COPPA Revisions to Protect Children's Privacy and Prioritize Children's Wellbeing in Roblox and Beyond

By Jessica Luan

Introduction:

In 1998, Congress passed the Children's Online Privacy Protection Act (COPPA) to give parents control over information collected from their children online[1]. The law requires websites–both those directed at children under 13 and general audience sites that collect information from children under 13–to obtain verifiable consent from the child's parent before collecting their child's name, home address, email address, telephone number, or Social Security number.

Children's relationship with the Internet has changed dramatically since the '90s. Websites and apps like TikTok, Facebook, YouTube, Fortnite, and Roblox have replaced AOL, Yahoo, and Geocities. Whereas 46% of Americans had access to slow Internet, and 62% of Americans had flip phones, today 90% of American households have broadband Internet[2] and smartphones are so ubiquitous that 70% of children under 8 had used smartphones or tablets to play games.

New websites and new mediums of access introduce new benefits, such as social connections to faraway friends and family, educational technology services, and opportunities for online self-expression. They also introduce new harms. In 1998, before sophisticated social networking sites like TikTok, Instagram, and Facebook existed, primary risks included easy access to pornography, contact from online predators[3], and deceptive personal information collection policies: many websites encouraged children to submit personal or family information in exchange for prizes or special characters without their parent's knowledge. Today, the Internet's harms run the gamut from disturbing children's content[4], exploitation of user psychology to increase their screen time, and privacy violations from algorithmic recommendations[5].

Understanding children's safety and privacy on Roblox is significant because the platform exemplifies new and old dangers and because of the platform's cultural and financial significance as an emerging metaverse company. The online game platform and game creation system is the 32nd most visited website in the world and the only game in the top 50 most visited websites[6]. Two-thirds of nine- to twelve-year-old children in the US are on the platform[7], which boasts 200 million monthly active users and 55 million daily active users. Developers can create games for other users, like how Youtubers produce videos for all viewers on the platform. Upon entering the website, users can access 50 million user-generated "experiences," where they can adopt pets, attend high school, or play copycats of every game imaginable: Flappy Bird, Minecraft, or Fortnite alongside other players in immersive environments[8]. But despite its strong parental controls, the platform struggles with online predators, sexual content[9], and an inability to categorize and recommend safe, age-appropriate content for its enormous user base[10]. Consequences to children include harms to physical safety[11] and mental and emotional distress from interacting with players or content beyond their social, cognitive, and emotional capabilities[12]. Roblox uniquely combines the stranger danger of online chatrooms from the 1990s with the content moderation issues shared by other 21st century platforms lie YouTube, Instagram, and TikTok. Roblox intends for its platform to serve as a social space providing diverse players with an abundance of educational and social experiences. But the increased online connection and interpersonal communication may lead to more opportunities for

information collection, presenting new challenges for lawmakers seeking to protect children's online privacy[13].

COPPA is ill-suited to protect children from risks such as the collection of personal data for internal recommendations or children's ability to access age-appropriate content due to its overreliance on parental consent, outdated definition of personal information, and limited scope for VPC requirements. Asking parents to consent to the collection of their child's name, email address, is no longer sufficient to protect their privacy and safety. On websites like Roblox, new games are constantly added, which means new opportunities for inappropriate content or dangerous adults to reach children's screens. Parents cannot and should not have to shield their children from ever-changing threats without assistance or from data collection techniques that they themselves might not understand. Studying practices that improve the privacy and safety of children within Roblox may inform policy decisions that bring rich, age-appropriate online experiences to children in all corners of the third major iteration of the Internet.

This paper proceeds as follows. Part I describes the Internet landscape, the relationship between children and the Internet, and why these factors necessitate improved privacy protections. Part II summarizes the COPPA's goals, contextualizes its passage, describes its past and present shortcomings, provides a deep dive into verifiable parental consent, and considers international approaches to children's privacy. Part III proposes recommendations to resolve technical and fundamental flaws with both the implementation of COPPA and the requirements of the Act itself. Part IV provides ideas about how these threats to children's privacy, safety, and wellbeing may evolve as the metaverse evolves.

I: Children's Relationship with the Internet and Threats to Online Safety and Privacy

A) Overview

Robust children's privacy protections and parental involvement are critical due to the ubiquity of the Internet, the nature of children, and emerging threats from a rapidly evolving Internet landscape.

Digital privacy issues are fundamentally children's issues because of how intertwined the Internet is in children's everyday lives. In 2017, 98% of children under 8 had access to a mobile device at home, 78% had access to a family tablet, and 42% of children had their own tablet[14]. In contrast, in 2011, 41%, 8%, and less than 1% of children under 8 had access to a home smartphone, a home tablet, and a personal tablet, respectively. With so many children are plugged into the Internet, which means issues with children's online safety, content moderation, and privacy directly impact an entire generation of American youth.

Additionally, despite the quantity of time that children spend on the Internet, their understanding of the consequences of their extensive Internet use is limited. Minors, from elementary schoolers to high school students, often don't understand how their data is collected, analyzed, and used for 3rd party marketing, even though they believe they have the right to erase or limit the use of their digital data[15]. Young children especially have limited cognitive capacity for reasoning[16], and often cannot conceptualize risks associated with online behaviors such as disclosing personal information or purchasing in-game currencies[17]. The unprecedented internet use by children means unprecedented opportunities for data collection of users who developmentally do not understand how to protect themselves online. With new innovations such as immersive, interactive mobile and PC gaming experiences, threats to children's privacy have evolved from information children provide the service through surveys or online web forms.

They can also include communication and behavioral patterns[18] of children's online activity. Thus, COPPA should be revised to expand the definition of personal data to include behavioral data to address present-day shortcomings, as well as biometric data that may soon be collected when the metaverse fully integrates the virtual and the physical. This also provides opportunities to incorporate mandatory privacy notices in COPPA to enhance children's understanding of their role as digital citizens.

Finally, the mobile Internet paradigm also changes the relationship between children, their parents, and the Internet, highlighting the need for more practical privacy legislation. The TV is a more "public" device than a tablet or smartphone. When children watch TV in the living room, the content they are viewing is simultaneously visible to others in the room, such as their parents. In contrast, tables and smartphones are much more solitary devices[19].When children access apps on smartphones or tablets, they can do so out of sight of their parents on a screen that only they can see. According to Common Sense Media, 37% of parents surveyed reported never or hardly ever playing or using mobile apps or games with their kids, and 20% of children find games or apps by themselves[20]. Children are increasingly online, but they are also navigating the virtual world alone on devices that strain the caretaker relationship between children and their parents. This underscores the necessity of child-centric revisions to COPPA that ensure that children understand privacy and data collection risks, instead of only providing this information to the parent.

COPPA's emphasis on the data collection and parental consent, rather than data sent and received[21] and children's agency, renders it ineffective against current and emerging threats. COPPA tasks parents with keeping kids safe online by seeking to obtain their verifiable consent before collecting personal information from children under 13. However, it fails to address the fact that many children navigate the Internet independently of the parents. It also fails to consider dangers beyond unwelcome advertiser mail or contact with dangerous individuals.

B) Significance of Roblox

Roblox exemplifies existing risks and introduces new dangers that may become commonplace as the metaverse expands.

First, games such as Roblox further impede parents' ability to monitor their children's online activities. Because Roblox houses millions of varied experiences on one platform, playing Roblox could mean adopting pets, buying new wigs for her avatar, or stumbling upon virtual strip clubs that have escaped the platform's content moderation system[22]. Just because a parent has consented to their child accessing the platform, doesn't mean that they consent to the child accessing every single experience in the system. There must be some way to catalog the platform's experiences and ensure that children can only access experiences that are appropriate to their age. On the user end, this would require accurate age verification systems and informed parental consent of the risks platform participation may involve. On the company end, it requires stronger content moderation and perhaps internal content rating systems, as the video game industry implemented in the 1990s. However, this issue is out of the scope of the paper. Revisions to COPPA that can address this problem include requiring verifiable parental consent before signing up for platforms that contain general audience content and requiring platforms to ensure that young users understand the risks of their platform through child-friendly notices.

Roblox's parental controls for young users are relatively strong. Parents can set an account PIN to lock their security settings, disable chat or messaging, restrict access to a curated list of age-appropriate games, and set a monthly limit on how much money their child can spend.

The game also automatically disables voice chat, filters chat for vulgar words, and limits chat capabilities to users in an approved friends list or players under 13. However, many parents raise concerns that these safety features are not enough. One father had enabled the strictest recommendations so that his eight-year-old son could only access 1000 Roblox-curated games out of the nearly 50 million "experiences" on the platform. Yet general audience games still showed up in his son's "recommended for you" lists, and his son encountered a popular role-playing game that featured songs with racist lyrics and sexual imagery[23]. This demonstrates that while Roblox's stringent parental controls may be effective at protecting children against traditional Internet dangers, such as contact from online strangers, parental controls are not enough to protect children from general-audience content that may be disturbing for young users. Parental controls against contact with strangers do not protect children from inappropriate or disturbing content. That said, parent consent is a necessary and effective tool for protecting children's safety, as it promotes parental awareness of platform risks–parents can't protect children if they're not aware of the fact that their kids may be in danger.

To protect children's safety and privacy on Roblox and similar websites, COPPA should be revised to: (1) include more accessible, 21st century-relevant verifiable parental consent methods that will promote truthful age submissions, (2) require VPC before children under 13 can access platforms that carry risks of general audience content, rather than solely for personal information collection, (3) promote children's agency, self-sufficiency, and digital literacy by expanding the privacy policy notice to include children as well as parents and (4) expand the types of information that fall under personal information.

II: What Policy Tools Exist to Protect Children's Safety, Privacy, and Wellbeing?

A) COPPA Overview

The Children's Online Privacy Protection governs the online collection of personal information of children under 13. Passed in 1998, the 24-year-old legislation requires operators of websites directed to children or websites that have knowledge that they are collecting personal information from a child to obtain verifiable parental consent before collecting, using, or disclosing personal information from children 12 and under. Additionally, operators must provide a transparent and accessible privacy policy, implement heightened security practices to safeguard minors' data, and limit the use of children's personal data for direct marketing purposes. The law defines personal information as including, but not limited to full name, home address, email address, photographs, geolocation, or a persistent identifier to recognize a user over time such as a cookies[24].

COPPA has been revised since its passing. In 2013, the FTC broadened the definition of children's personal information to include persistent identifiers, cookies, geolocation information, photos, videos, and audio recordings. In 2017, FTC revisions included addition of methods to identify parental consent (knowledge-based authentication questions and facial recognition) and reinforcement that COPPA applies to any Internet-connected device, including IoT devices and connected toys[25].

B) Historical Context

In 1997, the FTC responded to a petition from the Center for Media Education (CME) to investigate Kids Com. KidsCom was not unlike Roblox: it was an interactive website of virtual worlds frequented by children aged 4 to 15. To gain access to the website, users had to submit

information such as name, sex, birthday, email address, home address, and school year through an online survey. If users wanted in-service awards, they could submit name, address, and product and activity preferences. However, KidsCom didn't disclose that they were using this information to support marketing efforts[26].

In its response to the petition, the FTC established several principles that underlie COPPA:

1. Companies must obtain parental consent before releasing individual identifiable data about children
2. Personal identifiable information disclosure must be made to parents given that children may not understand this information.
3. Collecting PII for a particular purpose, when the information is used for another purpose parents may find material is deceptive.

The FTC's 1998 report "Privacy Online: A Report to Congress" built on these findings to assess whether self-regulation was effective in protecting consumer privacy online. The report is notable because it proposed parental control as the primary means to protect the online collection and use of personal information from children. The report attributed exposure to safety risk to lack of parental control and oversight of children's data. The report also recommended that any legislation Congress passed should place the responsibility of determining online data collection on parents.

COPPA reflects the language and principles in these two earlier documents. Senators Richard Bryan and John McCain introduced COPPA in the Senate in summer of 1998 to ensure that advances in telecommunications technology would not expose children to "exploitation and harm by deceptive marketers and criminals." To protect children on the Internet, COPPA sought to address the overmarketing toward children and collection of personal identifiable information from children, as well as unintentional sharing of information with online predators who could find it online[27].

The act sought to achieve 4 goals:

1. Enhance parental involvement in child's online activities to protect privacy of children in online environment
2. Protect the safety of children online such as chat rooms, home pages, and pen-pal services in which children may make public postings of identifying information.
3. Maintain the security of children 's personal information collected online
4. Limit the collection of personal information from children without parental consent

Their solution, however, was not to hold platforms accountable for keeping children safe from criminals or online marketers. Instead, the Senators concluded that "enhanced parental involvement" over children's online interactions could shield them from malicious activity and protect their safety in online locations such as chat rooms.

To achieve this objective, under COPPA the FTC would require the commercial website to:

1. Obtain parental consent for the collection, use, or disclosure of personal information from children 12 and under
2. Provide parents access to their children's personal information.
3. Establish and maintain reasonable procedures to ensure the confidentiality, security, accuracy, and integrity of personal information about children[28].

Notably, Senator Bryan also foresaw Internet proficiency as a "critical and vital skill that will be necessary for academic achievement in the next century." He strongly pushed for children's

independence online: “To tell children to stop using the Internet would be like telling them to forgo attending college because students are sometimes victimized on campus. A better strategy is for children to learn how to be street smart in order to better safeguard themselves from potentially deceptive situations.”[29]Despite this rhetoric, the final bill leaned heavily on parental decision-making rather than supporting children’s digital literacy.

C) Shortcomings

COPPA received early praise from privacy advocates for its strict regulations, uniform legal standards, and the awareness it brought to children’s concerns[30]. Additionally, the FTC’s 2002 review found that 90% of children’s websites made privacy policy publicly available, compared with 10% before[31]. Additionally, 45% of websites had made legitimate efforts to obtain verifiable parental consent by contacting parents through email instead of relying on an online form[32].

However, COPPA also had a chilling effect on youth-directed websites. Following the passage of COPPA, many startup websites shut down their youth divisions due to high costs associated with employing chat room moderators, training phone line personnel, and processing permission forms. The practical effect was not for websites to devote more resources to protect their young users. Instead, they banned users 12 and under, which incentivized age fraud from users and incentivized websites to circumvent their responsibility to obtain parental consent. Some sites disallowed children under 13 to access the site, while others shut down website divisions that could be attractive to children. Shuttered youth-directed sites often pushed children to access adult sites instead[33]. Additionally, COPPA suffered from general noncompliance. Children would open fake email accounts and give themselves permission, and sometimes parents even aided their efforts–they preferred that children falsify their age to giving children their credit card numbers[34]. Even in its immediate aftermath, COPPA’s verifiable parental consent requirement was at best useless and at worst counterproductive. In essence, COPPA “closed the playgrounds and sent kids to play in the street[35].”

These shortcomings have persisted and evolved. Data now encompasses more than just name, address, and email. It also includes byproducts of children’s online activities and invisible data harvesting of in-game behaviors, keystrokes, or mouse behaviors[36]. But the primary assumption underpinning COPPA was that privacy arise from personal information that children volunteer to the website. Consequently, the scope of COPPA’s VPC requirements and its definition of personal information are not comprehensive enough to protect children’s privacy and safety. First, COPPA only protects non-personal information such as keypress responses or achievement information if it's combined with personal information[37]. However, rapid developments in machine learning and data science enable companies determine a user’s identity even with normal data anonymization and sanitization[38]. This means that COPPA’s definition has not kept pace with innovation. Although COPPA prohibits the use of persistent identifiers to amass a profile by 3rd party advertisers, COPPA does not provide any provisions as to the use of personal data to provide personalized content recommendations for children, which, if inappropriate, can be equally harmful to children[39]. Second, COPPA seeks to empower parents to protect their children’s privacy and safety and ensure the security of children’s personally identifiable information by requiring parental consent when collecting such information[40]. But parents should be able to consent to more than just opting out of personal information collection. The Act defines privacy as compliant data collection of children but fails to consider that helping

parents control data collection to strive for safety from deceptive third-party marketers does not equate to keeping children safe from age-inappropriate online experiences.

Commented [JL1]: s

D) Verifiable Parental Consent

i) Overview

Under COPPA, parents are the primary mediators of children's online interactions. Just as parents must supervise their children in public spaces such as theme parks, grocery stores, and doctor's offices, COPPA similarly demands that parents and caregivers look after children's safety in online spaces. Senator Bryan cited the FTC's 1998 survey and pointed out that it had no provision for adult supervision: "less than 10 percent of the sites provide for parental control over the collection and use of [their child's] personal information . . . companies are attempting to build a wealth of information about you and your family without an adult's approval—a profile that will enable them to target and to entice your children to purchase a range of products[41]." Instead of directly regulating content, COPPA instead leverages parents' best judgment to determine what content children can and can't access to mediate risk and ensure age-appropriate online experiences. For operators, COPPA's VPC requirement means they must obtain the parent's consent, as well as a verification of the parents' identity[42].

However, identifying whether the individual providing consent is a child or an adult, or whether that adult is the parent of the child in question has proven difficult for the FTC. COPPA provides various recommendations for VPC techniques, many of which come straight from COPPA's 1998 report:

- Sign a physical consent form and send it back via fax, mail, or electronic scan
- Use a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder
- Call a toll-free number staffed by trained personnel
- Connect to trained personnel via a video conference
- Provide a copy of a form of government issued ID that the operator checks against a database. The identification must be deleted from internal records when the verification process is over.
- Answer a series of knowledge-based challenge questions that would be difficult for non-parents to answer
- Use facial recognition technology to verify a picture of a driver's license or other photo ID submitted by the parent, and then compare that photo to a second photo

While the FTC doesn't require operators to use these methods, most do so anyway as a precautionary measure. Consequently, the primary critiques with the FTC-enumerated methods of VPC include a lack of efficacy and innovativeness that hinder operators from obtaining verifiable parental consent[43]. These criticisms include:

- Security and Privacy Concerns
    - Parents are reluctant to give up sensitive credit card information. They argued doing so exposed them to the same privacy and security risks from which the law sought to protect children. Storing parent's credit cards securely also increases compliance costs for companies, who may be further dissuaded from producing child-directed websites[44]. Introducing new forms of verification such as facial recognition presents similar issues.
- General Noncompliance

    - While some methods were too burdensome to implement, others were easily circumventable. Even in 2000, children would create burner parent email accounts and grant themselves permission for game registration. Other low-tech methods include finding a parent's wallet and entering their credit card number without them knowing.
- Inaccessible
    - Undocumented immigrants may not have government-issued ID, while 8.4 million households lack bank accounts. Hinging a child's ability to use internet services on a parent having ID or a bank account may perpetuate inequality in technology access.
- Lack of Parental Education and Commitment
    - Parents are busy people, and parents who may not understand the nature of data collection may instead seek experiences to occupy their children that are easier to engage with (and more likely than not don't comply with VPC requirements)[45].

Cost, convenience, and security concerns deter online sites and services from creating FTC-adherent VPC methods. High costs associated with implementing COPPA-compliant VPC mechanisms create unnecessarily liability without enhancing children's privacy[46]. Additionally, such measures may be impossible for small businesses to implement given their limited legal and technical resources. If burdensome VPC requirements create barriers to caregivers' awareness of children's online activities, then children are more likely to access general audience websites that may contain unsuitable experiences, which defeats COPPA's very purpose of protecting children's safety online and from deceptive marketing.

E) Perspectives from Abroad

International approaches to children's privacy may offer the US improved solutions to protecting children's privacy. Whereas COPPA employs a parent-centric approach, children's privacy regimes in other countries utilize data minimization, privacy by design, and respect for children's autonomy to protect children online.

Two child-centric data privacy regimes include those in the UK and Ireland. The UK's Age-Appropriate Design Code applies to information society services likely to be accessed by children in the UK. It is the UK's implementation of privacy by design obligations in the UK GDPR, the law distinguishes itself from GDPR's general principle in that it centers children in decision-making, for example by providing prominent, accessible tools to help children exercise data protection and report concerns[47]. Ireland's Equivalent is the Fundamentals for a Child-Oriented Approach to Data Processing ("Fundamentals"). Whereas the Children's Code is more about the engineering and design of products and services, the Fundamentals focuses on data processing in the best interests of children[48]. For example, the Fundamentals state that operators can't bypass their privacy obligations by shutting down services or depriving child users of the full experience.

South Korea demonstrates innovation in verifiable parental consent methods: parents can consent via text, payment, and information authentication through smartphones, which acknowledges the role of smartphones rather than high-friction techniques like physical forms or credit cards in the US. Like Ireland and the UK, Korea's privacy legislation also states that operators must provide clear policies children can understand.

F) Takeaways of VPC and of COPPA

VPC exemplifies existing standards in family law about parent's obligations to protect their children. However, the flaw in COPPA's VPC requirement is misunderstanding the relationship between parents and children in the virtual (rather than the physical) world and underestimating the pace of technological change.

In the early 2000s, VPC failed to meet its purpose of enhancing parents' roles as protectors of their children because the methods proposed were easily circumventable when they were implemented, or so burdensome that some services ignored VPC requirements altogether. In 2022, the rapid expansion of the Internet has disrupted parents' ability to oversee and control kids' online activities. Consequently, VPC alone may not be effective. It's safer to assume that a parents *aren't* with their child when their child is using a device, installing new apps, or making decisions about what content to view, than that they are[49]. If parents aren't present to look over kids' shoulders every time they open their school-issued Chromebook or play on the family tablet in the backseat on a road trip, then website operators should have a responsibility to enhance children's digital literacy, respect children's agency, and provide children safe environments to develop self-sufficiency online. However, parental consent should still be incorporated so that parents provide reasonable supervision and gain a baseline level of awareness of risks such as contact with strangers, inappropriate content, and data collection when children access online platforms. The intention is not to phase out parental supervision, but instead to supplement it with children's self-sufficiency when their parents are not present.

III: Recommendations

A) Technical Recommendations to Improve VPC Methods

Since 2013, the FTC has approved two of six submitted VPC proposals. These proposals are knowledge-based authentication (KBA) in 2013 and face matching to verified photo identification (FMVPI) in 2015. The FTC's primary challenges when approving new VPC proposals include novelty, prematurity, legal sufficiency, and symmetry with COPPA. If a method lacks sufficient research backing up its claim to determine a parent's identity, it is premature. Another proposal the FTC denied was a "Device-Signed Parental Consent form," because the FTC does not consider digital signatures reliable methods of obtaining VPC.

Although ensuring stringent standards for verifiable parental consent can be beneficial, in this case the FTC needs to achieve a better balance. If the costs and inconveniences of verification are too high, and comprehension of the importance of data privacy for children is low, then many families may opt to ignore child-focused services and use general audience products instead. Given how much time children spend online and the quantity of unique websites children access (and not even considering the variety of experiences children access within a single website, like YouTube or Roblox), more realistic VPC mechanisms that parents will realistically follow might better ensure children's safety than idealistic mechanisms that parents ignore.

- Mobile Phones:
    - In South Korea, parents may provide consent via text, payment, information, or authentication through smartphones. Parents may also receive consent confirmation through their phones. Allowing American parents to provide consent via smartphone authentication, text, or mobile payment reduces friction when providing verifiable consent, given that 85% of American adults own smartphones[50]. Although the FTC has denied the use of mobile phones because of

difficulties verifying whether the person providing consent is the parent, incorporating existing features of mobile phones, such as fingerprint, facial recognition, or passcodes may strengthen the security of this mechanism.

- Leverage existing mobile operating systems.
    - Apple and Android already link parent and child accounts through features such as iCloud family. Developers can expand this software interface to allow for child accounts to submit permission requests to parents, again reducing friction and allowing for parents to easily consent anytime, anywhere instead of having to be physically with a child when they are signing up for the platform[51].
    - Utilize trusted third-party game platforms to verify children's age: Google Play Store, App Store, or Roblox Store should flag down young users instead of relying on individual developers (such as an app developer or game designer) to determine whether a user is underage. Such a measure would be amenable to parents, as it reduces the burden of parents having to provide age verification on a service-by-service basis. Providing verification once to a trusted large third party like the App Store may increase the supply of child-focused products, by placing the burden of obtaining VPC on large, well-resourced companies such as Google, Apple, or Roblox rather than individual app developers, Youtubers, or game designers[52]. Additionally, this action can ensure that children's access to general-audience apps in the first place is minimized, as many children first gain exposure to general audience or mature apps through the Android and Apple app stores[53].

B) Proposed Revisions to COPPA:

That said, relying on VPC alone to protect children online is inadequate. COPPA should include other measures that provide a second line of defense for children if VPC–even VPC that is better utilized – alone is ineffective. The most effective way to do so is to grant children, in addition to their parents, the tools to control collection of their own data and understand the implications of their online activity. Given widespread research that children discover new websites and services independently, adopting a non-paternalistic framework that embraces children's autonomy and digital savvy may achieve Senator Bryan's original ideals of developing children's digital literacy and enhancing their self-sufficiency online.

i) Require VPC beyond personal data collection:

Roblox does not track customers over time or across third party websites to provide targeted advertising (according to its privacy policy), so the collection of personal information may seem less pertinent. Roblox only asks for users' birthday and parent's email to validate the account, and does not ask the child's name, email address, or physical address. However, just because Roblox does not collecting personal information from children, and just because it doesn't use 3rd party advertising, does not mean that the platform cannot better utilize verifiable parental. Its privacy policy states that "Parents are responsible and will supervise and be solely responsible for your child's use of Roblox," and Roblox recommends but does not require parents to consent before children use the service[54]. This means children could enter age-inappropriate experiences without their parents' knowledge and protection. Modifying the parental consent requirement to include signing up for platforms that have risks of interactions with general audience content could resolve this issue. This measure can both teach children how to stay vigilant online while also allowing parents to verify the child's age as COPPA originally

intended. Truthful age representation then enables Roblox to better mediate interactions between children and adults by separating the two populations, such as by preventing young users from accessing age-rated games. One could argue that children would still be able to stumble into age-inappropriate games, given the inadequacy of Roblox's recommendation algorithm and moderation system (just 400 human moderators[55] for 50 million ever-changing experiences). Platform responsibility and content moderation, however, are outside the scope of this paper.

ii) Require adequate notice to parents and children:

Operators must provide children, teenagers, and parents adequate notice of the uses of personal information online and a meaningful opportunity to consent to those practices. For example, a new COPPA could require informed notice and consent in a manner that ensures maximum possible comprehension before any collection, use, or disclosure of personal information. This puts the burden of fair information practice on websites, instead of exclusively on parents.

For example, website operators must adopt creative mechanisms to ensure that the child and parent's consent are fully informed through age-appropriate techniques. For adults, a website might have the adult click through a slideshow of the privacy policy in simple English rather than scrolling through a page of legalese and checking a box. Children, as determined by inputted birthday, could instead view an animated video describing safety best practices and reminding the child to get their parent's consent in child-friendly language before entering the game. These solutions advance COPPA's goal of protecting children via a holistic framework. Informed consent from the operator complements parents' existing responsibilities under verifiable parental consent, and children who enter platforms that house millions of varied experiences like Roblox will better understand in-game policies surrounding data collection, interactions with other players, and engaging with age-appropriate content or reporting inappropriate general-audience content as they navigate the different worlds within the platform with or without their parents.

iii) Modify COPPA's definition of personal information:

Revisiting KidsCom illustrates the importance of relevant, up-to-date definitions of personal information. In 1998, COPPA defined personal information as (A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or the parents of the child that the website collects online from the child and combines with an identifier described in this paragraph. Lawmakers were concerned that giving up these specific pieces of information would lead to dangers such as harassment from 3rd party marketers or interactions with child predators.

However, the differences between the regulatory and Internet landscape in 1998 and present day are stark. While KidsCom and Roblox are both interactive virtual worlds popular with children, KidsCom illegal collection of personal information entailed asking users to submit personal information. In this case, having a parent looking over the child's shoulder on the family MacIntosh may have prevented the improper collection of data. Today, however, websites collect all types of information from their users such as location data based on your SIM card and IP addresses and GPS, data sent from in-app messages, metadata from uploaded content, the app and file names of the user's device, battery state and keystroke patterns and rhythms[56], in

ways that even parents might not understand, let alone prevent. Thus, the mechanisms that COPPA promotes for children's safety online are not adequate.

More importantly, the platform's misuse of the information, rather than the third-party marketer's use, has become more concerning to some parents. Understanding parent concerns with Fortnite, a related game, underscores the importance of potentially placing prohibitions on behavioral data that may foster addictive behaviors[57]. The more people play Fortnite, the more data they generate. This data provides key insights to game designers about what captivates players the most and what drives players to quit, and feeds machine learning algorithms designed to amplify player engagement and keep kids hooked on the game[58]. The use of personal data to increase kids' time on platforms like Fortnite does the exact opposite, by making parents feel powerless to protect their children against addiction. Prohibiting platforms not only from distributing personal information to third party advertisers, but also from using personal data against the best interests of young users is relevant to the original intent of COPPA: to increase parental involvement in children's online engagements, as parents hold their children's best interests.

Similarly, Roblox uses machine learning to power recommendation and search systems that drive Roblox content distribution and deliver kids a customized stream of exciting games. To protect children's safety, prevent video game addiction, and center children's wellbeing, the FTC should investigate whether the definition of personal information should be expanded to include children's in-game behaviors that aren't linked traditionally defined personal information, and whether personal information should also be restricted for internal advertising or machine learning algorithms with a discernible harm to children's self-control or psychology. Prohibitions on using user data (that may not be personally identifiable information) so that parents are more in control of their children's interactions online, as COPPA was designed to fulfill.

IV: Metaverse Implications

Roblox is significant because of its ubiquity among children and because of the implications of its popularity. More than 50% of Roblox's users are under 13[59]. Given Roblox's enormous popularity among kids in the US, changes to its privacy policies will have an outsize impact on children's privacy, like how Apple's privacy policies, such as its controversial anti-child porn scanning program[60], have an outsize effect on adult privacy. As one of the most influential metaverse companies, Roblox's changes to privacy policy may cause a ripple effect in the industry at large to the betterment or detriment of children's safety online.

Although it is not a fully metaverse company, understanding the safety and privacy concerns on this platform can inform policy decisions as the metaverse evolves. While the platform does not yet support the integration of the physical and virtual worlds with equipment such as VR headsets or biometric monitors, Roblox exemplifies many other features of a metaverse. It is a persistent, multi-user, shared virtual space that real-life users inhabit as avatars[61]. Avatars interact with other avatars, items, apps, services, and even businesses. While this next evolution of the internet and its incorporation of virtual and augmented reality technology presents exciting opportunities for new means of physical, digital, social networking, it will also unleash unforeseen privacy and security concerns. For example, the median Roblox user visited 40 unique experiences[62]–under COPPA in its current form, would a parent have to consent each time a child tries to enter a new world? Such a requirement defeats the purpose of a metaverse in the first place: quick, easy, seamless access between virtual worlds. Should

"personal data" also include text from in-game chats or a user's Robux purchase history? Studying practices that improve the privacy and safety of children within Roblox's platform may inform design and engineering decisions to ensure rich, age-appropriate online experiences that center children's well-being in the third major iteration of the Internet.

The immersive nature of the metaverse and the interoperability of its virtual experiences increases the quantity and quality of its privacy and safety threats. If more and more interpersonal communication and everyday activity migrates online, platforms gain access to even more behavioral and communication data[63]. Perhaps metaverse companies will collect information on real and virtual responses to the surrounding environment, such as avatar gait, pupil movement, and physiological responses such as heart rate. If a platform detects that a young user's heart rate changes more than the average user's in response to a friendly game of chess in the community square, perhaps it will recommend the user visit a virtual arcade, where the user will more likely purchase more in-game currency. For children, inadequate regulations could be even more concerning because research on the developmental consequences of these threats is limited[64]. For example, cyberbullying can become more intense: instead of just words and pictures, VR interactions include contextual details: when, where, and how. Harassment in VR could combine the anonymity of cyberbullying and the "he-said, she-said" nature of real-life bullying. Without policy changes, children may become the unwitting victims of these tectonic shifts on the Internet, as they did from the transition of Web1.0 to Web2.0. For example, internal reports from whistleblower Frances Haugen reveal how Instagram caused tangible harm to teen girls' mental and physical health for years. Without proactive policies that mediate the transition from traditional social networking to immersive metaverse-oriented services, the earliest adopters of these technologies–children–may again suffer the harshest blows to their privacy, safety, and development.

V: Conclusion

Some of the primary dangers on Roblox include contact with child predators, access to age-inappropriate media, and video game addiction. However, parents often are not aware of this problem because children can create Roblox accounts without parental consent (no parent email is necessary). Additionally, Roblox does not verify the age that children enter when they create accounts. One way to keep children safe from these harms is to ask for parental consent to them being on the platform while also asking the parent to verify the child's age. These measures help parents can lay the groundwork for safe Internet behavior, understand the risks inherent in general audience platforms, consent to data collection policies. Asking for verifiable parental consent before accessing the platform also facilitates truthful age verification, which can support a platform's internal efforts to deliver content to the right audiences. However, current verifiable parental consent is only required when it comes to collecting a limited subset of children's data under 13 under COPPA. When the law was passed, lawmakers assumed that the primary source of danger to children's safety and privacy would be the collection of personally identifiable information such as names, addresses, and passwords, and primary dangers could include unwelcome advertiser spam email and contact by child predators. In contrast, primary concerns with children's physical safety are often shadowed by worries with regarding children's right to self-development independent of advertiser or platform influence[65], video game addiction, and disruptions to children's mental and emotional development due to unwelcome intrusions of sexual or general audience content that falls through the cracks of an inadequate moderation system.

But children's online safety and privacy legislation is limited in scope and thus ineffective against such problems. COPPA only governs the collection of personal information such as name, address, email address, and age of children under 13. It requires operators who do so to collect verifiable parental consent from the child's parent and enumerates methods for obtaining verifiable parental consent. However, COPPA's reliance on parents to monitor children's online interactions is not tenable for the present day, given that digitally native children access the Internet independently, and given that the metaverse and other "world within a world" increases the difficulty for parents to watch over and consent to every new online interaction that collects data.

Thus, for COPPA to be effective against both present and future threats, Congress must revise the VPC requirement, broaden the definition of personal data, and include provisions to prioritize children's agency and decision making. First, VPC should be required for users under 12 to create accounts on platforms with risks of data collection, general audience content, and interactions with people of all ages. To increase the likelihood that platforms utilize VPC, the FTC should embrace and approve 21st-century technologies, especially smartphones. Additionally, personal information should include behavioral data, communication patterns, and biometric data, even data points untethered to the personal information, because advertisers and platforms can create detailed profiles of children and hyper-specific content recommendations without PII. Finally, COPPA must include privacy fortifications when children navigate the Internet without their parents. It should do so by providing for informed notice and consent to both children and parents. Ultimately, COPPA should be revised to reflect the fluid, dynamic relationship between children, their parents, and the Internet. Parents have the responsibility to protect their children, and parents may be better able to understand the implications of novel modes of data collection. However, children may be more comfortable using and exploring new websites and mediums. Updating COPPA's definitions and scenarios will better protect children in the present, but empowering children with the tools to understand their digital rights and responsibilities positions them to become responsible Internet stewards in Roblox and beyond.

[1] "Children's Privacy." Federal Trade Commission. Federal Trade Commission, February 11, 2022. https://www.ftc.gov/business-guidance/privacy-security/childrens-privacy.

[2] Fischer-Baum, Reuben. "What 'Tech World' Did You Grow up in?" The Washington Post. WP Company, November 26, 2017. https://www.washingtonpost.com/graphics/2017/entertainment/tech-generations/.

[3] Hersch, Melanie L. "Is COPPA a Cop Out? The Child Online Privacy Protection Act As Proof That Parents, Not Government, Should Be Protecting Children ' s Interests on the Internet." *Fordham Urban Law Journal*, 4, 28, no. 6 (2001). https://ir.lawnet.fordham.edu/.

[4] Maheshwari, Sapna. "On YouTube Kids, Startling Videos Slip Past Filters." The New York Times. The New York Times, November 4, 2017. https://www.nytimes.com/2017/11/04/business/media/youtube-kids-paw-patrol.html.

[5] McKinnon, John D. "Lawmakers Seek Tougher Online Safety Standards for Children." The Wall Street Journal. Dow Jones & Company, February 16, 2022. https://www.wsj.com/articles/lawmakers-seek-tougher-online-safety-standards-for-children-11645009201.

[6] "Most Visited Websites - Top Websites Ranking for March 2022." Similarweb. Similarweb LTD 2022, March 2022. https://www.similarweb.com/top-websites/.

[7] Lyles, Taylor. "Over Half of US Kids Are Playing Roblox, and It's about to Host Fortnite-Esque Virtual Parties Too." The Verge. The Verge, July 21, 2020. https://www.theverge.com/2020/7/21/21333431/roblox-over-half-of-us-kids-playing-virtual-parties-fortnite.

[8] "A Year on Roblox: 2021 in Data." Roblox Blog. Roblox, January 26, 2022. https://blog.roblox.com/2022/01/year-roblox-2021-data/.

[9] Breen, Kerry. "Experts, Users Warn about Explicit Content on Roblox." TODAY.com. TODAY, October 20, 2021. https://www.today.com/parents/roblox-experts-users-warn-about-inappropriate-content-t235027.

[10] Jargon, Julia. "Roblox Struggles with Sexual Content. It Hopes a Ratings System Will Address the Problem." The Wall Street Journal. Dow Jones & Company, April 21, 2021. https://www.wsj.com/articles/roblox-struggles-with-sexual-content-it-hopes-a-ratings-system-will-address-the-problem-11618660801.

[11] Smith, Mary. "Man Accused of Rape, Trafficking Girl He Met on Roblox." https://www.foxcarolina.com. Gray Television, Inc., March 3, 2022. https://www.foxcarolina.com/2022/03/03/man-accused-rape-trafficking-girl-he-met-roblox/.

[12] Mitchell, Heidi. “Are Virtual Worlds Safe for Children?” The Wall Street Journal. Dow Jones & Company, February 26, 2022. https://www.wsj.com/articles/are-virtual-worlds-safe-for-children-11645880401?mod=ig_technologyreport.

[13] Pietro, Roberto & Cresci, Stefano. (2021). Metaverse: Security and Privacy Issues. 10.1109/TPSISA52974.2021.00032.

[14] Rep. *THE COMMON SENSE CENSUS: MEDIA USE BY KIDS AGE ZERO TO EIGHT*. Common Sense Media, 2017. https://www.commonsensemedia.org/sites/default/files/research/report/csm_zerotoeight_fullreport_release_2.pdf.

[15] “FTC | The Future of the COPPA Rule: An FTC Workshop Part 1: Oct 7, 2019.” FTC, 2019.

[16] Courtney K. Blackwell et al., Children and the Internet: Developmental Implications of Web Site Preferen ces Among 8- to12-Year-Old Children, Journal of Broadcasting & Electronic Media, 58:1,1(Feb. 28, 2014),http://dx.doi.org/10.1080/08838151.2013.875022.

[17] Jun Zhao et al., “I Make Up A Silly Name’”: Understanding Children's Perception of Privacy Risks Online in CHI 19: Proc. of the 2019 CHI Conf. on Hum. Factors in Computing Sys. 1, 3 (2019),

[18] De Abreu, Andreina. “Is Behavioral Data Private Information?” Netquest. Netquest, October 28, 2019. https://www.netquest.com/blog/en/is-behavioral-data-private-information#:~:text=Do%20behavioral%20data%20violate%20privacy,or%20regulation%20in%20the%20world.

[19] *FTC | The Future of the COPPA Rule: An FTC Workshop Part 1*. *Ftc.gov*. Federal Trade Commission, 2019. https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_part_1_1.pdf.

[20] Rep. *THE COMMON SENSE CENSUS: MEDIA USE BY KIDS AGE ZERO TO EIGHT*. Common Sense Media, 2017. https://www.commonsensemedia.org/sites/default/files/research/report/csm_zerotoeight_fullreport_release_2.pdf.

[21] Mikhael, Mark. “COPPA: The Privacy Law That Wasn't .” *Law Student Scholarship Seton Hall Law*, 2021. https://scholarship.shu.edu/student_scholarship/.

[22] Breen, Kerry. “Experts Issue Warning to Parents over Hidden Explicit Content on Popular Gaming Platform.” 7NEWS. 7NEWS, October 23, 2021. https://7news.com.au/technology/experts-and-users-warn-about-explicit-content-on-popular-gaming-platform-roblox-c-4303308.

[23] Jargon, Julia. “Roblox Struggles with Sexual Content. It Hopes a Ratings System Will Address the Problem.” The Wall Street Journal. Dow Jones & Company, April 21, 2021. https://www.wsj.com/articles/roblox-struggles-with-sexual-content-it-hopes-a-ratings-system-will-address-the-problem-11618660801.

[24] Children‘s Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2006); FTC, FILE NO. 954,4807, PRIVACY ONLINE: A REPORT TO CONGRESS (1998) [hereinafter PRIVACY ONLINE REPORT], available at http://www.ftc.gov/reports/privacy3/toc.shtm.

[25] “The Federal Trade Commission Updates to the Coppa Faqs.” Future of Privacy Forum. Future of Privacy Forum, October 21, 2020. https://fpf.org/blog/ftc-updates-coppa-faqs/.

[26] Staff, InformationWeek. “How Coppa Came About.” InformationWeek. Informa PLC, January 14, 2004. https://www.informationweek.com/it-life/how-coppa-came-about.

[27] Rep. *THE STATE OF PLAY: Verifiable Parental Consent and COPPA*. Future of Privacy Forum, November 2021. https://fpf.org/wp-content/uploads/2021/11/FPF-The-State-of-Play-Verifiable-Parental-Consent-and-COPPA.pdf.

[28] Mikhael, Mark. “COPPA: The Privacy Law That Wasn't .” *Law Student Scholarship Seton Hall Law*, 2021. https://scholarship.shu.edu/student_scholarship/.

[29] 105 Cong. Rec. S8482 (July 17, 1998).

[30] Hersch, Melanie L. “Is COPPA a Cop Out? The Child Online Privacy Protection Act As Proof That Parents, Not Government, Should Be Protecting Children ' s Interests on the Internet.” *Fordham Urban Law Journal*, 4, 28, no. 6 (2001). https://ir.lawnet.fordham.edu/.

[31] *Ibid.*

[32] *Ibid*.

[33] *Ibid.*

[34] Hersch, Melanie L. “Is COPPA a Cop Out? The Child Online Privacy Protection Act As Proof That Parents, Not Government, Should Be Protecting Children ' s Interests on the Internet.” *Fordham Urban Law Journal*, 4, 28, no. 6 (2001). https://ir.lawnet.fordham.edu/.

[35] Federal Sites Breaching Children's Privacy Law, DALLAS MORNING NEWS, Oct. 7, 2000, at 3F.

[36] Chakravorti, Bhaskar. “Why It's so Hard for Users to Control Their Data.” Harvard Business Review. Harvard Business Review, January 30, 2020. https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data.

[37] Rep. *THE STATE OF PLAY: Verifiable Parental Consent and COPPA*. Future of Privacy Forum, November 2021. https://fpf.org/wp-content/uploads/2021/11/FPF-The-State-of-Play-Verifiable-Parental-Consent-and-COPPA.pdf.

[38] "Does Data Anonymization Really Hide Your Identity?" Duke's Fuqua School of Business. Duke University's Fuqua School of Business, April 6, 2022. https://www.fuqua.duke.edu/duke-fuqua-insights/jiaming-xu-does-data-anonymization-really-hide-your-identity.

[39] Maheshwari, Sapna. "On YouTube Kids, Startling Videos Slip Past Filters." The New York Times. The New York Times, November 4, 2017. https://www.nytimes.com/2017/11/04/business/media/youtube-kids-paw-patrol.html.

[40] Cobb, Stuart. "It's Coppa-Cated: Protecting Children's Privacy in the Age of YouTube: Published in Houston Law Review." Houston Law Review. Scholastica, April 19, 2021. https://houstonlawreview.org/article/22277-it-s-coppa-cated-protecting-children-s-privacy-in-the-age-of-youtube.

[41] 105 Cong. Rec. E1861 (Oct. 1, 1998)

[42] *Ibid.*

[43] *Ibid.*

[44] *Ibid.*

[45] *Ibid.*

[46] Federal Trade Commission, Public Submission, Comments of the Family Online Safety Institute (March 22, 2020), https://www.regulations.gov/comment/FTC-2019-0054-113172.

[47] Information Commissioner's Office, Code Standards, Age-Appropriate Design: A Code of Practice for Online Services, https://ico.org. uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/ code-standards/.

[48] Data Protection Commission, Fundamentals for a Child-Oriented Approach to Data Processing: Draft Version for Public Consultation (December 2020), https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf.

[49]"FTC | The Future of the COPPA Rule: An FTC Workshop Part 1: Oct 7, 2019." FTC, 2019.

[50] "Mobile Fact Sheet." Pew Research Center: Internet, Science & Tech. Pew Research Center, November 23, 2021. https://www.pewresearch.org/internet/fact-sheet/mobile/.

[51] Federal Trade Commission, Public Submission, Princeton University's Center for Information Technology Policy COPPA Rule Comments (March 25, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116874

[52] Federal Trade Commission, Public Submission, Comments of the Developers Alliance, COPPA Rule Review (December 9, 2019), https:// www.regulations.gov/comment/FTC-2019-0054-21655.

[53] "FTC | The Future of the COPPA Rule: An FTC Workshop Part 1: Oct 7, 2019." FTC, 2019.

[54] "Roblox Privacy Policy August 2021." San Mateo: Roblox Corporation, August 2021.

[55] "Understanding Moderation Messages - Roblox Support." Roblox Blog. Roblox Corporation, January 19, 2021. https://en.help.roblox.com/hc/en-us/articles/360020870412-Understanding-Moderation-Messages.

[56] Perez, Sarah. "Tiktok Just Gave Itself Permission to Collect Biometric Data on US Users, Including 'Faceprints and Voiceprints'." TechCrunch. TechCrunch, June 3, 2021. https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collect-biometric-data-on-u-s-users-including-faceprints-and-voiceprints/.

[57] Needleman, Sarah E. "Videogame Developers Are Making It Harder to Stop Playing." The Wall Street Journal. Dow Jones & Company, August 22, 2018. https://www.wsj.com/articles/wheres-the-off-switch-videogame-developers-are-making-it-harder-to-stop-playing-1534757400.

[58] Morris, Betsy. "How Fortnite Triggered an Unwinnable War between Parents and Their Boys." The Wall Street Journal. Dow Jones & Company, December 23, 2018. https://www.wsj.com/articles/how-fortnite-triggered-an-unwinnable-war-between-parents-and-their-boys-11545397200.

[59] Kastrenakes, Jacob. "Roblox Will Start Verifying the Age of Teenage Players." The Verge. The Verge, September 21, 2021. https://www.theverge.com/2021/9/21/22684672/roblox-age-verification-optional#:~:text=More%20than%20half%20of%20Roblox's,second%20quarter%20of%20the%20year).

[60] Kan, Michael. "Apple Delays Controversial Anti-Child Porn System for IPhones." PCMAG. PCMag, September 3, 2021. https://www.pcmag.com/news/apple-to-delay-implementing-anti-child-porn-system-for-iphones.

[61] Pietro, Roberto & Cresci, Stefano. (2021). Metaverse: Security and Privacy Issues. 10.1109/TPSISA52974.2021.00032.

[62] "A Year on Roblox: 2021 in Data." Roblox Blog. Roblox, January 26, 2022. https://blog.roblox.com/2022/01/year-roblox-2021-data/.

[63] Zhao, Ruoyu, Yushu Zhang, Youwen Zhu, Rushi Lan, and Zhongyun Hua. "Metaverse: Security and Privacy Concerns." arXiv preprint arXiv:2203.03854 (2022).

[64] Mitchell, Heidi. “Are Virtual Worlds Safe for Children?” The Wall Street Journal. Dow Jones & Company, February 26, 2022. https://www.wsj.com/articles/are-virtual-worlds-safe-for-children-11645880401?mod=ig_technologyreport.

[65] Growing up in a connected world, UNICEF Office of Research – Innocenti, Florence, 2019.