Work in Progress: Privacy Protection for Children 13+ in Virtual Worlds

Molly Maclaren, Jared Jose, Runpeng Jian, Zheng Zeng, Jay Jhaveri, Imani N.S. Munyaka
University of California, San Diego

Abstract

The percentage of children that engage in gaming experiences has increased over time, likely due to the increasing accessibility and diversity of games and the social experiences provided by gaming platforms. However, for parents, allowing children to interact within virtual environments requires trusting that the companies that operate the service will protect children's data and reduce or eliminate the chances of risky experiences. This can be difficult when some gaming companies have already been criticized for the lack of protection. In this work, we investigate the privacy protection of teens by (1) conducting a user survey to determine who adult gamers believe is responsible for children's privacy and (2) analyzing privacy policies to identify how gaming platforms express their data privacy practices to teen players. Thus far, our results suggest that most adult gamers believe that parents are responsible for the privacy of children, and gaming companies are responsible for the privacy of gamers in general. However, our results also suggest that gaming companies have room for improvement in how they express their practices to players. As we continue this line of research, we plan to expand our studies and include player interviews to help identify data privacy gaps in virtual environments.

1 Introduction

According to the Entertainment Software Association, one-fourth of all gamers are children, with 77% of children in the United States of America being part of the number. Gaming for children over the age of 13, or teens, has provided social benefits such as making new friends or maintaining friendships in virtual environments [11].

Virtual environments are simulated experiences that exist almost entirely in the digital realm. Historically, these environments have been hosted by gaming platforms and accessed through a screen, keyboard, and mouse. However, newer environments have begun leveraging mobile devices and, more recently, virtual reality (VR) equipment to allow users to fully immerse themselves in these spaces. With the rise of new VR hardware technologies and advances in mobile device technology, new ways to track and make use of user data have been developed. However, there are strict trade-offs between the degree of user engagement and personal privacy. While the collection of new data types can improve user experience and increase player engagement, parents are concerned about the data collected from their children [1].

In a world where technology and digital spaces are becoming more intertwined with the daily lives of their users, many companies now have access to immense amounts of personal data. While the Federal Trade Commission (FTC) in the U.S.A. is "concerned about teen privacy," the statutes outlined in Children's Online Privacy Protection Act (COPPA) only apply to the handling of data from children under the age of 13 [9]. In their final report, the FTC provided seven principles to guide company decisions. The work focused on the following four principles:

1. Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

2. Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

3. Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

4. Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

However, even with this legislation and the tips the FTC has provided for protecting teens, some companies have had trouble protecting this data [8]. We define teens as children over the age of 12 but under 18 years of age. Thus, we investigate how teens are protected in virtual environment games (Fortnite, Roblox, VRChat, Horizon Worlds). Specifically, we explore the following research questions:

R1 What information is provided in the privacy policies of each game?

R2 In what ways is the information in each privacy policy accessible to children over the age of 12?

R3 From the perspective of adult gamers, who is responsible for the privacy of children in gameplay?

Future Work How do children over the age of 12 and their parents conceptualize the privacy practices of online gaming platforms?

2 Methodology

A mixed methods approach was used to answer our research questions. We (1) identified four online multiplayer platforms with both social and gaming experiences to review, (2) evaluated their privacy policies based on prior work and the principles outlined by the FTC, and (3) conducted a small-scale survey with adult participants. In our future work, we will interview teen gamers and their parents about their perspectives on privacy within these games.

2.1 Game Selection

For the purpose of this study, we chose to review the privacy policies for Fortnite, Roblox, VRChat, and Horizon-Worlds/Meta. Each platform was selected because they have all been publicly criticized in the U.S.A. for how they manage the in-game experiences of children. Roblox has been criticized for displaying ads to children [4]. Fortnite has been fined for violating children's privacy law [7]. VRChat was selected due to a BBC report that found the game allowed children to engage in adult experiences [5]. Lastly, we selected Horizon Worlds. Although, at the time of writing this paper, it is not a popular game or platform amongst gamers, it was selected as a result of Meta monetizing youth data [8].

2.2 Privacy Policy Analysis

We conducted a privacy policy analysis of the four games, pulling techniques of previous work [3, 17], by investigating compliance with industry guidelines such as FTC recommendations and COPPA using deductive content analysis. Four researchers read each privacy policy and used predefined guidelines to identify the content present. Once complete, the researchers met and discussed areas of difference to resolve any conflict. The guidelines are provided in the Appendix.

2.3 Privacy Policy Readability

A readability analysis was conducted to determine if teen players would be able to read and understand the policy. First, we identified five countries that had the most engaged players for each game [2, 12, 13, 15]. Then, each privacy policy was also evaluated to determine if it was available in the most spoken language affiliated with each country. Finally, we identified the average reading level for students in that country using the PISA reading level. The PISA test evaluates the reading proficiency of students between the age of 15 and 16 in a particular country. The average score among the participating countries determines the average reading level. Since the countries of interest scored in or right below the average reading level of the U.S.A., we assume that the PISA reading levels correlate to high school reading levels. Thus, for each game, we used the Flesch-Kincaid score [10] to determine if a privacy policy was written at any of the high school grade levels.

2.4 Adult Survey

The survey was completed by 40 participants who were mainly between the ages of 31 and 40 (64%), white (87.2%), male (70%), and married (82%). All of our participants were from the United States of America and identify as gamers. The survey consisted of a series of vignettes, which are brief descriptions of scenarios involving potential privacy situations a user may encounter on platforms used by the participants, multiple choice questions about privacy preferences, and extended response questions regarding privacy opinions, all of which were presented in a randomized order. For the purpose of this paper, we will focus on the extended response question that asked, "Who is responsible for the privacy (of children) in virtual environments?" to help us characterize the expectation of adults in America.

2.5 Ethical Considerations

Our survey was approved by the University of California, San Diego Internal Review Board. The survey was conducted on Amazon's Mechanical Turk, where MTurk workers were paid $15/hr for their responses. Any potential identifying information from the extended responses was removed before analysis. At the conclusion of our study, we will provide our results to each platform in an effort to encourage change.

Table 1: Privacy Policy Analysis & Readability Results

Game	Player Demographic: Top 5 Countries	Language	Reading Level	Privacy Policy: Language Available ?	Reading Level	Content Included
Fortnite	US	English	10th-11th	✓	College	Children Data Collection Data Security Data Sharing
	Russia	Russian	9th-10th	✓		
	Brazil	Portuguese	9th-10th	✓		
	Poland	Polish	10th-11th	✓		
	Mexico	Spanish	9th-10th	✓		
Horizon Worlds	India	Hindi	9th-10th*	✗	College	Data Collection Data Security Data Sharing
	US	English	10th-11th	✓		
	Indonesia	Indonesian	9th-10th	✗		
	Brazil	Portuguese	9th-10th	✓		
	Mexico	Spanish	9th-10th	✓		
Roblox	US	English	10th-11th	✓	College	Children Data Collection Data Security Data Sharing
	Brazil	Portuguese	9th-10th	✓		
	U.K	English	10th-11th	✓		
	Phillipines	Tagalog	9th-10th	✗		
	Mexico	Spanish	9th-10th	✓		
VRChat	US	English	10th-11th	✓	College	Children Data Collection Data Security Data Sharing
	Japan	Japanese	10th-11th	✗		
	UK	English	10th-11th	✓		
	Canada	English	10th-11th	✓		
	Germany	German	10th-11th	✗		

3 Results

In this section, we detail the outcomes of our various investigations. It is important to note that the results presented are from work currently in progress. We present these results to demonstrate the need for more work in this topic area and spark discussion.

3.1 Privacy Policy Analysis

A majority of our criteria analysis fell into three major categories: data collection, third-party transparency, and data security. Each policy clearly defines which forms of data are collected and used, in addition to permitting the deletion of all user account-related data upon request. For third parties, only Roblox clarifies that privacy is protected when user data is shared with third-party resources. While all of the policies state that their practices of sharing data with governments and third parties are "transparent," none of them explicitly state that they will notify the user when these parties have requested their data. On the security end, each policy provides some form of reassurance that data is kept secure, but none of them clarify whether personal data is encrypted. Additionally, only Roblox states that it will send a notification to the user if there is unauthorized access to their data.

Out of the 4 policies analyzed, only 3 platforms (Fortnite, Roblox, and VRChat) directly addressed the protection of children's privacy. As for Horizon Worlds, children are neither mentioned in the Meta privacy policy nor the Supplemental Meta Platforms Technologies privacy policy, which covers Meta's VR products. While none of the policies specifically address the 13-18 age group demographic, Fortnite and Roblox allow the creation of a child account for users under 13 with parental control settings to limit select features in compliance with COPPA. VRChat proposes that it will delete the account upon being notified that the user is under 13.

3.2 Readability of Privacy Policies

The readability results shown in Table 1 show that none of the privacy policies were written at a level suitable for comprehension by players 13-18 years old. All of the privacy policies were written for college-level readers. Since an average reading level is typically below 12th grade, most minors would struggle to understand these privacy policies independently. Additionally, while all of the policies are available in English, the Fortnite privacy policy is the only policy available in each of the languages affiliated with the five countries that have the most engaged players.

3.3 Responsibility

As we explored data privacy for children online, we asked MTurkers, that identified as gamers, who is responsible for data privacy during gameplay. When this general question was asked, 56% of participants said that the developers or gaming companies were responsible for this protection. However, when we asked who was responsible for safeguarding the data of child users, 66% of participants stated that the parents were responsible, while only 33% of participants stated that developers or the gaming company held some responsibility.

3.4 Limitations

Our user study results are limited by the small number of participants and lack of demographic and location diversity. While our results are similar to that of another study, we believe that a larger number of participants would help us identify any differences in opinion caused by marriage status, gender, location, or parental status. In the next stages of our work, we intend to test to see if these factors have an effect on results. In particular, we plan to survey participants from the countries mentioned in our study. Additionally, our privacy policy analysis and readability measurements are limited by the small number of privacy policies reviewed and the lack of input from gamers 13-17 years old. In our future work, we will expand our list of games and explore privacy policy usability and content from the perspective of gamers.

4 Discussion

The aim of this study was to assess the state of privacy protections for minors ages 13 and above in virtual environment games and identify ways to support this age group when gaming in virtual worlds. (R1) Privacy policy analysis showed that while some platforms recognized children as a unique user group needing protection, only one offered policies or controls specifically targeting minors and families. (R2) Fortnite's policy was the only one available in all languages matching major user groups. Other platforms lacked policy translations for large user bases, preventing some children from providing informed consent regarding their data. (R3) A majority of gamers surveyed believe that while companies hold responsibility for privacy during gameplay broadly, parents are primarily responsible for their own children's privacy.

4.1 Inclusion in Privacy Policies

While our privacy policy analysis found that most privacy policies included a direct reference to COPPA or children and, at the bare minimum, included information about data collection, our readability analysis discovered that some of the privacy policies are not fully accessible by teens from countries that use the platforms the most. These results suggest that some teen players may have difficulty reading the policy because it is unavailable in their language. Additionally, these privacy policies are written for college-educated readers, which are unlikely to be teenage gamers. Based on the PISA scores, players between the ages of 15 and 16 likely read at or below the average student at their level. Thus, privacy policy comprehension could be difficult. We encourage privacy policies to be available in multiple languages and formats to be more inclusive of the player base.

4.2 Community Responsibility

The results of our study suggest that many adult gamers believe that parents are the main entity responsible for the privacy of children during gameplay but that this responsibility falls on gaming companies and developers when children are not directly considered. We believe we received this result because the responsibility of protecting children or teens is generally the responsibility of the parent or legal guardian. Additionally, studies have suggested that video games have negative effects on children and that teens engage in risk-seeking behavior while online, so parental controls and other guidance are often provided for parents [6, 14]. However, some studies now suggest that all children may be experiencing risky situations by simply existing in online spaces [16]. Parents are responsible for their children. However, in online spaces, where parents lack total control, assistance from the gaming companies, developers, and gaming community as a whole might prevent some of the negative or risky experiences children and teens experience online.

4.3 Conclusion & Future Work

In this paper, we present our preliminary findings with the goal of identifying how children of all ages can be better protected online. Thus far, our preliminary results show that although COPPA only requires parental permission for players under 13, privacy policies are not written at an appropriate level for players between 13 and 18 years of age. As we move forward in this research, we plan to explore our research questions further through interviews, a large-scale user study, and an analysis of more privacy policies.

Acknowledgments

We would like to give special thanks to Professor Mai ElSherief and Vaidehi Gupta for their support and guidance throughout the early stages of this project.

References

[1] Parenting generation game. 2019.

[2] Chaitra Anand. The 10 countries with the most facebook users: Is australia among them?

[3] Jasmine Bowers, Bradley Reaves, Imani Sherman, Patrick Traynor, and Kevin Butler. Regulators, mount up! analysis of privacy policies for mobile money services. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*, SOUPS '17, page 97–114, USA, 2017. USENIX Association.

[4] Patrick Coffee. Roblox criticized by children's advertising watchdogequently asked questions. 2023.

[5] A Crawford and T Smith. Metaverse app allows kids into virtual strip clubs. *BBC News*, 2022.

[6] Epic Games. Epic games parental controls.

[7] Federal Trade Commission. Fortnite video game maker epic games to pay more than half a billion dollars over ftc allegations of privacy violations and unwanted charges.

[8] Federal Trade Commission. Ftc proposes blanket prohibition preventing facebook from monetizing youth data.

[9] Federal Trade Commission. Complying with coppa: Frequently asked questions. 2020.

[10] Rudolph Flesch. A new readability yardstick. *Journal of applied psychology*, 32(3):221, 1948.

[11] Amanda Lenhart. Teens, technology and friendships. 2015.

[12] Roblox. A year on roblox: 2021 in data.

[13] Daniel Ruby. Fortnite statistics for 2023 (users, revenue & devices).

[14] Joel Santo Domingo. How i (mostly) stopped my teen from gaming all night s. 2023.

[15] similarweb. Vrchat geography country targeting.

[16] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, Daniel F Perkins, and John M Carroll. Dear diary: Teens reflect on their weekly online risk experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3919–3930, 2016.

[17] Joanna C Zimmerle and Anne S Wall. What's in a policy? evaluating the privacy policies of children's apps and websites. *Computers in the Schools*, 36(1):38–47, 2019.

5 Appendix

5.1 Content Analysis Guidelines

Each researcher considered the questions below and marked the areas of the privacy policies that answered them. Similarities in policy markings determined the agreement.

1. Does the policy say when it was last updated?
2. Does the policy say what was changed since the last time it was updated?
3. What language(s) is the privacy policy available in?
4. What is the Flesch-Kincaid score of this policy?
5. Does the privacy policy state how the customer can contact the company about anything in the privacy policy?
6. Does the privacy policy discuss how it protects children?
7. Does the privacy policy state that it keeps users' data secure?
8. Does the privacy policy state that users need to make a password?
9. Does the company encrypt users' information?
10. Does the privacy policy state that users can control the data that the company collects?
11. Does the privacy policy state that users can delete their data when they leave the service?
12. Does the privacy policy state what information the company collects?
13. Does the company collect only the information needed for the product to function?
14. Does the privacy policy state that users' privacy is protected when used by third parties?
15. Does the privacy policy detail how they use data from the users?
16. Does the privacy policy state that users will receive a notification if the company changes its privacy policy?
17. Does the company comply only with legal and ethical third-party requests for users' information?
18. Does the company require users to verify identity with government-issued identification, or with other forms of identification that could be connected to users' offline identity?
19. Does the privacy policy state that the company notifies users of any unauthorized access to data?

20. Does the privacy policy state that the company is transparent about its practices for sharing users' data with the government and third parties?

21. Does the privacy policy state that the company sends notifications if the government or third parties request access to users' data?