

Parental Use of Privacy Controls in Online Games to Protect Children

April 12, 2021

1 Introduction

Popular online games such as Roblox provide built-in systems and opt-in parental controls that, in addition to limiting usage or exposure to undesirable content, can help protect children’s privacy. Some example controls include blocking access to chat interactions, anonymizing the child’s screen name to others, or prohibiting the broadcasting of gameplay. Epic Games, the developer of Fortnite, recently acquired SuperAwesome Games [5], a company focused on technical implementations to make online services compliant with child data privacy laws such as COPPA and GDPR-K.

While there is related work on general parental involvement in protecting children’s privacy online, there is a research gap on how frequent specific, in-game tools are used by parents. It is not understood if there are any relationships between the general privacy attitudes of parents and the behaviors they exhibit when it comes to utilizing opt-in controls to protect their children’s presence online. The study of this relationship may expose gaps in the usability of parental controls: whether the gaps are awareness, access to the controls, or if the controls sufficiently satisfy the privacy and security concerns of parents. This paper seeks to contribute one look at this relationship by determining if parents are sufficiently aware of in-game tools that protect the security and privacy of children under 13 in Roblox and if they meet parental expectations through a 146-participant survey. We tested if parents lack awareness of tools available within Roblox which may provide security and privacy functionality that is desirable according to their perceptions of privacy and security.

In the next section, we discuss background information and related works in the field of parental involvement in children’s and privacy online. In Section 3 we cover the methodology used for this study. In Section 4 we present the results of our pilot study, and in Section 5 we discuss opportunities for future work in this field and potential revisions of the study.

2 Background and Related Work

This section first provides a brief overview of the main laws protecting children online, GDPR-K and COPPA, and the online game platform Roblox. We then provide a survey of related works evaluating parental involvement in children’s privacy and security.

2.1 Children’s Privacy Laws

2.1.1 COPPA

COPPA, the Children’s Online Privacy Protection Act, is a law in the United States that was created to protect the privacy of children under 13. The Act was passed in 1998, took effect in 2000, and then it was updated in 2013 [13]

COPPA specifies that sites must require parental consent for the collection or use of any personal information on website and online service users 12 and under. The term “online service” broadly covers most services available over the Internet or services that connect to the Internet. This includes mobile apps, games, social networking sites and more [13]. It outlines additional PII classifications that encompass what PII requires parental consent. If a service does not specifically target audiences under the age of 13 but the service owner has reason to believe some of its users are under the age of 13, they must comply with COPPA.

2.1.2 GDPR-K

The General Data Protection Regulation for Kids (GDPR-K) has been described as COPPA for European children [6]. The provision is specifically written to protect the data privacy of children under 16 while they participate in online activities. Specifically, a child is defined as under 16 years old in Germany, Italy, and The Netherlands, France has defined a child as under 15 years old but The UK and Ireland have defined a child as under 13. Practically speaking, games developed for children operating across Europe will need to consider any audience under 16 as children. The law applied to any service or internet-facing experience that is not expressly dismayed, denied, or prevented from being accessed by children as defined above. With increased data protection regulations for online products, to include games, most developers and product companies need to be aware of the regulations as applied to customers that fall within the jurisdiction of the GDPR-K.

2.2 Roblox

Roblox is a global platform where millions of people gather together every day to imagine, create, and share experiences with each other in immersive, user-generated 3D worlds [12]. Roblox has 37.1 million daily active users worldwide [11].

The platform markets to children, and provides additional policies, default features, and opt-in features to provide compliance with GDPR-K and COPPA in addition to providing added functionality. While some features, such as 2FA on new device logins, are common controls provided on many platforms, Roblox also implements controls that are specific to the type of platform it runs, such as allowing users to control who can see their in-game inventory (items can be purchased using real money, sparking a secondary market for selling accounts with valuable or rare in-game items) or who can message them on the integrated messaging platform.

2.3 Related Works on Parental Involvement in Child Privacy

Children spend more time engaging online than with other forms of media, but typically do not fully understand online privacy risks on their own [1]. Most parents aim to utilize technical safeguards to protect children’s privacy online, but the primary focus of the majority of parents is on content exposure rather than the collection of personal information by application providers or malicious actors [2]. In “Are Children Well-Supported by Their Parents Concerning Online Privacy Risks, and Who Supports the Parents?”, less than 20% of surveyed parents check app-specific privacy permissions or review privacy policies when installing applications [3]. This means they may not be doing enough to actively protect their children’s privacy online. In addition to device-provided controls, third-party controls are available to protect children from malicious sites that can steal personal information through network filtering, but these tools themselves are at risk of data leakage and compromise [4].

The risk of personal information exposure when children engage online increases when it comes to games because of the added social interaction element and the difficulty on-device or third-party tools have in providing protection for games without fully prohibiting their use. Our study pilot may help extend existing work by highlighting the awareness of these challenges and the usage of parental controls within games that address them.

3 Methodology

The goal of our study was to prove or disprove that parents do not use Roblox-provided security and privacy controls to protect their children’s Roblox accounts because they lack awareness of their availability. We conducted an online study that surveyed three main components: security and privacy attitudes of parents, the security and privacy attitudes of parents towards their children, and their usage of the catalog of in-game security and privacy controls in Roblox.

Prior to conducting the pilot we conducted a study review with 6 outside individuals and presented drafts of the instrument to our classmates and professors. The survey was refined based on the feedback provided and their responses were not included in the data set. We then ran a test study of 10 participants

on Prolific. These participants were paid \$1.27. The purpose of the test study was to determine if the Qualtrics survey was integrated properly and no issues were reported with regard to completing it. The data of these 10 participants was not included in the analyzed data set.

For the pilot we recruited 146 participants through the recruitment platform Prolific. The Prolific study was titled “Security and Privacy Controls in Online Games for Children” and participants were screened based on if they had children and if the children had regular access to technological devices. Participants had to be 18 years or older. Participants were paid \$1.27 for the survey, which normalizes to \$18.08 per hour. Median time to complete the survey was 3.6 minutes. Of the 146 participants, 85 had children between the ages of 5 and 12 who played Roblox. The other 64 participants completed the first two main components and were not asked to complete Roblox specific portions.

3.1 Component 1: Screening Criteria and Demographics

Because this survey aims to measure the security attitudes of parents, the first group of questions confirms that the participants who made it through the initial screener are further screened to now skew our data toward non-parents. This section was made up of repeat questions from the pre-screener to measure both whether the participants have children and if their children have an online presence and/or play games, specifically Roblox. We found it important to verify the demographics of our participants due to the specific nature of the focus of this study. We also aimed to ensure that the children themselves were not responding to the survey.

3.2 Component 2: General Security and Privacy Attitudes

The IUIPC [7] research and Westin’s privacy attitude [8] study showed that there are three categories of attitudes towards privacy: unconcerned, pragmatist and fundamentalist. The second section of survey is focused on finding the privacy attitudes of parents to lay a baseline for their privacy attitudes toward their children. The hypothesis here is that, the more concerns of privacy of parents, the higher motivation of protecting children’s privacy in online games.

There are a total 6 questions in this section of survey, that covers how parents are concerned about the online game data collection, protection, deletion, and the confidence of parents regarding the game company’s reputation.

To find out the parent’s actual online behavior [9], we designed a questionnaire to ask whether it is ok to “collect personal information” and whether it is ok to “collect personal in-game behavior data” for the same purpose (“to improve game quality”). These two questions are essentially the same, since the “in-game behavior data” is “personal information”. However, the general public may be more sensitive to the term “personal information”, instead of “in-game behavior data”. The latter is technical jargon that is less familiar to the general public.

3.3 Component 3: Security and Privacy Attitudes Towards Their Children

Security and privacy do not only exist for the individual. Perceptions about security and privacy are shaped not only by personal experience and attitudes but also via the social constructs that the security and privacy controls are being applied within. The internet and technology ecosystems are inherently social places and the understanding of its users are shaped by their social interactions as much as their technological interactions. Perceptions of privacy are socially constructed through communication and transactions with social entities over a networked environment, a process that involves a certain level of technical skill and literacy [10]. Component 3 of this paper aims to answer the question: what aspects of online privacy and security do parents find important when applied to their children?

This section of the study aims to find differences between participants' attitudes towards security when applied to themselves vs. to others, specifically their children. The hypothesis is that attitudes will shift towards more controlled or less risk tolerant when applied to children of participants. Instructions to the participants were: "When answering the following questions, please consider any and all interactions your child(ren) has with online platforms. E.g., mobile applications, gaming platforms, virtual school, social media, etc."

This section of the survey had a total of 7 questions that assess the participants' understanding of the online game data collection, protection, deletion, and the confidence of parents regarding the game company's reputation when specifically applied to their children.

3.4 Component 4: Usage of Roblox Controls for Child Accounts

To determine which features to measure the usage of, we created a test Roblox account and set the player's age to 10 during account creation. Roblox alters the user experience depending on if the account owner's reported age during account creation is above or below 13 years of age. For example, an account for a player 13 years or older is requested to input their email address for verification purposes. An account for a player 12 years or younger is requested to input their parent's email address to receive their parent's consent. A player 12 years or younger is also unable to access certain features by default, such as linking their account to other platforms like YouTube and Twitch. We then evaluated and catalogued each security and privacy feature to choose. We omitted controls required by default, such as email verification.

3.5 Analysis Methods

We applied basic statistical analysis to identify top-level trends and potential correlations. We used our hypothesis and intuitions to guide us on what categorizing and bucketing to focus on. Because our measurement of privacy attitudes

is modeled after Westin’s privacy index [7], we categorized responses to estimate which privacy attitude to categorize the participant as.

After implementing some of the improvements identified elsewhere in this paper, future analysis could validate some findings with a level of statistical significance or uncover unknown patterns.

3.6 Limitations

In the scope of this study, we did not consider the perspectives of participants without children. In our review of parents privacy attitudes when considering themselves and their children, we cannot make a complete comparison because we did not measure if parents use in-game controls for their own, personal accounts.

When researching Roblox, we accept that we are only getting the perspective towards a single platform. Online games attract many audiences with potentially differing privacy attitudes. Future opportunities could conduct between-group studies of the audiences of multiple games.

4 Results

4.1 Component 2: General Security and Privacy Attitudes

The full set of component results are in the Appendix, Table 6.

Table 1: Question Mapping to Privacy Attitudes

Q46	Q39	Q41	Q43	Q44	Q45
Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly Concerned
Somewhat agree & disagree	Somewhat agree & disagree	Somewhat agree & disagree	Somewhat agree & disagree	Somewhat agree & disagree	Somewhat Concerned
Strongly disagree	Strongly disagree	Strongly disagree	Strongly disagree	Strongly disagree	Not Concerned Not Sure
Fundamentalist	Pragmatic	Unconcerned			

100pt100pt

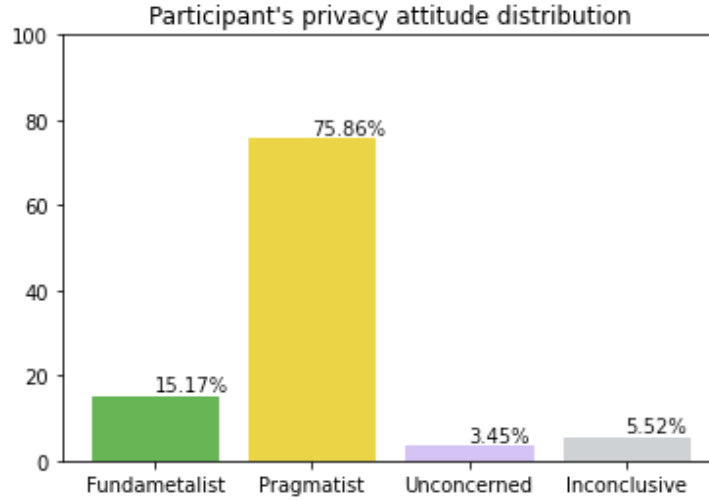
To determine which category a participant belongs to, we need to look into survey questions Q39, Q41, Q43, Q44 and Q45. We would ignore the data for Q46, because the Q39 reflects the real type of a participant based on [9].

Q39 - Q45 are equally weighted. If a participant has 3 or more choices that fall into the same category, this participant should belong to the desired category as shown in table 2 (example) and table 3 (full distribution) below:

Table 2: Sample Participant Attitude Labeling

Q39	Q41	Q43	Q44	Q45	Conclusion
Strongly agree	Strongly Agree	Strongly agree	Strongly agree	Strongly concerned	Unconcerned
Somewhat agree	Somewhat Agree	Somewhat disagree	Somewhat agree	Somewhat concerned	Pragmatist
Strongly agree	Strongly Agree	Somewhat disagree	Strongly disagree	Strongly concerned	Fundamentalist
Somewhat agree	Strongly agree	Somewhat disagree	Strongly agree	Strongly concerned	Inconclusive

Figure 1: Component 2 Participant Attitude Distribution



4.2 Component 3: Security and Privacy Attitudes Towards their Children

As previously covered, this section aimed to measure the security and private sentiments and attitudes of parents when they apply the knowledge to their children. Overall, most (97%) participants found it either important or extremely important to not only educate their children on how to protect their security and privacy when online but to also take an active role in helping their children enact these protections. The specific questions from this section of the survey are outlined below in Appendix, Table 7 with annotated results. The mapping of responses to privacy attitudes is below in Table 4.

Table 3: Overall Participant Attitude Distribution

Q13	Q14	Q15	Q16	Q18	Q19	Q20
Extremely / Very Important	Extremely / Very Important	Extremely / Very Important	Extremely / Very Important	Extremely / Very Important	Extremely / Very Important	Extremely / Very Important
Somewhat agree & disagree	Somewhat agree & disagree			Somewhat agree & disagree	Somewhat agree & disagree	Somewhat agree & disagree
Not At All Im- portant	Not At All Im- portant	Not At All Im- portant	Not At All Im- portant	Not At All Im- portant	Not At All Im- portant	Not At All Im- portant
Fundamentalist	Pragmatic	Unconcerned				

The analysis of each section after Component 2 of this paper could be expanded with further comparative analysis but was not fully conducted during this pilot. Future research could be used to determine not just the sentiments of the parents who participated in our survey but to measure and observe the actual actions they undertake to enforce security controls and protections for their children outside of games to determine how the platform impacts actions of parents.

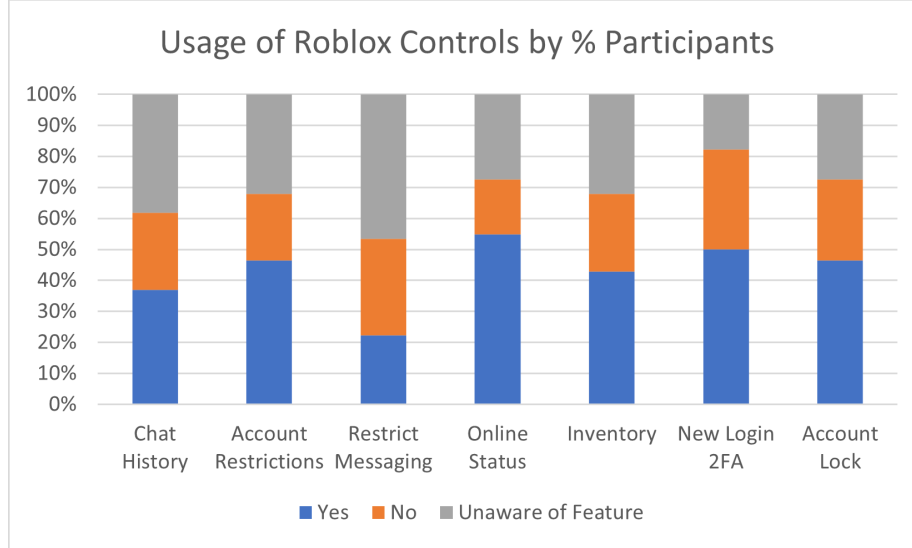
4.3 Component 4: Usage of Roblox Security and Privacy Controls

We found that the majority of participants use at least one privacy and security control available for children’s accounts in Roblox. 4% of participants whose children played Roblox reported that their comfort with the privacy and security controls in Roblox was a factor in letting their child play. Of the participants whose children do not play Roblox, 3.7% of participants reported their concerns about privacy and security were a factor in their decision. Similarly, 5.8% and 4.1% of participants reported they were concerned about their child interaction with strangers or being exposed to inappropriate content, respectively.

80% of participants with children that play Roblox were aware of and use at least one control available to them in Roblox. Of these controls, the most commonly used control was restricting who can see your child’s online activity in Roblox. The least commonly reported used control was restricting who can message your child in Roblox.

Figure 2 shows the reported usage of each control measured in the survey. Participants were only asked about restricted messaging if they did not answer yes to account restrictions because it sets messaging restrictions on by default.

Figure 2:



5 Discussion and Future Work

When analyzing the data, we looked at if the buckets of participants we categorized by Westin’s index (Fundamentalist, Pragmatists, Unconcerned) in component 2 had any statistically significant correlations with using Roblox controls. We examined if answers to component 3 about general privacy behaviors and attitudes towards their children had any statistically significant correlations with Roblox control usage. For each of these, we first looked at control usage by bucketing responses as “uses control” and “does not use control or is unaware.” For controls that have a clear mapping to component 3 responses, such as monitoring behavior and reviewing Roblox chat history, we looked at the relationship between the specified behavior in component 3 and the non-bucketed does use, does not use, or unaware responses.

We ran the analysis methods described above against all seven measured Roblox controls. This section will outline some of the statistically significant relationships we found and those that are close to being statistically verifiable. Other relationships showed some trends but would require a refined study to demonstrate significance.

5.1 Privacy Pragmatists Use Blanket Controls the Most

The Account Restrictions setting can be considered one of the more strict controls in Roblox because it sets multiple settings to their strictest parameters. Editing those additional settings is not possible unless the account restrictions setting is turned off.

By looking at a chi-squared test, there is a statistically significant relationship between privacy attitude as labelled in Component 2 and using the Account Restrictions feature ($p=0.0475$). 89.5% of participants who use the account restrictions feature belong to the pragmatist group. One possible explanation is that pragmatists are concerned about privacy but also balance ease of control. By using the account restriction feature, pragmatists get increased privacy on their child's account without having to review each individual setting. Fundamentalists used the feature at a statistically significant rate lower than participants in the Pragmatist and Unconcerned categories. We posit that a privacy fundamentalist wants to be informed of each privacy decision they make, and as such are interested in reviewing each possible control and making a decision as opposed to only accepting the behavior prescribed by using the Account Restrictions feature.

5.2 Differences in Behavior Between Gamer and Non-Gamer Participants

One demographic question we asked is if the participant played online games at least once a month. The purpose of this question was to explore any difference between parents who did and did not have first hand experience of modern online games. We found that there was a statistically significant relationship between being an online gamer and using two-factor authentication on their child's Roblox account to monitor logins on new devices (chi-squared test $p=0.0161$). Across all but one measured feature, participants with online game experience used privacy and security features at a higher rate than participants with no online game experience.

The outlying feature in this instance is restricting who can message your child in-game. For this feature, 78.6% of participants who reported not restricting messaging capabilities were online gamers themselves. One possible explanation is that parents who are online gamers understand the risks and benefits to social interaction in online games, and may rely on education outside of the game to inform their child's behavior. Attempting to understand the reasons why parents choose not to use certain privacy and security features is an opportunity for further study in this topic.

5.3 Participants Actively Monitor Their Child's Online Activity Even In-Game

Participants that report actively monitoring their child's online activity use at least one measured privacy or security feature in Roblox. Our pilot found 89% of participants who use at least one feature of Roblox report that they actively monitor their child's online activity in general (chi-squared test $p=0.001$). More specifically, 93.5% of participants who use the chat history feature actively monitor their child's online activity in general (chi-squared test $p=0.054$). A larger study may validate that participants are willing to act on their privacy attitudes when it comes to their children with $p < 0.05$.

5.4 Participants Are More Often Unaware of Controls Than Not Use Them

42 participants reported that they actively monitor their child’s online activity for privacy risks but were unaware of at least one feature measured in the survey. 26 participants who were unaware they could view their children’s chat history in-game reported that they actively monitor their child’s online behavior in general. 3 participants were unaware of any feature measured in the survey. These data points suggest a trend that there are parents who have privacy attitudes that they do not act on in Roblox because they are unaware they are able to.

5.5 Future Work

There is more understanding that can be done in the space of parents involvement with in-game privacy and security controls. While we did find that many participants care and use privacy controls, they were not aware of all features present. Some participants care about privacy but explicitly do not use in-game controls. This work could be extended with additional studies and interviews to understand reasons why parents do not use in-game controls when they may use privacy controls elsewhere. Usability studies on the settings interfaces of Roblox may also highlight areas where game developers can make their settings more discoverable and increase usage. One example is that account restrictions, which sets both content curation and privacy settings, is found in the “security” settings page, and not the “privacy” settings page. Similarly, the account pin setting which locks all setting pages is only accessible from the “security” settings page.

Lastly, we are interested in understanding if there are differences between game platform audiences. Future work in this area could involve surveying the privacy attitudes and behaviors of parents whose children play other titles. We have shown that parents who play online games are more likely to use in-game controls for their children, and understanding if they make similar privacy decisions for their own game experiences is also worth exploring to fully understand the differences in parental privacy attitudes when considering themselves versus considering their children.

6 Conclusion

We set out on this survey to explore the security sentiments of parents of gamers when applied to themselves and to their children. Specifically, we wanted to address whether parents were aware of or are using in-game security and privacy controls for their children when engaging online and on Roblox. Through our pilot, we were able to determine that most parents of gamers value their children’s online privacy while also trusting in them to secure their own personal data. They also are educated on security and privacy matters but may not ap-

ply them to themselves as much as their understanding would suggest. Ideally, we would dive deeper into the correlations between parents who game and the security controls their children use or into the correlations between parents who value security and how secure their children actually are online.

7 Acknowledgements

Thank you to our instructors, our classmates, and our coworkers and friends who initially critiqued and provided feedback to our pre-pilot survey questions and data and analysis methods.

8 References

- [1] G. Wang, J. Zhao, and N. Shadbolt, “Are Children Fully Aware of Online Privacy Risks and How Can We Improve Their Coping Ability?,” ArXiv190202635 Cs, Feb. 2019, Accessed: Feb. 16, 2021. [Online]. Available: <http://arxiv.org/abs/1902.02635>.
- [2] J. Zhao, U. Lyngs, and N. Shadbolt, “What privacy concerns do parents have about children’s mobile apps, and how can they stay SHARP?,” ArXiv180910841 Cs, Sep. 2018, Accessed: Feb. 16, 2021. [Online]. Available: <http://arxiv.org/abs/1809.10841>.
- [3] J. Zhao, “Are Children Well-Supported by Their Parents Concerning Online Privacy Risks, and Who Supports the Parents?,” ArXiv180910944 Cs, Sep. 2018, Accessed: Feb. 16, 2021. [Online]. Available: <http://arxiv.org/abs/1809.10944>.
- [4] S. Ali, M. Elgharabawy, Q. Duchaussoy, M. Mannan, and A. Youssef, “Betrayed by the Guardian: Security and Privacy Risks of Parental Control Solutions,” Annu. Comput. Secur. Appl. Conf., pp. 69–83, Dec. 2020, doi: 10.1145/3427228.3427287.
- [5] “SuperAwesome joins the Epic Games family,” SuperAwesome. <https://www.superawesome.com/superawesome/joins-the-epic-games-family/> (accessed Feb. 19, 2021).
- [6] “GDPR-K: How the kids data privacy law affects games publishers everywhere,” Games Industry Biz. <https://www.gamesindustry.biz/articles/2018-04-03-gdpr-k-how-the-kids-data-privacy-law-affects-games-publishers-everywhere> (accessed Apr. 11, 2021).
- [7] N. K. Malhotra, S. S. Kim, and J. Agarwal, “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model,” Information Systems Research, vol. 15, no. 4, pp. 336–355, 2004.
- [8] P. Kumaraguru and L. Cranor, “Privacy indexes : a survey of Westin’s studies,” Carnegie Mellon, 2017.
- [9] S. Barth and M. D. T. de Jong, “The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review,” Telematics and Informatics, vol. 34, no. 7, pp. 1038–1058, 2017.
- [10] T. Dinev and P. Hart, “Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact,” International Journal of Electronic Commerce, vol. 10, no. 2, pp. 7–29, 2005. [11] “Roblox Usage and Growth

Statistics,” Backlinko, <https://backlinko.com/roblox-users> (accessed Apr. 11, 2021).

[12] “For Parents,” Roblox, <https://corp.roblox.com/parents> (accessed Apr. 11, 2021).

[13]. “What is COPPA and how does it Affect My Game Company?” Odin Law, <https://odinlaw.com/what-is-coppa-and-how-does-it-affect-my-game-company> (accessed Apr. 11, 2021).

9 Appendix

Table 4: Component 2 Question Results

Q46: Online game companies should collect personal information to improve game quality			Q39: Online game companies should collect personal in-game behavior data to improve game quality		
Strongly Agree	3.57%	3	Strongly Agree	9.52%	8
Somewhat Agree	19.05%	16	Somewhat Agree	55.95%	47
Somewhat Disagree	42.24%	38	Somewhat Disagree	20.24%	17
Strongly Disagree	32.14%	27	Strongly Disagree	14.29%	12
Q41: Online game companies collect too much data			Q43: Online game companies do a satisfactory job at protecting your information		
Strongly Agree	37.65%	32	Strongly Agree	7.06%	6
Somewhat Agree	45.88%	39	Somewhat Agree	40.00%	34
Somewhat Disagree	15.29%	13	Somewhat Disagree	47.00%	40
Strongly Disagree	1.18%	1	Strongly Disagree	5.88%	5
Q44: Online game companies should be allowed to share your personal information with third party with your consent			Q45: Would you be concerned about data online game companies keep about you if you deleted your account?		
Strongly Agree	5.88%	5	Strongly Concerned	47.00%	40
Somewhat Agree	22.35%	19	Somewhat Concerned	43.50%	37
Somewhat Disagree	28.24%	24	Not Concerned	7.00%	6
Strongly Disagree	43.53%	37	Not Sure	2.35%	2

Table 5: Component 3 Question Results

Q13 - How important do you feel it is to educate your child(ren) on online privacy and security?

Extremely Important	87.06%	74
Very Important	12.94%	11
Moderately Important	0.00%	0
Slightly Important	0.00%	0
Not at all Important	0.00%	0

Q15 - Do you actively monitor your child(ren)'s online activity for privacy risks or what personal information they divulge?

Yes	83.53%	71
No	16.47%	14

Q18 - How important is protecting your child(ren) from divulging private information about themselves?

Extremely Important	80.00%	68
Very Important	20.00%	17
Moderately Important	0.00%	0
Slightly Important	0.00%	0
Not at all Important	0.00%	0

Q20 - How important is preventing others from divulging private information about your child(ren)?

Extremely Important	76.47%	65
Very Important	21.18%	18
Moderately Important	4.35%	2
Slightly Important	0.00%	0
Not at all Important	0.00%	0

Q14 - How important do you feel it is to actively enforce online privacy and security rules for your child(ren)? E.g., using built-in parental controls and features, sharing accounts with your child(ren), etc.

Extremely Important	60.00%	51
Very Important	32.94%	28
Moderately Important	7.06%	6
Slightly Important	0.00%	0
Not at all Important	0.00%	0

Q16 - You trust your child to actively protect their personal information online.

Yes	62.35%	53
No	37.65%	32

Q19 - How important is protecting your child(ren) from divulging private information about other members of your family?

Extremely Important	72.94%	62
Very Important	22.35%	19
Moderately Important	4.71%	4
Slightly Important	0.00%	0
Not at all Important	0.00%	0