way to tackle[34] the problem of uninformed consent is for the privacy policies shall be simplified and presented in such a manner that any average user can comprehend it.

4.2.1. Solution

We often see, that all the gaming websites and apps most of the time have a complex and technical privacy policy due to which the children are unable to interpret what kind of data is being collected and processed by the company and what purpose this collection of data will serve. So, these companies to reduce the complexities in these privacy policies can use simple and plain English in writing their privacy policies which an average user can understand easily. Technical Terms and Legal jargon should be avoided in the policies. Gaming companies can also incorporate visuals like short explainer notices, and infographics where the user can simply click and know about the specific aspects of the policy and data being collected to give informed consent. All the user-centric benefits should be explained in a clear and visible manner like why the game collects specific data and how it benefits the user experience (such as security features, and personalization). The companies should also outline the easy navigation of user control options related to data collection and usage. It should also be ensured that privacy policies are not hidden and are not on hard-to-find locations.

4.3. Manipulative & Persuasive Design

To collect the data of children and use them for target advertising purposes, game developers usually use manipulative and persuasive designing methods in the game. The use of persuasive designing techniques encourages the users as well as children to spend more time in the game and provide more data. Manipulative techniques[35] included but were not limited to addictive features such as music and sound notes in the game that aim

[34] Ibid.
[35] Chung (2023).

to de-sensitize the child to its immediate physical environment, loot box after viewing the ads, or use of enticing rewards which makes it challenging for the users to exit the game. Children are completely unaware of the fact that the data they are giving consent[36] for is used for what purposes. Hence, data collection and its use are opaque to children, and it can have implications for the digital service's ability to persuade children to stay longer in the gaming universe. Critiques believe that this manipulation of users in the game by the use of persuasive design tactics has sparked ethical concerns. It is contented that game developers prioritize profits over user welfare, employing strategies that encourage excessive data capturing by engaging the user for a long time in the game.

4.3.1. Solution

The problem of manipulative design can be curbed by clearly disclosing how the game makes money like, in-app purchases, and in-app advertising. Gaming companies should avoid deceptive practices like disguised ads or unclear pricing for virtual goods. They should design the core gameplay loop to be rewarding and engaging without relying on manipulative tactics. Their core focus should be on creating a fun and balanced experience that respects the player's time. They should provide opt-in choices for users to collect the data and an explanation should be provided for how the data is used and how users can opt out of their data collection. To promote the well-being of the players game developers should implement features such as 'Time Management Tools' which will help players track their playtime and set healthy limits. They should also consider features like notifications or gentle nudges to encourage breaks after a set interval. In the time management tool. Parents should be provided with robust parental control features that will allow them to manage in-game spending, playtime, and access to specific features of the game. The company should also regularly go for independent audits of the game design practices to ensure ethical data collection and responsible monetization strategy for the game.

[36] Lieber (2018).

4.4. DATA Sharing With The 3rd Parties

While anyone is playing an online game, a certain set of data is being collected by the companies such as, "In-Game Data[37]", "Real-World Data[38]" and "Sensitive Personal Data[39]". 'In-game data' is collected where the child is playing and represented by his in-game choices such as his conduct during the game, his avatar, the costume of the avatar, and the inter-player interactions. This data once compiled and analysed can contribute to the creation of a detailed profile of the user. 'Real-world data' is collected when the social media accounts of the player are linked to the gaming account. Here data such as cookies or the location of the player exploiting the GPS or IP may be processed. These data are often used to enhance the player's experience and service itself for profiling children and contribute to behavioural advertising. 'Sensitive Personal Data' relates to data on physical & mental health, sexual orientation, gender, etc. This type of data can be extracted by inter-player interaction during the game via voice chat, video camera, or in-game calls or by in-game chatting. These interactions are stored by the gaming companies undoubtedly. The gaming platforms[40] can come into possession of sensitive personal data of children by profiling them based on their in-game choices and behaviour. These data collected by gaming companies[41] often share with third parties for advertising, as a part of a merger, or if the company is being acquired. This raises an alarming issue of data security and its misuse. Stricter norms and regulations are needed to ensure children's data is not being compromised and exploited for the commercial gains of the company without explicit and well-informed consent.

4.4.1. Solution

The challenge of Data Sharing with 3rd parties can be tackled by these gaming entities via 'Clear Disclosures' of what kinds of data being collected via means of short privacy notices, the notices should also mention of how this data is used and with whom this data

[37] Enescu (2020).
[38] Ibid.
[39] Federal Trade Commission (2020).
[40] Information Commissioner's Office (2023).
[41] Faraz et al. (2022).

is being shared. The language of the notices should be simple and understandable by the users and parents. The entities should also give their users a granular control over the data which will include options to opt-out of data collection entirely and choosing what kind of data is shared with the third parties and allowing the users to manage how their data is used for advertisings and other purposes. The entities can also use 'Data minimization' strategies where they are only collecting the data which is necessary for the core functionalities of the gameplay and they should avoid collecting unnecessary data especially sensitive personal data. As a part of 'Data Minimization' techniques 'encrypting the data' can be used as a practise to protect the user data at rest as well as in transit. The entities should also regularly conduct 'Data Security Audits' to keep a check on the threats and vulnerabilities of data storage and transmission.

4.5. Advertisements

The validity of the consent is determined by the informed and free consent given. Children are usually unable to understand the extent of data collection, the risks involved, and how their data is being processed and used by sharing it with third parties for advertisement purposes. Children are soft targets of advertisers[42] as they are the most vulnerable group of advertisements. Children's critical thinking abilities are immature and can't be compared with adults to control their impulses. As per a survey, it has been found that school-aged children and teenagers may be able to recognize advertising but are unable to resist it when it is embedded within trusted social networks encouraged by social media or celebrity influencers, or delivered next to personalized content. Some games encourage children to share their progress on their social media handles in the form of pop-ups and buttons in return for a reward of coins in the game to proceed further. In a popular game 'Talking Tom' the gift[43] looked as if it was a part of the game but when tapped on it, the player was asked to watch videos and win coins in the game. Furthermore, some games are filled with pop-up ads which interrupt the gameplay usually and the cancel button is hardly visible to the player. Recently it has been reported[44] that *a 10-year-old girl spend more than £2,500 on the gaming site Robolox after she changed*

[42] UNICEF (2019).
[43] My Talking Tom Friends (n.d.).
[44] Bird (2023).

the password on her family's iPad tablet without the consent of her mother. It was found that uninformed consent and advertising in the game played a major role in the game for this child to make in-game purchases without the consent of her parents.

Therefore, getting and managing consent for children's data in online games requires addressing challenges related to age verification, tackling complex privacy policy, in-game advertising, manipulative design of the game, and lastly what kind of data is being shared with the third party. Balancing these considerations is essential to protect children's privacy rights in the context of online gaming.

4.5.1. Solution

The issue of Target Advertising on children's can be tackled in the following manners: The Gaming entities should implement a stricter age verification process which will ensure that advertising only reach to the late teenagers (16-17 years of age group). These entities should also regularly conduct independent audits of their game design practices to identify and address the manipulative advertising tactics (if any). The gaming entities should also make a clear demarcation between advertisements and in-game contents as ads would be visually distinct and not disguised as a part of the game. Moreover, if advertising must exist then it should be limited to contextual advertising relevant to game's content and not based on the player data.

5. Legal And Regulatory Implications Of The Consent Mechanisms

The Legal frameworks[45] and norms governing consent mechanisms[46] for the protection of children's personal data in online gaming vary from jurisdiction to jurisdiction. It reflects the evolving jurisprudence of data protection and the set of challenges posed by online gaming. The key aspects of these frameworks include Age of Consent, Parental Consent Mechanism, Operator Responsibilities, and Enforcement-Penalty mechanisms. We shall be discussing all these key mechanisms in depth.

[45] Information Commissioners Office (2018).

[46] Hunton & Williams LLP Centre for Information Policy Leadership (2018).

5.1. Age of Consent

Each jurisdiction has a different set criterion for age limit. According to EU-GDPR (General Data Protection Regulations)[47] has set criteria of an age limit of 13 to 16 depending upon the member states for giving consent. This is being followed across all industries including Online Gaming. Whereas in America, the Children Online Privacy Protection Act (COPPA) requires verifiable parental consent for children under the age of 13 years. If we talk about China[48], has enacted a *'Provision for Cyberprotection of the Personal Information of Children (PCPPIC)[49]'*. As per this act, any person under 14 years of age will be considered minor and entitled to protection. To curb gaming & gambling addiction among minors' mandatory registration under a real name was introduced in popular games in China. PCPPIC applies a ban on persons under the age of 18 playing between 10:00 PM to 8:00 AM[50]. If we look at Indian Jurisdiction then the *Digital Personal Data Protection Act 2023 ("DPDPA")* has provided for the definition of 'children' as anyone who is less than 18 years[51] of the age and has to obtain a parental consent every time they share their data with any of the data fiduciaries or the processors and this is also applicable for the gaming entities operating in the Indian jurisdiction.

5.2. Parental Consent Mechanism

Legislation like COPPA[52] focuses on obtaining parental consent before collecting the personal data of the children. COPPA ensures that parents know what information is being shared and with whom. The company must get parents' verifiable consent before collecting, using, or disclosing personal information from their kids. The operator must choose a viable method to ensure the person giving consent is the child's guardian or parent. If we look at South Korea's position[53] then the consent requirement there is the strictest globally. South Korea has mandated that operators obtain parental consent before

[47] Public Consultation Paper (2019).
[48] Smyr and Ulianova (2022).
[49] Provisions on the Cyber Protection of Children's Personal Information (2019).
[50] Zialcita (2019).
[51] Manvee (2024).
[52] Discussion Draft (2021).

[53] Ibid.

collecting the personal data of users under 14. Amendments in privacy laws in South Korea, specify methods through which operators can obtain written parental consent. Parents can opt to consent via

(i) payment,

(ii) text,

(iii) information, or

(iv) authentication via smartphones.

Post obtaining consent the operators are required to send written confirmation to the parents through the abovementioned methods. If we talk about the position in China[54], as per its statutory enactment operators must also get explicit parental consent before collecting data from children aged 14 years and older. Not only this, but it also prohibits children under 16 to live broadcasting on their accounts. Also, it requires parental consent when children aged 16 years and older open live broadcasting accounts and imposes a "unified electronic identity authentication system" for online gaming. If we look at position of India then the DPDPA mandates for everyone who is less than 18 years of the age[55] to obtain verifiable parental consent with respect to giving consent for processing of their personal data during the gameplays or to any other process for data collection by the gaming entities.

5.3. Operator Responsibilities

European Union's GDPR[56], compels gaming companies to provide transparent privacy policies and terms of services which should be simple to understand the users. The privacy policy shall explicitly mention detailed data collection practices, especially those involving children. This empowers parents and guardians to make an informed decision with respect to children's online engagement. In America as per COPPA, use persistent identifiers such as user IDs[57] stored in cookies while playing the games. These identifiers enhance the users' game experience, allowing customized account settings and

[54] China (2023).
[55] My Talking Tom Friends (n.d.).
[56] Ibid.
[57] Enescu (2020).

maintenance of in-game achievements. COPPA restricts[58] the operators to disclose these persistent identities to any third party or any advertising network to deliver target advertisements or create a detailed user profile.

5.4. Enforcement and Penalties

In USA regulatory bodies like Federal Trade Commission (FTC) and in the UK, The Information Commissioner's Office enforces compliance via penalties and investigations if there is any company or entity found indulged in data malpractice. Recently FTC in June 2023 imposed a penalty of $20 million on Microsoft. As Microsoft[59] was found violating COPPA by collecting the personal information of children who signed up for the Xbox gaming system. Microsoft without notifying the parents of the children and without obtaining the consent of parents illegally obtained the data and retained the personal information of the children. In December 2022, FTC imposed a $520 million fine on Epic Games[60] as it tricked kids intentionally to make in-game purchases through the manipulative design of its game Fortnight.

Thus, the legal frameworks and regulations governing consent for children's personal data in Online gaming reflect an interplay of complex regulations and national and regional considerations. Recent developments in laws globally give a clear indication of that growing focus on children's data protection with enforcement actions setting precedents for upcoming generations.

6. Conclusion

In this paper, we have dealt in depth with the intricacies of the consent mechanism for protecting children's personal data in the context of online gaming. As the gaming industry continues its rapid expansion with internet penetration and access to 5G technology in the smartphone market the significance of safeguarding children's data becomes a serious concern to ponder. Our analysis revealed the key considerations and

[58] Ibid.
[59] Federal Trade Commission Protecting America's Consumers (2023).

[60] Morrison (2022).

challenges in the consent mechanism, ranging from complex privacy policies, and age verification to manipulative designs and data sharing.

Parents and guardians play an important role in consent mechanisms. Parents and guardians must actively engage in supervising their children's online activities, discerning age-appropriate games, and ensuring that their consent is aligned with the data protection norms. International Legal frameworks for Data privacy like GDPR, and COPPA emphasize more on parental consent as a foundation for processing children's personal data, it also strikes a balance between children's digital engagement and their privacy rights.

However, if we look into Indian Context, the DPDPA[61] prompts a critical examination of consent mechanisms for children in Online Gaming. The act demands 'verifiable parental consent' for anyone under 18 years[62] of age. The act also gives a generalized definition of 'children' as anyone who is less than 18 years of age which is in detriment to most of the teenagers of the country. This can hinder young adults' internet access as there is a difference between[63] how an 11-year kid reacts and how 16 years old teenager reacts to their external environment. A standardized approach empowering the government to lower the age of minors for low-risk digital services is suggested. Also, the government should come up with guidelines on DPDPA and provide clarity on the age verification method that is essential and would emphasizes data protection principles. Moreover, Parental consent based on self-declaration and validated government documents must be streamlined to prevent inadvertent data exposure.

Lastly, robust consent mechanisms stand as a cornerstone in ensuring the protection of children's personal data in online gaming. While challenges persist, the collective determination to prioritize children's privacy rights offers a promising pathway forward. As we navigate this dynamic terrain, we must remain steadfast in our commitment to refining and enhancing consent mechanisms, ensuring that the digital realm remains a safe and enriching space for children's exploration and growth. The ever-evolving

[61] Ibid.
[62] Bird (2023).
[63] Joshi and Mohan (2023).

landscape demands continual evaluation and improvement of consent mechanisms. Striking the right balance between fostering a positive gaming experience for children and safeguarding their privacy necessitates a collaborative effort from regulators, industry stakeholders, and parents alike.

References

Almeida J (2019) Women in gaming and how their characters have evolved, The Hindu. https://www.thehindu.com/sci-tech/technology/women-in-gaming-pixelled-paragons/article26507581.ece.

Bird N (2023) 'Roblox: Ten-year-old spent £2,500 of mum's money without her knowing', BBC. https://www.bbc.com/news/uk-wales-65659896.

Children's Online Privacy Protection Rule (1998). https://www.ecfr.gov/current/title-16/part-312

China (2023) 'Global Data Privacy & Security Handbook' BakerMcKenzie. https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/china/topics/minors.

Chung E (2023) 'Using Persuasive Design to Influence User Behavior', Medium. https://uxplanet.org/using-persuasive-design-to-influence-user-behavior-7b8f81fa7973?gi=6999d1ec5755.

Cluley G (2024) 'Sexual assault in the metaverse investigated by British police'. https://grahamcluley.com/sexual-assault-in-the-metaverse-investigated-by-british-police/.

Convention on the Rights of the Child (1989). In: OHCHR. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

Denham CBE E and Wood S (2022) 'Data protection trends in children's online gaming', International Association of Privacy Professionals. https://iapp.org/news/a/data-protection-trends-in-childrens-online-gaming/.

Discussion Draft (2021) 'THE STATE OF PLAY: Verifiable Parental Consent and COPPA'. https://fpf.org/wp-content/uploads/2021/11/FPF-The-State-of-Play-Verifiable-Parental-Consent-and-COPPA.pdf.

Discussion Paper Series: Children's Rights and Business in a Digital World (2019) 'Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry, UNICEF. https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf.

Enescu M (2020) 'Protecting Children's Personal Data in a Video Game Environment' International Journal of Science Arts and Commerce, No. 11, ISSN: 0249-5368, November 2020. http://www.ijsac.net/node/460.

European Commission, 'Can personal data about children be collected?'. https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en;

Faraz A et al. (2022) 'Child Safety and Protection in the Online Gaming Ecosystem'. https://ieeexplore.ieee.org/iel7/6287639/9668973/09933399.pdf .

Federal Trade Commission (FTC) (2020) 'Complying with COPPA: Frequently Asked Questions', Business Guidance Resources. https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

Federal Trade Commission Protecting America's Consumers (2023) 'FTC Will Require Microsoft to Pay $20 million over Charges it Illegally Collected Personal Information from Children without Their Parents' Consent'. https://www.ftc.gov/news-

events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information.

General Data Protection Regulation (GDPR) (2018). https://gdpr-info.eu/.

Hoover A (2022) ‘he metaverse has a sexual harassment problem and it's going to get worse, Morning Brew. https://www.morningbrew.com/stories/2022/06/14/metaverse-has-a-harassment-problem.

Hunton & Williams LLP Centre for Information Policy Leadership (2018) ‘GDPR Implementation In Respect of Children’s Data and Consent’. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf.

Information Commissioner’s Office (2023) ‘New guidance to industry issued for game developers on protecting children’. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/02/new-guidance-to-industry-issued-for-game-developers-on-protecting-children/.

Information Commissioners Office (2018) Applications Children and the GDPR.https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf.

Joshi S and Mohan S (2023) ‘Data Protection Bill 2023: What the law must do for children online’ The Indian Express. https://indianexpress.com/article/opinion/data-protection-bill-2023-law-must-do-children-online-8873392/

Lieber C (2018), ‘Tech companies use “persuasive design” to get us hooked. Psychologists say it’s unethical’, Vox. https://www.vox.com/2018/8/8/17664580/persuasive-technology-psychology.

Manvee (2024) 'Navigating the Dilemma: Balancing Data Protection & Growth in India's Gaming Industry for Children', MNLU Mumbai Law Review Blog. https://lawreview.mnlumumbai.edu.in/2024/05/08/navigating-the-dilemma-balancing-data-protection-growth-in-indias-gaming-industry-for-children/.

Manke C (2000) 'Student-on-Student Sexual Harassment: A Case Comment on the Supreme Cour eme Court's Decision in Da s Decision in Davis v. Monroe County Boar oe County Board of Education. Denver Law Review 78(1). https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1716&context=dlr.

Morrison S 'Fortnite maker Epic Games has to pay $520 million for tricking kids and violating their privacy' Vox. https://www.vox.com/recode/2022/12/19/23516925/epic-games-ftc-settlement-520-

'My Talking Tom Friends', Talking Tom & Friends, available at: https://talkingtomandfriends.com/mttf-rewards/en.

Oehlenschlager M (2021) 'Online Games Gamble with Children's Data', Data Ethics. https://dataethics.eu/wp-content/uploads/GameTechEnglishVersion.pdf.

Office of the Privacy Commissioner of Canada (2019) 'Gaming and personal information: playing with privacy'. https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/digital-devices/gd_gc_201905/

Office of the Privacy Commissioner of Canada (2015) Collecting from kids? Ten tips for services aimed at children and youth. https://www.priv.gc.ca/en/privacy-topics/business-privacy/bus_kids/02_05_d_62_tips/.

Patel NJ, 'Reality or Fiction?', Medium. https://medium.com/kabuni/fiction-vs-non-fiction-98aa0098f3b0

Provisions on the Cyber Protection of Children's Personal Information, (2019) 'Order of the Cyberspace Administration of China No.4'https://www.managebac.com/files/Provisions-on-the-Cyber-Protection.pdf.

Public Consultation Paper (2019), 'Processing of Children's Personal Data and the Rights of Children as Data Subjects under the GDPR' https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Submission%20from%20Facebook.pdf.

Russell NC, Reidenberg JR and Moon S (2018) 'Privacy in Gaming' Fordham Law Legal Studies Research Paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3147068.

Smyr D, Ulianova E (2022) 'Legal Issues of Children's Personal Data Protection'. https://centerprode.com/ojls/ojls0501/coas.ojls.0501.01001s.pdf.

The Danish Society of Engineers' Working Group on Ethics and Technology & DataEthics.eu (2021), 'Report on GameTech Online Games Gamble with Children's Data', Data Ethics. https://dataethics.eu/wp-content/uploads/GameTechEnglishVersion.pdf.

The White House, Office of the Vice President, 'Vice President Biden Announces Strengthening of Title IX', April 20, 2010, https://obamawhitehouse.archives.gov/the-press-office/vice-president-biden-announces-strengthening-title-ix.

United Nations Children's Fund (UNICEF), 'Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry', Discussion Paper Series: Children's Rights and Business in a Digital World (2019). https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf

United Nations Children's Fund (UNICEF) (2020) 'Online Gaming and Children's Rights: Recommendations for the Online Gaming Industry on Assessing Impact on

Children' https://sites.unicef.org/csr/css/Recommendations_for_Online_Gaming_Industry.pdf

Wienrich C (2024) 'Personal space invasion to prevent cyberbullying: design, development, and evaluation of an immersive prevention measure for children and adolescents', Virtual Reality, Springer Nature. https://link.springer.com/article/10.1007/s10055-024-00964-7.

World ESports IESF, Code of Conduct, International Esports Federation, available at: https://drive.google.com/file/d/1_p3s7Pdr0paFH1Smj-vAXwTzLJYtPHIC/view

Zialcita P (2019) 'China Introduces Restrictions on Video Games for Minors', NPRhttps://www.npr.org/2019/11/06/776840260/china-introduces-restrictions-on-video-games-for-minors.

Cases Cited

Davis v. Monroe County Bd. Of Ed., 526 U.S. 629 (1999).