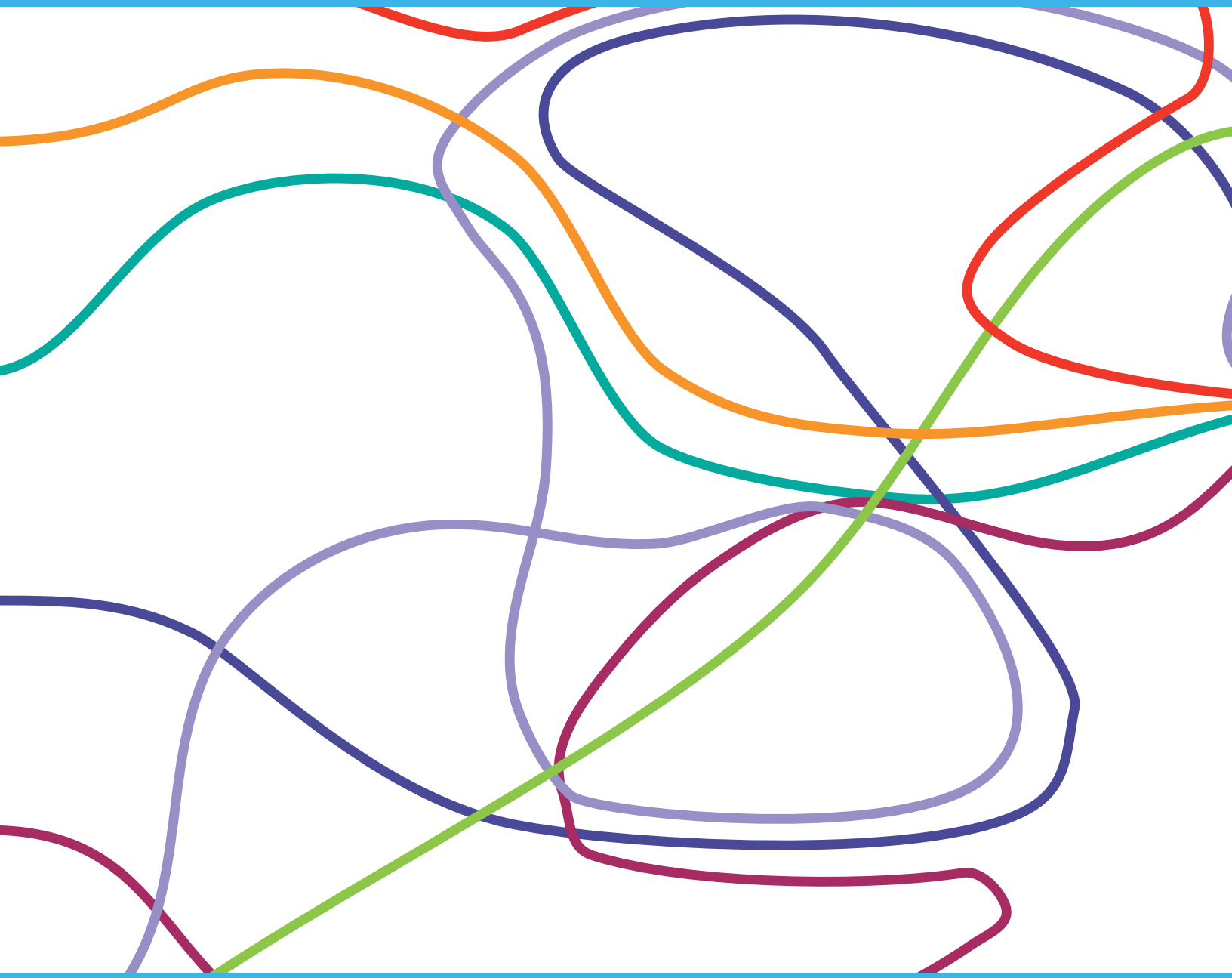
THE STATE OF PLAY: Verifiable Parental Consent and COPPA

DISCUSSION DRAFT



NOVEMBER 2021

FUTURE OF PRIVACY FORUM

Executive Summary

Children's online data privacy protections in the United States developed in response to concerns about risks to children's safety and wellbeing, including exposure to data practices that commercialize children's data, child predation, and age-inappropriate content. In 1998, lawmakers sought to put parents in control of how their children engaged with the internet by enacting COPPA, the Children's Online Privacy Protection Act. COPPA requires that operators subject to the law obtain ***verifiable parental consent*** before collecting personal information online from children under 13, with certain exceptions.

This approach is intended to have several benefits: it provides baseline protections for kids; enables parents to tailor online experiences to their particular child's needs rather than mandating identical treatment for all children based on age; encourages online firms to offer services to adults, children, or both; and sets reasonably clear rules for services aimed at kids. However, COPPA's reliance on verifiable parental consent has elicited critiques: Stakeholders from industry, academia, and civil society argue that: it can be difficult to distinguish between kids and adults online; it is harder still to establish whether a particular child is related to a particular adult, to say nothing of the nature of the relationship; parental consent mechanisms often exclude some families from online services; some parents are reluctant to provide financial or ID information that is required for some verification mechanisms to function properly; the costs and inconvenience of verification can lead families to abandon child-focused services for riskier general audience products; and these costs can spur tech firms to provide less robust offerings to children or spurn youth-directed services altogether.

The Federal Trade Commission has approved certain mechanisms for obtaining verifiable parental consent, and in the decades since COPPA's passage, online sites and services rely on those approved mechanisms to ensure they appropriately obtain verifiable parental consent. However, these approved mechanisms do not come without challenges and emerging technologies and policy frameworks may provide an opportunity to augment or modify consent requirements.

While much attention has been given to COPPA and its challenges more broadly, the challenges surrounding verifiable parental consent have been less explored. This discussion draft seeks to outline the existing landscape of verifiable parental consent in practice. To better understand the policy considerations underpinning the verifiable parental consent requirement, the draft begins by providing an overview of COPPA's history, introduction, and passage. The draft then explores international approaches to regulating children's data privacy, to understand how alternative

Executive Summary

developed in the wake of COPPA, as well as the tensions in reconciling those alternative approaches. Then, the draft explains COPPA's framework, the verifiable parental consent requirement, and existing approved mechanisms. After providing this overview, the draft summarizes challenges and solutions raised by stakeholders regarding the implementation and effectiveness of verifiable parental consent.

Informed by research and insights from parents, industry leaders, advocates, and academics, this discussion draft highlights key friction points that emerge in the verifiable consent process, including:

- Efficancy
- Accessibility
- Hesitancies, Privacy, and Security
- Convenience and Cost Barriers

This discussion draft is the first piece of FPF's in-depth exploration into verifiable parental consent. The suggested solutions offered in the draft are a non-exhaustive list developed through FPF's research and insights from stakeholders. Because this white paper is a discussion draft, we intend to develop the challenges and perspectives outlined, which will ultimately inform solutions, including a forthcoming set of best practices for industry stakeholders seeking to provide children with safe, privacy-protective experiences. We invite collaboration and input from all involved stakeholders, including parents, advocates, academia, industry, regulators, and policymakers.

It's hard to get VPC right!

Is it even worth it to develop experiences for kids?

Operator designs experience for kids and chooses VPC method

ADULT DESIGN

Operator abandons design

Child accesses experience online

DAD! Can I play this game?

Parent notified & VPC triggered

Signed Form

Print form, complete information and return by mail, fax or scan

Phone Call

Call a toll free number

Video Conference

Connect via video conference to a call center

Photo Comparison

Provide scan of Government ID and second photo taken with a phone or web camera for comparison and validation via facial recognition

Database

Provide Government ID identifier (Driver's license ID number or SSN) for validation against a database

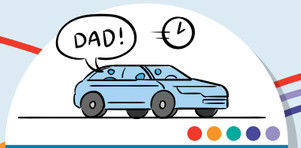
Credit/Debit Card

Provide credit/debit card number, bank processes a small monetary transaction (in US) to verify card holder identify.

Knowledge-Based Questions

Answer a set of knowledge-based questions pulled from publicly available information (ie: In what city were you born?)

PARENT FRICTION POINTS



CONVENIENCE

Time investment and/or tools required become "too much"

EFFICACY

This does not always produce appropriate results and leads to frustration

ACCESSIBILITY

Not all parents have equal or easy access to the tools required

HESITANCIES

The method gives parents pause. "Why do you need this info?"

SECURITY / PRIVACY

Concern with providing this personal information to unkown service providers

POSSIBLE OUTCOMES

Child plays with permission

Adult Provides Consent

Approved methods confirm adult status, not parent relationship

Child lies about age, and potentially accesses age-inappropriate content

VPC Abandoned

Child prevented from engaging with an online experience

LET'S SOLVE THIS!

FPF is calling on industry, advocates, and academics to help identify possible solutions to untangle these challenges and remove friction from the VPC flow.

Suggestions for improvements, mechanisms, and methods include incorporating the use of mobile phones for greater flexibility, leveraging major platforms to facilitate compliance, considering alternatives to credit cards, and exploring emerging technologies including implementing age assurance tools.

TABLE OF CONTENTS

TABLE OF CONTENTS

Introduction: Why Verifiable Parental Consent?

Historically, concerns for children's safety and well-being online have driven American legislative and regulatory approaches to children's data protection and privacy. These concerns have led policymakers to position parents and caregivers as intermediaries who provide consent to certain online data practices related to their children's information. In the United States, the Children's Online Privacy Protection Act[1] (COPPA) requires an operator of a commercial online service directed to children under 13 (or with actual knowledge that it has collected personal information from children under 13) to provide parents with detailed, direct notice and to obtain their affirmative express consent—verifiable parental consent (VPC)—prior to the operator's collection of a child's personal information.

COPPA does not regulate online content specifically. The purpose of VPC is to give parents control over their children's data and what their children access in order to mitigate risks to children online and ultimately ensure age-appropriate experiences for them. Without VPC, these desired outcomes prove difficult to achieve. Although VPC has been legally required since COPPA's enactment in 1998, those subject to the law have faced challenges in its implementation. These challenges risk undermining the VPC requirement and could introduce new risks to children online. As the Federal Trade Commission (FTC) conducts its COPPA Rule review and legislators continue to introduce bills that would update COPPA or create new children's privacy frameworks, this white paper seeks to inform those efforts by exploring the current status of VPC and identifying opportunities to improve VPC mechanisms, in terms of their 1) efficacy; 2) accessibility; 3) associated mental barriers related to privacy and security; and 4) convenience and cost barriers. This report can also inform future approaches to protecting children online.

Children Today Are Increasingly Connected

The internet has become a staple in the lives of American children. According to a survey conducted by Common Sense Media in 2020, children from birth to age eight in the United States engage in about two-and-a-half hours of "screen media" per day on average.[2] Internet use became essential during the COVID-19 pandemic and the social isolation that ensued. During the pandemic, children needed to use the internet to communicate; keep in touch with their friends, families, and teachers; and maintain their social skills.[3]

From education to gaming to art, the landscape of children's online products has expanded in recent years. Children interact with various types of products: mobile applications, including gaming and creation applications; extended reality experiences; edutainment; and other devices within the Internet of Things (IoT) directed to children. However, recent studies have shown that children are heavily connected online, even through media not explicitly directed to children; they also use their parents' devices.[4] This section explores the many media through which children connect to the internet and popular methods of their engagement online. This brief exploration is necessary to gain an understanding of the online access points children engage with.

A recent study from the Family Online Safety Institute (FOSI) indicates that most children are heavily connected to the internet. Of the parents participating in the study, 45 percent indicated that their children have three or more of their own personal connected devices.[5] An additional 42 percent of parents reported that their children have two or more of their own connected devices.[6] Parents most likely to report having children with three or more of their own devices included those "with children age nine to 12 (61%), parents of color (53%), those with household incomes over $75,000 (51%), those with some college education (50%), and Millennials (49%)."[7]

While many children have their own connected devices, most children have access to connected devices. Most parents (67 percent) reported that their child has their own tablet computer or iPad, and some parents reported that children have access to a tablet computer or iPad (22 percent).[8] For cell phones and tablets, 36 percent of parents indicated their child had their own device, and 53 percent indicated their child had access to one of these devices; for desktop or laptop computers, 29 percent of parents reported that their child had their own, and 67 percent reported that their child had access; for video game consoles, 50 percent of parents reported their child has their own device, and 33 percent reported their child had access; for wearable devices, 10 percent of parents reported their children have their own, and 21 percent have children who have access; and the children of 31 percent of participating parents own connected toys, and the children of 4 percent of participating parents have access.[9]

In addition to using their own personal connected devices, children use other connected technology and devices in their households. The FOSI study identified connected or smart TVs and internet-connected speakers as the connected devices that children most commonly use. A majority of parents participating in

the study own connected or smart TVs (67 percent). Of parents who own a smart TV, 96 percent indicated that their child uses it. Of parents who own a voice-controlled, internet connected speaker (23 percent), 94 percent reported that their child uses it. Parents even reported that their children use devices such as their internet-enabled thermostats and internet-enabled security systems; 67 percent of parents who own internet-enabled devices and 64 percent of parents who own internet-enabled security systems devices reported that their children use the devices.

The ways that children use the internet are as varied as the media through which they access it. Some children have their own social media accounts, such as Snapchat or TikTok, or their own email accounts.[10] Over 80% of children aged 3-11 spend time watching videos on YouTube,[11] which has dedicated an entire area of its platform to content for children. Gaming and mobile gaming are also popular uses of the internet among children: in 2020, mobile gaming for those between the ages of two and 12 increased by 9 percent in comparison to 2019.[12] Augmented reality (AR), virtual reality (VR), and mixed reality (MR) digital experiences—collectively referred to as extended reality (XR)—are popular internet uses for children and are typically associated with gaming due to their potential for experiential play. Additionally, according to Deloitte, the "market for educational XR is poised to be among the fastest-growing XR segments over the next few years," and overall XR headset sales are projected to increase "by 100 percent in 2021 over 2019 levels."[13] Beyond gaming, children often turn to applications offering simulated experiences that allow them to explore different social scenarios—in settings ranging from hair salons to the kitchen.[14]

Children today are heavily connected. With this increase in connectivity comes the potential for an increase in data collection. Although concerns remain about children's well-being, safety, and privacy, parents and educational institutions alike have embraced the use of connected technology to engage and empower children. As children's lives increasingly play out online, parents, policymakers, consumer advocates, and industry stakeholders need to understand the current protections for children online and whether those protections effectively safeguard children while empowering children's rights and agency.

How We Arrived at the Current State of Play

In the United States, the prevailing approach to regulating children's internet behavior is to ensure that parents or caregivers mediate their children's online interactions. The FTC's COPPA enforcement reflects a social and political demand for parental supervision to ensure that children are safe on the internet.[15] However, there is no robust digital identity system for the internet—there is no one, simple method for identifying whether a website or service user is a child or an adult, let alone identifying whether an individual providing consent is the parent of a child user. To fill this gap, a variety of VPC techniques and technologies have emerged.

To better frame the current state of VPC and the challenges regarding its mechanisms, it is important to outline the legal and historical context of COPPA and its VPC requirement. This section briefly explains the legal and historical context of privacy frameworks in the United States, theoretical underpinnings of the country's approach to children's privacy rights, the history and current state of COPPA, and the history of COPPA enforcement.

The 1970s: Data Privacy in an Increasingly Computerized World

In response to the increased "computerization of information" and public concerns about the federal government amassing data on citizens, policymakers and regulators began introducing significant data privacy regulations and frameworks.[16] These early data privacy developments have influenced much of the nation's approach to consent-based data collection and use, especially the structuring of U.S. children's privacy protections around parental consent. This section provides an overview of the key data privacy frameworks introduced during a period fraught with these concerns.

Three data privacy frameworks introduced during this period are the Fair Information Practice Principles (FIPs), The Federal Privacy Act of 1974, and the Family Educational Rights and Privacy Act (FERPA). These frameworks laid the groundwork for subsequent children's privacy protections: the FIPs introduced the importance of informing data subjects about how their information was used and empowering them to consent to use of their data; the Federal Privacy Act was the first to codify these principles; and FERPA introduced the concept of the parent providing consent to how their children's data is shared.

In 1973, the Department of Health, Education, and Welfare (HEW) published a report analyzing citizens'

rights regarding the government's increased data collection. This report introduced "The Fair Information Practice Principles" (FIPs), a framework that has "played a significant role in framing privacy laws in the United States" and around the world.[17] The report recommended the institution of a code of practices:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[18]

The FIPs laid the foundation for the Federal Privacy Act of 1974, enacted just one year after the HEW report's publication.[19] The Privacy Act builds on the FIPs by enacting practices governing the collection, maintenance, use, and disclosure of information about individuals and maintained by federal agencies.[20] The act requires agencies to notify the public of their systems of records in the Federal Register, allows individuals to seek access to and amend their records, and establishes various agency record-keeping requirements.[21] The act also prohibits the disclosure of an individual's record from a system without the individual's written consent, unless a statutory exception requires the disclosure.[22]

Also in 1974, lawmakers enacted the Family Educational Rights and Privacy Act to protect the privacy of education records.[23] Lawmakers introduced FERPA amidst concerns about centralized computer systems amassing sensitive data about students, with little to no privacy or security protections.[24] Policymakers cited concerns about parents' lack of understanding about how their children's data was used, especially given the risk of schools misusing or improperly disclosing student data with no oversight.[25] When introducing FERPA, Senator James Buckley stated, "the sense of a loss of control over one's life and destiny, which many social commentators say is growing amongst our citizens, seems to be increasingly felt by parents

with respect to the upbringing of their own children."[26]

Regarding how schools misused or improperly disclosed children's data, Senator Buckley stated that parental consent could mitigate these risks: "the requirement of parental consent informs the parents, to some extent, about what is being done with and to their children in schools, and it offers the best available protection against educational abuses that I can think of." FERPA provides parents (and eligible students, those 18 or older or enrolled in a post-secondary institution) more control over their children's (or their own) education records. Additionally, with certain exceptions, FERPA requires education institutions subject to the law to gain parental consent (or an eligible student's consent) before disclosing "personally identifiable information in education records."[27]

The 1990s: Concerns for Children's Policy Online

Lawmakers passed COPPA in 1998 in response to concerns about children's data privacy. In the 1990s, the internet expanded rapidly, prompting a desire to protect consumers' privacy, with specific concerns for children's data privacy. Some websites and advertisers collected large amounts of consumer data, and people had concerns about the lack of legal mandates regarding consumer protections that could curb these practices. An FTC survey noted that nearly 85 percent of websites collected personal information from consumers, yet only 14 percent of a random sample of websites provided any notice regarding information practices.[28] With regard to children's websites, 89 percent collected personal information from children. Of those websites, 23 percent told children to seek parental permission before the children provided their information, 7 percent of websites said they would notify parents of their information practices, and fewer than 10 percent provided parental control over the collection and/or use of children's information.[29]

In response to these concerns about children's privacy, the FTC increasingly scrutinized how websites treated the information of young users. In 1997, the FTC set forth principles that should apply to children's information:

> It is a deceptive practice to represent that a Web site is collecting personally identifiable information from a child for a particular purpose (e.g., to earn points to redeem a premium), when the information will also be used for another purpose which parents would find material, in the absence of a clear and prominent disclosure to that effect.
>
> * * *
>
> [A]ny disclosure regarding collection and use of children's personally identifiable information must be made to a parent, given the limited ability of many children within the target audience to comprehend such information. An adequate notice to parents should disclose: who is collecting the personally identifiable information, what information is being collected, its intended use(s), to whom and in what form it will be disclosed to third parties, and the means by which parents may prevent the retention, use or disclosure of the information.
>
> * * *
>
> [B]efore releasing individually identifiable data about children, the company should obtain parental consent.[30]

These principles were included in the FTC's response to a petition that the commission investigate KidsCom, an interactive website designed for kids aged 4–15.[31] In 1996, a consumer advocacy organization, the Center

for Media Education (CME), had requested that the commission investigate KidsCom's practices, which included requiring users, mostly children, to answer a survey asking for information such as the child's name, sex, birthday, email address, home address, number of family members, and grade before the child could access the site. KidsCom also incentivized children to provide their name and email address, along with their product and activity preferences, in exchange for in-service awards, but the company did not disclose that this information would inform marketing practices.[32]

Additionally, the commission found that parents did not have "adequate notice and an opportunity to control the information" nor an opportunity to consent to the release of their children's personally identifiable information before it was disclosed; and children were at risk of being contacted by adults posing as children on the site.[33] While the FTC found that certain KidsCom practices were likely deceptive or unfair and thereby in violation of Section 5 of the FTC Act, the FTC recommended no enforcement action because in the time between the CME petition and the FTC letter, KidsCom had stopped these practices.

The FTC's 1998 report "Privacy Online: A Report to Congress" also reflects the commission's attention to children's privacy protections.[34] At this time, no comprehensive legislation existed to protect children's information online, so collection of personal information was subject only to self-regulatory schemes. Submitted to Congress, the report assesses the effectiveness of self-regulation as a mechanism to protect consumer privacy online.

Although the report focuses on general consumer privacy, one section details growing concerns about children's privacy. The report recommends that "Congress develop legislation placing parents in control of the online collection and use of personal information from their children," and laid the groundwork for many of COPPA's language and requirements.[35] To support its recommendation for legislation governing children's privacy, the report indicates several risks to children online stemming from the lack of parental control and oversight of their children's data, including the risk of children's information being commercialized and children being exposed to safety risks.

With regard to commercialization, the report notes that 14 percent of America's 69 million children are online, and "[t]heir growing presence online [] creates enormous opportunities for marketers to promote their products and services to an eager audience."[36] The report documents concerns about data collection practices bypassing parents, who "have traditionally protected children from marketing abuses."[37] Because children lack the judgment to provide meaningful consent to disclose their own personal information online, particularly in the context of registering for a contest or game, the report notes the need for parents to play a significant role in providing consent.[38]

Echoing the FTC's letter about KidsCom, the report also notes the FBI's and Justice Department's finding that online services were quickly becoming the most powerful resources that predators used to identify and contact children.[39] The report identifies the risk in children sharing personally identifiable information in publicly accessible places, including chat rooms, which "runs contrary to [the] traditional safety message" parents give to children to avoid speaking with strangers. The report concludes that the internet encourages children to interact with strangers in their homes.[40]

Discussing how to mitigate these risks, the commission reflected on the traditional relationship between parents and children, tying in how the FIPs and FERPA can inform mitigation strategies. The report argues that the user rights of FIPs should apply to parents, given the typical special status of children under current legal frameworks. The report also cites FERPA as a federal statute that, regarding privacy rights, recognizes "both the need for heightened protections for children and the special role that parents play in implementing these protections."[41]

With respect to the FIPs principles of notice and consent, the report states that parents should receive notice and be able to control the collection and use of personal information about their children, indicating the principles outlined in the letter about KidsCom:

To assure that notice and choice are effective, a Web site should provide adequate notice to a parent that the site wishes to collect personal identifying information from the child, and give the parent an opportunity to control the collection and use of that information. Further, according to the [KidsCom] letter, in cases where the information may be released to third parties or the general public, the site should obtain the parent's actual or verifiable consent to its collection.[42]

Notably, the report also defines the "actual or verifiable parental consent" that the FTC recommended websites obtain before disclosing a child's information:

Mechanisms for obtaining actual or verifiable parental consent include having the parent: mail or fax a signed form downloaded from the site; provide a credit card number; or provide an electronic (digital) signature. An e-mail message submitted without a digital signature may not be adequate to assure parental consent, since a site operator has no means of knowing whether the message is from a parent or a child. This is particularly true because most children do not currently have their own e-mail addresses and instead share their parents' e-mail addresses. While electronic signatures may be the best solution in the future, they may not be widely available at this point. In the meantime, children's Web sites may need to adopt traditional consent mechanisms, such as written consent forms and credit card numbers.[43]

The influence of the report is echoed in COPPA's definition of consent. The report concludes by recommending that Congress develop legislation "placing parents in control of the online collection and use of personal information from their children."[44]

COPPA's Introduction and Passage in 1998

Considering the FTC's 1996 survey and 1998 report, Senators Richard Bryan and John McCain introduced COPPA in the Senate in July 1998.[45] In October 1998, then-Representative Edward Markey introduced a House companion bill that enveloped COPPA in an "Electronic Privacy Bill of Rights," which also included separate privacy protections for adults.[46]

In their introductory remarks, Senators Bryan and McCain recognized the significant benefits that children receive from the internet but identified concerns that compelled the bill's introduction, including risks to children's safety and the commercialization of their information—echoing the FTC's report.[47] In his introductory remarks, Senator Bryan noted that "the same marvelous advances in computer and telecommunication

technology that allow our children to reach out to new resources of knowledge and cultural experiences are also leaving them unwittingly vulnerable to exploitation and harm by deceptive marketers and criminals."[48]

The Senators then connected these issues to the lack of parental control over how children interact online. Senator Bryan indicated the FTC's survey finding that "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."[49] Although the Congressional record on the House version of COPPA is limited, Representative Markey similarly highlighted the law's parental control aspect, introducing COPPA as "a subset of parent's privacy rights," whereby parents have knowledge, receive notice, and an opportunity to say no to "reuse or resale of [their child's] personal information."[50]

> **"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."**
>
> *—Senator Richard Bryan*

The introduction of COPPA reflected the notion that children should not be stopped from engaging with the internet because of the concerns motivating the legislation. Senator Bryan continually noted the significant benefits that children receive from the internet, arguing that children should not have to expose themselves to potentially harmful marketing practices or safety risks in order to enjoy those benefits.[51] The senator also advocated for children's digital literacy: "I think all would agree that proficiency with the Internet is a critical and vital skill that will be necessary for academic achievement in the next century."[52] To address these concerns, the senators proposed legislation that would enable the FTC to create rules requiring commercial websites to take the following actions:

Provide notice of personal information collection and use practices;

- Obtain parental consent for the collection, use, or disclosure of personal information from children 12 and under;
- Provide parents with an opportunity to opt out of the collection and/or use of personal information collected from children 13 to 16 (an element that did not make it into the final legislation);
- Provide parents access to their children's personal information;
- Establish and maintain reasonable procedures to ensure the confidentiality, security, accuracy, and integrity of personal information about children.[53]

When Congress passed COPPA on October 21, 1998, it included nearly every element of the proposed legislation, except for parental opt-outs for teenagers aged 13–16, because of concerns about teen privacy. At the time, privacy advocates argued that this element would reduce the privacy rights that teens deserve.

In response to COPPA's directive, the FTC announced the COPPA Rule, which became effective on April 21, 2000. Thirteen years later, the Rule was amended, effective on July 1, 2013.

International Approaches to Children's Privacy

While this report focuses on VPC under COPPA, the international landscape is also relevant because operators subject to COPPA often operate globally and are thus subject to multiple consent regimes that further differing policy goals. Exploring international approaches also provides insight into how other countries approach children's data privacy.

Many other jurisdictions similarly believe that younger children and teens are especially vulnerable and deserve stricter protections, but unlike the US, do not offer solutions based on parental consent alone. Instead, they take a multipronged approach that includes not only parental consent but data minimization, privacy by design, and respect for children's autonomy (e.g., drafting policies in language that allows children to understand their own rights and choices). Some countries also take a more aggressive approach, such as China's strict limitations on children under 16 accessing gaming platforms. This section provides an overview of how other countries have structured children's data privacy protections, in comparison to COPPA.

Multi-Jurisdictional Approaches

Several legal regimes have based their child privacy protections on Article 3 of the United Nations Convention on the Rights of the Child (CRC), an international treaty ratified by 195 countries.[54] While the United States has not ratified the CRC, UNICEF notes that it has become the most widely ratified human rights treaty in history.[55] Signatories include Australia, Brazil, France, Germany, Ireland, Mexico, Singapore, South Korea, and the UK.[56] Section 1 of Article 3 states, "[i]n all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interest of the child shall be a primary consideration." Emphasizing the "best interests of the child" has informed how other countries seek to create a safe environment for children online.

Another multi-jurisdictional approach is the recently adopted Organisation for Economic Co-operation and Development (OECD) Recommendation of the Council on Children in the Digital Environment. OECD is an international organization that establishes international standards regarding social, economic, and environmental challenges.[57] Thirty-eight countries are members, including the United States.[58] Like the CRC, the recommendation recognizes that the child's best interests should be a primary consideration for children online. The recommendation's goal is to balance protecting children from risk and "promoting the opportunities and benefits that the digital environment can provide."[59]

In addition to adopting these multi-jurisdictional approaches, many countries have their own laws governing child privacy and VPC that align with the CRC and OECD frameworks. A few laws discussed below demonstrate the breadth of approaches throughout the world.

GDPR:[60] General Data Protection Regulation

The European Union has no COPPA-equivalent independent law for children's data protection. The EU incorporates children's privacy in the General Data Protection Regulation (GDPR), which includes data protections for people of all ages. However, the GDPR specifies that "children merit special protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."[61]

Acknowledging that children require special protection, the GDPR includes instances in which privacy standards must be higher for data collected from children.[62] Like COPPA, the GDPR requires parental consent when consent is the basis for processing a child's data in the context of providing "information society services.".[63] However, the GDPR leaves it up to the service to "make reasonable efforts to verify in such cases that consent is given or authorised by the holder of the parental responsibility over the child, taking into consideration available technology."[64] Like COPPA, GDPR and other EU laws reflect a sliding scale approach to parental consent, through the concept of proportionality. Under the GDPR, processing personal data of children can also be justified by one of the available lawful grounds other than consent. For example, a legitimate interest[65] can be a basis for data collection, but relying on a legitimate interest requires a balancing test between this interest and the rights and interest of children as a "vulnerable group" before the processing takes place, and would not require consent.

Additionally, the GDPR does not address parental access to children's data. Some stakeholders suggest that only the child can make access or deletion requests, which raises a conflict if parental consent is the basis for data collection in the first place. Nonetheless, the GDPR recognizes that children do not lose their rights to transparency just because a parent has consented on their behalf.[66]

Currently, the GDPR allows individual Member States limited flexibility in determining the national age of digital consent for children: between the ages of 13 and 16. For example, Ireland has set the age of digital consent at 16, which the Minister for Justice will review by May 2022. The UK set its age of digital consent at 13. However, on June 24, 2020, the European Commission published a Communication regarding the mandated two-year evaluation of the GDPR, in which it discusses as a future policy development "the possible harmonisation of the age of children consent in relation to information society services."[67] The Commission expressed concerns that the variation in ages across the EU results in uncertainty for information society services and may hamper "cross-border business, innovation, in particular as regards new technological developments and cybersecurity solutions.[68]

Given the challenges of age variations, the Commission also initiated a pilot project to create an infrastructure for implementing rights and protection mechanisms for children online, which began on January 1, 2021.[69] The project aims to map age-verification and parental consent mechanisms both in the EU and globally to create "an interoperable infrastructure for child online protection including in particular age-verification and obtaining parental consent of users of video-sharing platforms or other online services."[70] Currently, Member States require or recommend varying age-verification and parental consent mechanisms. This program has become a consortium of EU stakeholders currently working to develop "pan-European, open-system, secure and certified interoperable age verification and parental consent" mechanisms for operators subject to the GDPR.[71]

The United Kingdom

In addition to creating the guidelines set forth in the UK GDPR,[72] the UK recently enacted the Age Appropriate Design Code (or Children's Code). The Children's Code holds the child's best interests as a core standard, stating the "best interest of the child should be a primary consideration when you design and develop online services likely to be accessed by a child."[73] The Children's Code became effective on September 2, 2020 and allowed a 12-month transition period for company compliance. It applies to "information society services likely to be accessed by children" in the UK. The code's territorial reach includes services that are based in the UK, have an office in the UK and process personal data in the context of the company or service's activities, are offered to UK users or monitor their behavior, and are likely to be accessed by children.

The Children's Code details the privacy by design obligations in the UK GDPR and requires companies to incorporate privacy by design principles to limit data collection, and grants children more direct control over data. The Children's Code requires geolocation, data sharing, and profiling to be inactive by default unless an organization can demonstrate a compelling reason for these practices, taking into account the child's best interests. To center children in the data collection process, the Children's Code requires prominent, accessible tools to help children exercise their data protection rights and report concerns. It also requires services providing parental controls to also give children age-appropriate information and an obvious signal when they are being monitored.

Ireland

Ireland has also taken a child-centered approach to protecting privacy through the Irish Data Protection Commission's (DPC) Draft Fundamentals for a Child-Oriented Approach to Data Processing (the Fundamentals), which detail the legal obligations in the GDPR and were released in draft form for public consultation in December 2020.[75] The DPC accepted submissions until March 31, 2021 and is currently reviewing responses before it publishes a final version. The Fundamentals are similarly rooted in the United Nations Convention on the Rights of the Child and emphasize Article 3(1)'s best interests of the child. The Fundamentals apply to all online and offline organizations that process children's data. This includes services directed at children and services that children are likely to access, like COPPA. The Fundamentals' territorial scope will likely reflect the territorial scope of Ireland, which includes the European headquarters of many technology companies, such as Apple, Facebook, LinkedIn, TikTok, and Twitter.

While the Children's Code focuses on the engineering and design of products and services, the Fundamentals provide a rationale and framework for understanding data processing in the best interests of the child. The Fundamentals call for allowing children to have their say, by noting that "[o]nline service providers shouldn't forget that children are data subjects in their own right and have rights in relation to their personal data at any age. The DPC considers that a child may exercise these rights at any time, as long as they have the capacity to do so and it is in their best interests."[76] Another key principle is not to shut out child users or downgrade their experience. The Fundamentals state, "[i]f your service is directed at, intended for, or likely to be accessed by children, you can't bypass your obligations simply by shutting them out or depriving them

of a rich service experience." If a website appeals to children, then the website operator has obligations under the Fundamentals.

Both the Children's Code and the Fundamentals define a child as a person under the age of 18, following the UNCRC's definition of a child. However, it is necessary to distinguish this definition from the age at which a child may exercise their rights to give consent and practice their data rights. Standard 15 of the Children's Code also requires "provid[ing] prominent and accessible tools to help children exercise their data protection rights and report concerns."[77] Like the Fundamentals, the Children's Code does not specify the age at which children may exercise their digital rights; instead, it provides guidelines to develop age appropriate online tools based on age ranges—similar to the CRC's "evolving capacities" definition.

Germany

The German youth protection law focuses on content protection. The law requires businesses to use scheduling restrictions to ensure that content harmful to children is not available during the day, when children are online; to use technical methods to keep children from accessing inappropriate content, such as sending adults a PIN after age verification; and to use age labeling that youth-protection software, downloaded by parents on their children's devices, can read. However, the efficacy of these methods is unproven.

China

China deems the personal information of children under the age of 14 to be "sensitive personal information."[78] China's recently enacted Personal Information Protection Law (PIPL) includes strict rules regarding children's privacy, including heightened standards for operators of sensitive personal information. Specifically, the law's requirement that operators obtain parental consent from users under 14 does not include an exception for operators that are unaware or have no reason to be aware of the data subjects' young age.[79] Operators must also get explicit parental consent before collecting data from children aged 14 and older.[80]

The children's privacy landscape in China also includes the country's Law on the Protection of Minors, recently adopted in 2021. As revised, the law restricts children under 16 from opening live broadcasting accounts.[81] This policy is significant because it forgoes parental consent and, instead, is a prohibition. Moreover, the law requires parental consent when children aged 16 and older open live broadcasting accounts, and imposes a "unified electronic identity authentication system" for online games. Finally, the law imposes a curfew on gaming and recommends that accounts for social networking, gaming, and online media entertainment be in "minor protection mode."[82] In addition to the legal requirment, through regulation, the country's National Press and Publication Adminstration restricts online gaming to minors for one hour on Friday--Saturday, as well as on national holidays.[83] The impacts of this relatively new law are not yet clear. However, reports already indicate children attempting to circumvent some of the law's curfew and time limitations on playing electronic games.[84] The Chinese government has already taken steps to address this through a new regulation that would require service providers to ensure that no one registers an account with false information.[85]

Singapore

Singapore's Personal Data Protection Act of 2012 (PDPA) largely governs the country's data protection landscape. The PDPA does not specify requirements regarding children's privacy. In general, a risk-based approach applies in determining how to handle personal data. Additional measures should be taken to

respect personal data that is sensitive in nature, including data related to children. However, Advisory Guidelines from the Personal Data Protection Commission (PDPC) address the data governance of minors. Civil law defines the age of majority as 21, meaning minors are individuals under 21.[86] As Lim Chong Kin of Drew & Napier LLC explains, under PDPC guidelines,

> a minor who is at least 13 years old would typically have sufficient understanding to be able to consent on his own behalf for the purposes of the PDPA. Notwithstanding, if an organisation has reason to believe, or it can be shown that a minor does not have sufficient understanding, the organisation may obtain consent from someone who can legally provide consent on the minor's behalf (e.g., parent or legal guardian).[87]

These guidelines are unique in assuming that a child 13 years or older can sufficiently understand and consent to matters relating to their data. Moreover, Singapore's approach centers less on the child's age and more on capacity. Similar to many countries' policies, the PDPC guidance addresses parental consent when an operator has knowledge or should have knowledge that they collect children's data. However, Singapore's guidelines are unique in that the knowledge operators have or should have pertains not to the user's age but, rather, to the user's degree of understanding.

South Korea

Consent requirements in the Republic of Korea are often considered the strictest globally. South Korea has long required that operators obtain parental consent before collecting personal information from users under 14. Since revisions enacted in 2020, South Korea's child privacy laws now also specify methods through which operators can obtain written parental consent.[88] Parents may choose to consent "via text, payment, information, or authentication through smartphones."[89] After obtaining consent, the operators must send written confirmation to the parents through one of the aforementioned methods.[90]

The country's laws also emphasize the need for operators to provide clear policies that children can comprehend.[91] As the next section discusses in greater detail, ensuring that children have adequate information about how services use their information promotes autonomy over one's data and teaches children valuable digital literacy skills.

Brazil

Brazil's General Personal Data Protection Law (LGPD) requires parental consent before the processing of any child or adolescent data.[92] The country's Statute of the Child and Adolescent (ECA) defines "children" as individuals under 12 and "adolescents" as individuals between 12 and 18.[93] As one publication notes, the ECA asserts that "children and adolescents have a peculiar condition of being in development."[94] Reflecting this philosophy, the LGPD's parental consent requirements tend to be heavier than those in many other countries.[95]

Under the LGPD, the only time child or adolescent data collection does not require parental consent is when "collection is necessary to contact the parents or the legal representative, and as long as the data are used one single time and not stored, or for their protection, and under no circumstances shall the data be passed on to third parties without consent."[96] The policy prohibits operators from conditioning children's and

adolescents' participation on "games, internet applications or other activities providing personal information beyond what is strictly necessary for the activity."

While the LGPD approach appears to favor parental consent, the law also recognizes the autonomy of children and adolescents. One section requires operators to communicate about data practices in a manner that child and adolescent users can comprehend.[97] This provision aligns with the child-centered approaches in countries such as the UK and Ireland in that it seeks to involve children and adolescents in decisions about their data by helping them understand how operators use their information. Brazil's policies on minors' data embody both parent-focused and autonomous philosophies. While the LGPD imposes strict parental consent for users under 18 years, with limited exceptions, the law also seeks to involve minor users in decisions regarding their data by requiring operators' policies to be accessible to young users.

Navigating Each Country's Approach to Children's Privacy is Challenging

As the first law of its kind, COPPA has influenced how children in other countries access the internet and how their data is protected.[98] Despite COPPA's influence around the world, there are challenges to implementing parental consent mechanisms globally given countries' different policy approaches to children's rights online. Practical differences, such as varied age restrictions and parent verification methods, and different philosophies distinguish the US and international approaches.

In practical terms, companies operating internationally often struggle to adapt to the varied age restrictions across jurisdictions. While "children under 13" became the default because COPPA was the first law of its kind, other countries have set their own digital consent limits, with most ranging between 13 and 16. Additionally, some countries, rather than defining "child" in terms of a number, use age ranges to develop age-specific and appropriate online tools. As a guideline, the UK's Children's Code uses the age ranges of 0–5, 6–9, 10–12, 13–15, and 16–17.[99] These age ranges are meant to guide the design of age-appropriate services.

In philosophical terms, countries such as the United States and China place more emphasis on parental consent in their child privacy laws, placing an emphasis on parental consent. In contrast, countries such as Singapore and many European nations incorporate but do not center parental consent, leading to a more flexible approach to parental guidance over youth internet activities.[100] In 1989, the UN Convention on the Rights of the Child adopted a rights-based approach to children's consent, recognizing "children as rights holders in and of themselves—rather than mere persons in need of protection through child-specific measures."[101] Although the GDPR retains some of the focus on parental judgment that is present in COPPA, it balances protection and autonomy in a way that the United States' regulations do not reflect. On the other end of the spectrum, the Children's Code emphasizes a company's decision or determination of risk, rather than parental control. Furthermore, whereas COPPA details acceptable methods for parental identity verification, GDPR does not, mirroring the broader COPPA language on verifying a parent. The GDPR states, "reasonable efforts to verify in such cases that consent is given or authorised … taking into consideration available technology."[102]

COPPA applies to services either directed to children or that have actual knowledge that children access the service. Critics of COPPA have argued that this "actual knowledge" standard incentivizes willful ignorance for general-audience sites and services that children access. As in both the Children's Code and the Fundamentals, the scope includes not only services directed at children but those that children are likely to access. "Likely to access" indicates a much broader scope, particularly given the varying age thresholds across jurisdictions. A service may appeal equally to adults and teenagers.

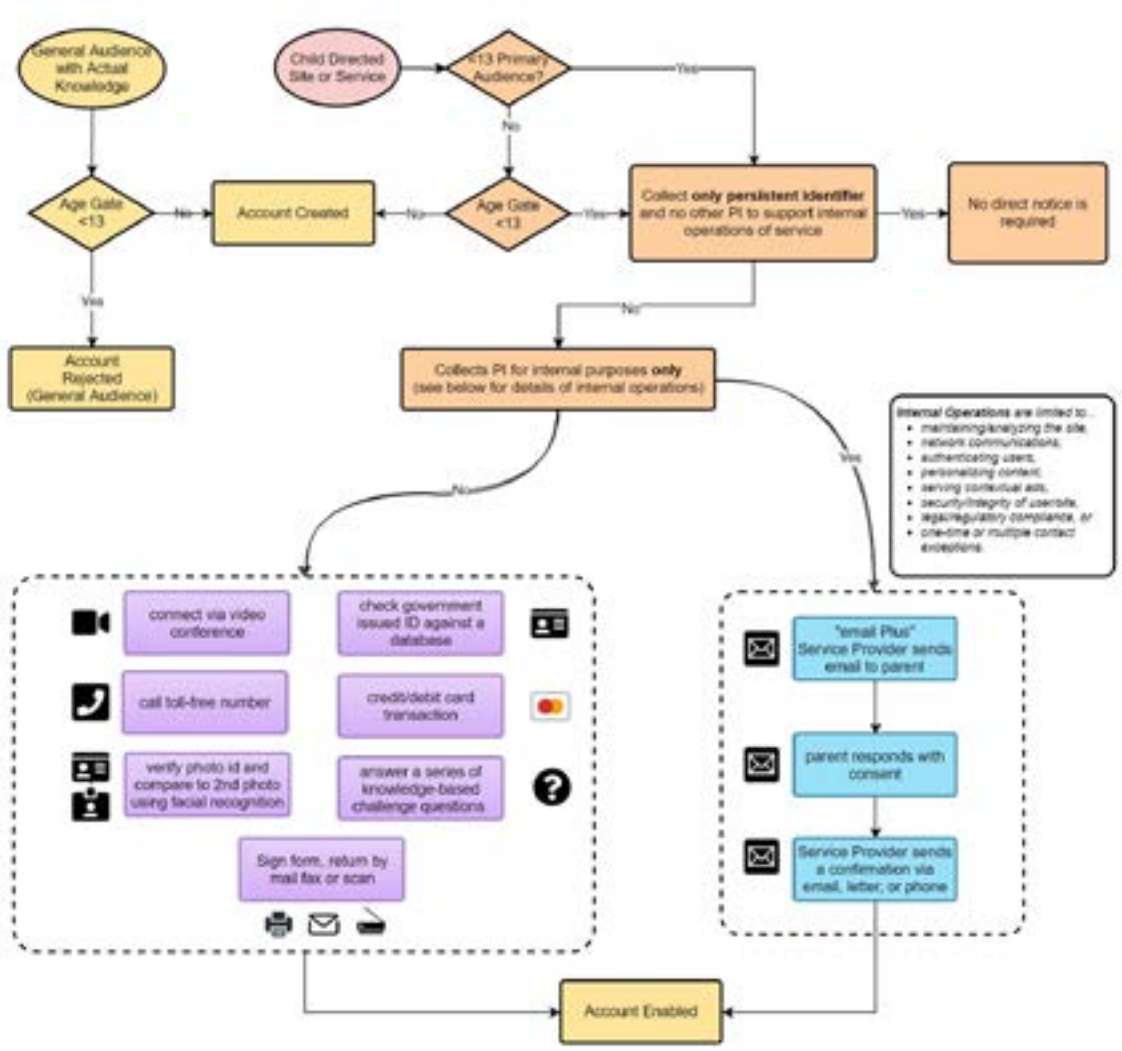
A Deep Dive into Verifiable Parental Consent

COPPA[103] requires an operator of a commercial online service directed to children under 13, or with actual knowledge that it has collected personal information from children under 13, to take several steps to protect the privacy of personal information collected from children. These steps include posting a privacy policy that identifies, among other things, how the operator handles children's personal information; providing parents with direct notice of information practices; obtaining the parent's verifiable consent before collecting, using, or disclosing their children's personal information; and respecting parents' subsequent requests to review or delete data collected about their children.[104]

Directed to Children. The FTC determines whether a site or online service is directed to children on a holistic, case-by-case basis. It considers specific factors, including but not limited to the subject matter of the site or service, the nature of activities, and whether advertising on the site is directed to children.[105] If the FTC determines that the online service targets children under 13 as an audience, even if children are not the primary audience, the online service is still "directed to children" according to COPPA.[106] This is often called a "mixed audience" site. The FTC highlights that "the 'mixed audience' category is a subset of the 'directed to children' category, and a general audience site does not become 'mixed audience' just because some children use the site or service."[107]

Actual Knowledge. Even if a site or service is not directed to children, COPPA still applies if an operator has "actual knowledge" that it collects personal information from children under 13. Determining whether a site or service has "actual knowledge" involves a fact-specific inquiry and can occur in almost any way, including via emails, a parent flagging content on a platform, or any other accumulation of facts indicating that data collected likely comes from children. For example, a third-party ad network operating on an operator's website or service will have actual knowledge "if a child-directed content operator . . . directly communicates the child-directed nature of its content to [an ad network] or where a representative of an ad network recognizes the child-directed nature of the content."[108]

Before collecting, using, or disclosing a child's personal information, an operator must provide direct notice of privacy practices to parents. Additionally, operators must obtain VPC, which means the operator must obtain the parent's consent to such collection and verify the parent's identity. While some exceptions exist, the requirement for operators to obtain VPC is a key component of COPPA.[109] This section outlines the intricacies of COPPA's current VPC requirement, aspects of which the flow chart below depicts.



The general audience portion of the flow chart assumes that the online service already has actual knowledge through a path other than an age screen that they are dealing with a child.

Step Zero: Age Screening Systems

To determine whether a user requires VPC—a step before the formal VPC process begins—websites and online services whose primary audiences are not children under 13 often rely on an age screening system, frequently called an "age gate." Certain general audience websites may also implement age screening systems to prevent children under 13 from accessing the service. For example, social media sites commonly use age screening systems to screen out children under 13, and sites that advertise alcohol or other age-restricted products also use such systems to screen out people under 18 or 21.[110]

Per FTC guidelines, age screening systems must prompt users to provide their age by asking their month and year of birth, rather than asking if they are 13 or older. This approach seeks to prevent child users from understanding that they need to input a particular birth year, regardless of their actual age, to access the service. The FTC prohibits sites directed to children from implementing age screening systems to prevent users under 13 from accessing their service, because if the service is directed to children, it must meet the

requirements for providing access to children under 13. VPC is required for PII collection on sites directed to children regardless of an age screen.[111]

The chart below summarizes age screening applicability under COPPA:

Site or Service	Children?	Is <13 Primary Audience?	May Age Screen?	May Reject <13?
General Audience	No	No	Yes	Yes
Mixed Audience	Yes	No	Yes	No
Directed to Children	Yes	Yes	No	No

Direct Notice

The COPPA Rule outlines the information operators must include in the direct notice to parents.[112] Operators must provide "direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented."[113] Direct notice is required in three circumstances: when 1) obtaining a parent's affirmative consent to the collection, use, or disclosure of a child's personal information; 2) communicating with a child multiple times; and 3) protecting a child's safety.[114] In the first instance, when operators notify parents about VPC requirements, operators must disclose

> (i) That the operator has collected the parent's online contact information from the child, and, if such is the case, the name of the child or the parent, in order to obtain the parent's consent;
>
> (ii) That the parent's consent is required for the collection, use, or disclosure of such information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;
>
> (iii) The additional items of personal information the operator intends to collect from the child, or the potential opportunities for the disclosure of personal information, should the parent provide consent;
>
> (iv) A hyperlink to the operator's online notice of its information practices required under 16 CFR § 312.4(d);
>
> (v) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and
>
> (vi) That if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records.[115]

FTC-Approved Verification Methods

Rather than mandate the method an operator must use to obtain parental consent, COPPA states that an operator must 1) choose a method that is "reasonably designed in light of available technology" 2) in order to ensure that the child's parent gives consent.[116] The FTC has determined that several methods meet the rule's standard. Listed below are the current FTC-approved methods for obtaining VPC:

- 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, as long as that identification is deleted from internal records upon completion of the verification process;
- Answer a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer;
- 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 submitted by the parent, using facial recognition technology.

Many of these methods come straight from the FTC's 1998 report that spurred COPPA's introduction, including allowing parents to mail or fax a signed consent form and having parents share their credit card information.[117] Most recently, in 2013 and 2015, knowledge-based questions and facial recognition technology have been approved as VPC methods.[118]

When Is VPC Required?

COPPA obligations, including VPC, apply when an operator (or third party with actual knowledge) collects, uses, or discloses a child's personal information. Collection of a child's personal information can occur through 1) requesting, prompting, or encouraging a child to submit personal information online; 2) enabling a child to make personal information publicly available (for example, providing access to a public chat forum where children can share information, without first making reasonable efforts to redact the information before posting and deleting the information); or 3) passive tracking of a child online, such as through the collection of persistent identifiers (for example, by allowing third-party platforms to collect device identifiers for ad-targeting at an online site or service directed primarily to children).[119]

COPPA-Protected Information and Prohibited Practices

COPPA defines personal information as "individually identifiable information about an individual collected online,"[120] a broad definition that includes "persistent identifier[s][121] that can be used to recognize a user over time and across different websites or online services."[122] In addition, operators must treat non-personal information, such as a child's keypress responses or achievement levels in a game, as if it were personal information if it is combined with personal information. Some of the personal information protected by COPPA includes persistent identifiers, including information stored in cookies as well as IP addresses.

- **Persistent identifiers** such as user IDs stored in cookies can serve purposes such as to customize a child's account or to maintain a child's achievement level in a game. This practice fosters an anonymous yet somewhat personalized experience for the child, without collecting more personally identifiable information than necessary; thus, COPPA allows it. However, COPPA does not allow this practice if operators disclose the identifiers to advertising networks to serve tailored advertisements or to create detailed profiles of child users.

- **Cookies** are small text files that a website places on a user's browser, which are then sent back to that website in internet traffic to enable personalized online experiences, among other things. If a unique ID is placed in a cookie, it can enable websites to do things such as recognize returning visitors so that the visitors do not have to re-enter log-in information or start a new shopping cart. On a website directed to children, holding a persistent identifier in a cookie allows the site to recognize a person by a username or first name, welcome them back, and allow them to pick up a game or activity where they left off. Modern web browsers provide options for users to view and delete their cookies, and may automatically block some cookies by default. Additionally, because cookies allow websites to recognize a return user, this practice allows operators to better understand their audience.

- An **IP address** is an identifier assigned to every internet-connected device on a network at a given point in time, to enable that device to send and receive internet traffic. Most websites and online platforms log their visitors' IP addresses to conduct routine governance tasks, including basic visitor analytics, spam filtering, and fraud detection. Because IP addresses are assigned and managed by the internet service operator and can rotate, they are typically not stable enough to serve as persistent identifiers; nonetheless, they may be used for purposes such as identifying that several devices are using the same network, to reveal whether those devices are related.

SPECIAL CONSIDERATIONS: METADATA AND VOICE DATA

Certain types and uses of data may trigger COPPA VPC obligations: metadata that includes COPPA-protected personal information, and, in the case of audio files of a child's voice, unique COPPA obligations. These distinctions are important for understanding when COPPA requires VPC.

User-provided photos may include metadata that contains COPPA-protected personal information, and photos are personally identifiable information when they contain a child's likeness or image. Digital cameras save exchangeable image file (EXIF) data, which may include detailed geolocation information such as the date, time, longitude, and latitude if the camera includes GPS capabilities. In some cases, this geolocation information could meet the definition of COPPA-protected location information (information "sufficient to identify street name and name of city or town"), which would make the EXIF data PII under COPPA.[123] Other photo formats might contain similar metadata.

Online services, including mobile apps, IoT devices, and internet-connected toys, sometimes also collect audio files of a child's voice. Under COPPA, audio files of a child's voice are personal information that require VPC. However, the FTC has issued a limited non-enforcement policy, stating that when an operator collects an audio file containing a child's voice solely as a replacement for written words, such as to perform a search or fulfill a verbal instruction or request, and only maintains the file for time necessary to fulfill that purpose, the FTC will not take an enforcement action against the operator for failing to obtain VPC.[124] The operator must, however, still provide clear online notice of its collection, use, and deletion policy regarding these audio files.[125] This non-enforcement policy applies only to the collection of applicable audio files and would not apply if operators request information via voice that is categorized as COPPA-protected personal information. An example of such information is a child's full name.

SPECIAL CONSIDERATIONS: VERIFIABLE PARENTAL CONSENT AND SCHOOLS

When schools contract to use a site or service, operators may rely on the contract as evidence that the school has obtained the necessary parental consent.[126] This allowance is consistent with FERPA's "school official exception," under which a school can consent on behalf of parents when the service collects student information for an exclusively educational purpose. In its COPPA FAQs, the FTC indicates that operators must provide the school with all notices required by COPPA, including "a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information upon the school's requests."[127]

However, the school's ability to provide this consent is limited to the educational context, in which an operator collects personal information from students for the use and benefit of the school and for no commercial purpose. If the operator wishes to use the student's information for its own commercial purpose in addition to the provision of educational services to the school, it must directly obtain VPC.[128] In this context, the school can serve as the intermediary to help the operator obtain parents' consent.

Exceptions to COPPA's Parental Consent Requirement

COPPA's general requirement that operators obtain parental consent before collecting children's personal information is subject to eight narrow exceptions:

1. When an operator is undergoing the process of obtaining parental consent (an operator must thereafter contact the parent to get parental consent—VPC or email plus—and if consent is not obtained, the operator must delete the information obtained);
2. When an operator provides voluntary notice to a parent about their child's participation on a site or service that does not collect personal information;
3. When an operator responds directly to a child's specific, one-time request;
4. When an operator responds directly more than once to a child's specific request—an operator must notify the parent and provide an opt-out option (for example, if the child wants to receive a newsletter);
5. When an operator is protecting a child's safety;
6. When an operator is protecting the security or integrity of a site or service, to take precautions against liability, to respond to judicial process, or—as the law permits—to provide information to law enforcement;
7. When an operator permits a third-party plugin to collect PI from the operator's site directed to children. This exception applies in this context only if:
    a. The third-party operator collects only a persistent identifier and no other personal information;
    b. The user affirmatively interacts with the third-party site or service to trigger the collection; and
    c. The third-party operator has already screened and verified the person is 13 or over.
8. When an operator collects a persistent identifier and no other personal information and uses the identifier only to support the internal operations of the website or online service. In such cases, there also shall be no obligation to provide notice under 16 C.F.R. § 312.4 (the COPPA Rule).[129]

What does support for internal operations mean, in practice? Parental consent is not required for the collection and use of a persistent identifier to support the internal operations of a site or service.[130] Such activities include but are not limited to analyzing the functioning of a site, serving contextual ads (see below) or limiting the number of times a particular ad appears to the same user, authenticating users or personalizing content, supporting payment and delivery functions, spam protection, statistical reporting and analytics, debugging, and so forth.[131]

Contextual Advertising. Contextual ads include those based on a user's current visit to a website or single search query, without the collection of personal information about the consumer's online activities over time. In other words, an advertisement based on point-in-time data is acceptable as long as it is not based on collection of information from across sites and platforms or on a user's detailed profile.[132]

In addition to the above-noted exceptions to the VPC requirement, operators that do not disclose children's personal information to third parties or make that information publicly available may rely on a process called email plus. This process involves two steps, in which an operator first requests that a parent respond to the operator with their consent; then, the operator sends a confirmation to the parent via email, letter, or phone call.[133] Operators may rely on email plus when using cookies to, for example, maintain a user's opt-out status, personalize content by saving a game score or achievement level, or customizing the colors or design of a child's account. However, if the cookie is not used over time and across websites and other collected information is not PII under the COPPA Rule (e.g. user name), email plus is not necessary. For example, if only a cookie is used to maintain opt-out status, personalize content, save a game score or color preferences, it may fall under the support for internal operations exception to parental consent and may not require the operator to use email plus.

COPPA Safe Harbors

COPPA also allows operators to apply for certification as COPPA-compliant through a "safe harbor" program, which is consistent with the FTC's prior approach to consumer privacy: industry self-regulation.[134] The safe harbor programs act as self-regulatory bodies. A company may comply with COPPA if it is a member of an FTC-approved safe harbor program and complies with the program's guidelines.[135] Participation in a safe harbor does not guarantee that the FTC will not take adverse action, but the commission does look favorably on companies for their participation. The FTC oversees and reviews the safe harbors, and each program must state requirements that are "the same or greater" than those of the COPPA Rule.[136]

The programs assess the compliance of member services and take disciplinary action if a service does not comply with the safe harbor's requirements. The current approved safe harbor programs are the Children's Advertising Review Unit (CARU), Entertainment Software Rating Board (ESRB), iKeepSafe, kidSAFE, Privacy Vaults Online Inc (PRIVO), and TRUSTe.[137] In addition to certifying COPPA compliance, safe harbors can authorize VPC methods that operators may rely on to fulfill their COPPA obligations.

Beyond VPC: COPPA Today

In addition to requiring VPC and the elements discussed in section I of this report, COPPA includes several other protections for children's data and provisions informed by the US approach to children's online protection. This section discusses some of those elements, including prohibitions on profiling, self-regulatory elements, strict liability for relevant operators in relation to third parties, and confidentiality and security requirements.

COPPA does not prohibit advertising to children, but as modified in 2013, COPPA does prohibit the use of persistent identifiers to amass a profile or through behavioral targeting before the operator has first obtained verifiable parental consent. Additionally, COPPA precludes many advertising uses of data that are mainstream in other contexts, unless parental consent is obtained.

Operators of online services directed to children are also strictly liable for the practices of their third-party partners that collect information on the operator's site or service, even if those third parties do not own, control, or have access to the personal information collected, unless actual knowledge applies.[138] This means that operators of sites directed to children are responsible for data collection that occurs through integration of advertisements or third-party trackers in their app, site, or service, including through plugins, social media engagement tools, or other embedded content. The operators are required to complete diligence on third parties as well.[139]

Potential COPPA violations may occur when an operator subject to the law integrates tools from third-party advertising platforms or embeds third-party features or other outside content. Common sources of third-party data collection include the following

Plugins and Social Media Integrations. Plugins can collect information from users through the sites and services that embed the plugins. Some social media platforms are not compatible with sites directed to children, while others may provide configurations so that their plugins can be embedded in a site or service directed to children.[140]

Embedded Third Parties. COPPA makes operators liable for the activities of third parties that operate on the operators' sites, but many operators often overlook that this may include embedded content served in third-party video players. For example, some embedded video players collect persistent identifiers for advertising purposes and, as a result, may conflict with COPPA even if the operator did not embed the videos for these purposes.

COPPA Flags. COPPA flags are a method that some, but not all, advertising platforms use to signal that a website is directed to children. The presence of a COPPA flag suggests that a third party has actual knowledge that the flagged service is directed primarily to children.[141] Typically, a COPPA flag might involve sending an integer of "1" or "true" as the value of a parameter such as "tfcd," a tag for treatment directed to children,[142] into the network traffic to indicate to a third-party ad network that a website, service, or specific users[143] are or are not directed to children. There is no standard, and each third party can define their method of signaling or none at all. Once an operator's site, service, or user has been tagged as directed to children, the third-party advertising network can take steps to disable online behavioral advertising and retargeting for that site.[144]

While COPPA and other flags and signaling[145] can be useful tools, flagging a site, embedded content, or API request as directed to children may not be sufficient for an operator to avoid violating COPPA. For example, not all ad networks and third-party plugins recognize COPPA flags. Moreover, other types of flags may affect only whether behaviorally targeted ads appear on an operator's website, but they may have no effect on third-party tracking technologies that collect information on the site in order to direct targeted advertisements elsewhere. If a third party collects data at the operator's site and uses that data to direct targeted ads at another site, it would likely be because a persistent identifier was collected and used over time and across websites, which would violate COPPA.

COPPA also requires operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from a child.[146] Operators must institute adequate policies and procedures for protecting a child's personal information from loss, misuse, unauthorized access, or disclosure. Operators must also take reasonable steps to release children's personal information only to service providers and third parties able to maintain the information's confidentiality, security and integrity, and who provide assurances to that effect.

COPPA does not include a specific definition of "reasonable security," but a recent settlement between the FTC and Zoom Video Communications, Inc. provides insight into what the commission expects of all operators collecting personal information, whether the company is subject to COPPA. The expected security practices include the following:

- assess and document on an annual basis any potential internal and external security risks and develop ways to safeguard against such risks;

- implement a vulnerability management program;
- deploy safeguards such as multi-factor authentication to protect against unauthorized access to its network; institute data deletion controls;
- take steps to prevent the use of known compromised user credentials; and
- review any software updates for security flaws and ensure the updates will not hamper third-party security features.[147]

Previous FTC orders have also indicated the types of security practices the commission expects of operators subject to COPPA. For example, in a settlement with VTech, an electronic learning developer, the FTC found that VTech failed to take reasonable steps to secure children's data, as COPPA requires.[148] The FTC ordered that VTech establish and implement a comprehensive security program that is "fully documented in writing.... contain administrative, technical and physical safeguards appropriate to [VTech]'s size and complexity, the nature and scope of [VTech]'s activities, and sensitivity of personal information."[149] Written security programs must also include designated staff responsible for the programs, a risk assessment process, regular testing and monitoring of programs' effectiveness at addressing such risks, and more.[150]

COPPA Enforcement

The FTC is the main regulatory body that enforces COPPA. COPPA also gives state attorneys general the authority to enforce compliance with the law. The FTC has outlined six steps for complying with COPPA. Websites or services should

1. Determine whether they collect PII from or on behalf of children under 13 or with actual knowledge that a child under 13 provided the PII.
2. Publicly post a COPPA-compliant privacy policy.
3. Provide direct notice to parents before collecting personal information from their children (subject to some exceptions) and send an updated notice if their privacy practices substantially change.
4. Obtain verifiable parental consent before collecting PII.
5. Give parents the option to review the PII collected, revoke consent for future collection of PII, and delete PII already collected.
6. Maintain internal security practices that reasonably protect the security of collected PII.[151]

Limited resources allow the FTC to bring COPPA enforcement actions at a rate of one to two per year, and these often involve instances that clearly violate COPPA. These actions especially involve situations in which services directed to children collected children's personal information without first obtaining the required VPC, or the service had actual knowledge and used personal information collected from a child without obtaining VPC.[152] However, this approach to COPPA enforcement has left many unanswered questions regarding the law's grey areas. Enforcement actions are useful not just to ensure children's online privacy but also to guide companies trying to understand how to best comply with COPPA's requirements. FTC enforcement actions detail which practices did not follow the law and the remedial measures required to ensure the company complies. Moreover, the relatively low level of enforcement compared to the high cost and burdens associated with COPPA compliance and VPC actually disincentivizes operators from even attempting to design COPPA-compliant sites and services.

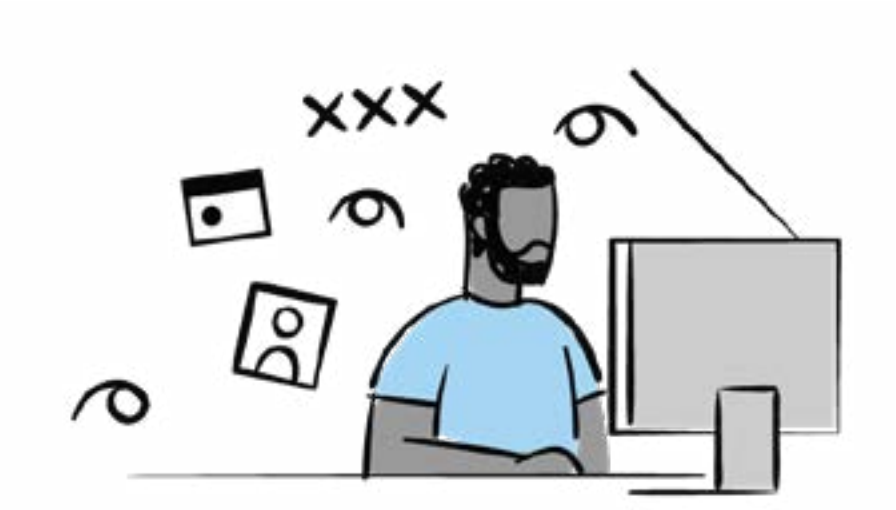
Critiques of COPPA

Criticisms of COPPA's VPC methods generally relate to efficacy and innovation, specifically, whether the consent methods provide a way to accurately identify that the operator is dealing with a parent and whether the methods are technologically efficient.[153] This section analyzes how COPPA's supporters and critics have attempted to fill gaps in children's online protection by institutionalizing parents' rights to control how children experience the internet.

Society has traditionally viewed parents as protectors of their children, but the rapid expansion of the internet disrupted parents' ability to oversee and control their children's activities. Given that the internet is often described as the "Wild West," with unlimited information and potential risks to children, such as contact with strangers, inappropriate content, and bullying, the demand for parental supervision is reasonable. Legislators enacted COPPA over fears, as noted by the former FTC commissioner in a statement during a hearing on the issue, of "the ability of the online medium to circumvent the traditional gatekeeping role of the parent."[154] Concerns about these risks arose because before COPPA, there were no restrictions on what was available to children online or how children should be treated in an online environment.[155]

Over time, parent and governmental concerns included tracking, data mining, and targeted advertisements. These worries prompted Congress and the commission to craft a regime that situates parents as necessary guradians of children's online activity. The following excerpt from the FTC's 1998 report to Congrss regarding online privacy highlights the ways in which parental supervision in traditional arenas extends to internet activities:

> [Children's] status as a special, vulnerable group is premised on the belief that children lack the analytical abilities and judgment of adults. It is evidenced by an array of federal and state laws that protect children, including those that ban sales of tobacco and alcohol to minors, prohibit child pornography, require parental consent for medical procedures, and make contracts with children voidable. In the specific arenas of marketing and privacy rights, moreover, several federal statutes and regulations recognize both the need for heightened protections for children and the special role that parents play in implementing these protections.[156]



A Deep Dive into Verifiable Parental Consent

What are the perceived dangers of the internet? According to the FTC, the extent to which children enjoyed "unfettered access to chat rooms" and other websites collecting personal information without parental permission in the pre-COPPA internet era was large enough to raise privacy and safety concerns.[157] Congressional action in light of these concerns was, in the FTC's words, "deliberately paternalistic" while accounting for the "promise of technologies."[158] Since COPPA's enactment, concerned stakeholders have devoted significant resources to ensuring that operators do not mine children's data for commercial activities, since children cannot "meaningfully understand" the potential harms of sharing their personal information online.[159] As some have noted, children, whose brains are still developing, are no match for advanced profiling and analytics techniques.[160] The potential for minors to be "victims of their own inexperience with technology" underlies the perspective that parents and the government have a legitimate legal basis for protecting children.[161] Such supervision would grant children the "right to grow, learn, and develop without surveillance, sorting, steering or suppression."[162]

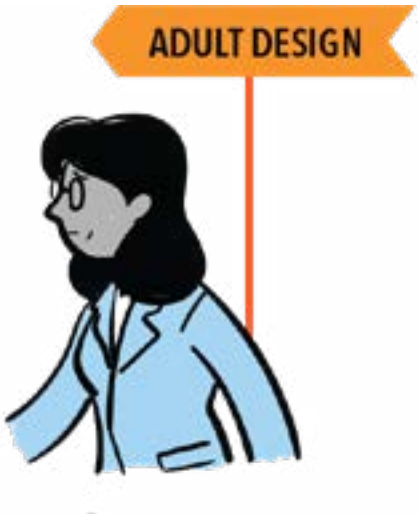
The goal of COPPA is to help parents control the collection of their children's data and to protect children, and as written, doesn't necessarily ensure that children engage in age-appropriate online experiences. Parents typically expect to be able to protect their children from predation.[163] Thus, COPPA's granting the power of consent to parents was meant to remedy the lack of parental control over data collection during the early years of the internet.

However, some stakeholders question whether the internet is actually perilous in a way that warrants such concerns. Critics such as Professor Simone van der Hof, Professor of Law and Digital Technologies at Leiden University, challenge the assumptions that children are inherently vulnerable and that parents, rather than children, are the appropriate decision makers regarding their children's privacy and data protection.[164] She argues that if both assumptions are true, little opportunity remains to secure children's rights.[165]

Other critiques of COPPA find that COPPA incentivizes operators to ignore children online. For example, in a publication describing age assurance, 5Rights Foundation described COPPA as "a marketing code [enacted] at a time when the digital world was neither as pervasive nor persuasive as it is now," noting that the framework "has driven a 'don't look don't see' attitude to the tens of millions of under 13s who enter an adult world of aggressive data collection, targeting and harmful content. This sanctioned blindness has also disincentivised the development of services and products for children."[166]

A Deep Dive into Verifiable Parental Consent

Some advocates seek to grant children, rather than parents, the tools to control their personal data and improve their ability to make informed choices about their online activity.[167] These advocates argue that parents, in a complex and quickly evolving digital enviroment, may not have the digital literacy skills to guide their child's online interactions, whereas some children do. Such a framework, advocates claim, give children the ability to have private spaces separate from their parents and develop into self-sufficient internet users with the capacity to understand good practice.[168] This holistic, rather than "deliberately paternalistic," approach most aligns with the European approach to regulating children's online activities.[169]



Verifiable Parental Consent in Practice: Parent, Industry, Advocate, and Academic Perspectives

To understand the challenges associated with implementing VPC, Future of Privacy Forum thoroughly reviewed public-facing industry representatives' and advocates' statements on COPPA and solicited insights from parents and industry stakeholders about VPC. Through these statements and insights, parents, industry representatives, advocates, and academics have identified unique challenges in current VPC mechanisms and approaches. This section outlines those challenges.

Efficacy

Stakeholders frequently stated that child users who complete the process in lieu of their parents or lie about their age easily circumvent the current methods for obtaining VPC. Representatives of Yoti, a digital identity platform, submitted comments about COPPA, indicating that "certain age gating or parental consent methods are easy to circumvent by either children or adults."[170] This results in children under 13 accessing social media sites and age-restricted content online, which means that COPPA's intended protections for children do not work in these cases.[171]

Similarly, several parents noted that in some cases, their children were able to lie about their ages to access certain services, especially social media. A parent even described VPC as privacy theater, because their children can get around VPC by making up birthdays, finding wallets around the house for their parents IDs, or entering their own credit card or email information into a VPC prompt. As a result, one parent questioned the value of VPC generally, noting that there was no point in sharing their sensitive information to provide VPC when their children can circumvent the requirement—they would only be trading one problem for another. Parents were more comfortable when asked about specific VPC flows, such as calling a phone number and using physical parental consent forms. However, the same parents noted that these methods are still easy for their children to circumvent.

The Computer and Communications Industry Association similarly noted that "high-friction" pre-approved VPC mechanisms, including requesting parental consent through users submitting credit card information, "may encourage circumvention."[172] In its 2019 COPPA comments, SuperAwesome, provider of kidtech solutions for developers, noted that current VPC methods risk people who are not parents or caregivers completing the VPC process.[173] SuperAwesome describes the "two most prominent methods" for VPC: using a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder or providing a form of government ID that the operator checks against a database. The company critiques these two methods as

> only partially meeting the FTC's intended standard for confirming parental identity. At best, they confirm the authorizer is an adult. However—as more and more children and young adults use credit cards, that assumption may not be so readily apparent. In a 2019 survey, 17% of parents reported that their children aged 4-19 had credit cards.[174] Further, there is no failsafe, cost-effective way to verify parental identity.[175]

Parents similarly noted that current methods make it difficult to prove whether the respondent is a parent, another adult, or a savvy child.

Accessibility

Several stakeholders have also noted that currently approved robust mechanisms for obtaining VPC can hinder accessibility and equity. The prevalent methods of obtaining VPC are often tied to a parent providing credit card information or government identification information.[176] Several industry and advocate

stakeholders noted that these methods may result in inequitable outcomes. The Internet Association noted that requiring monetary transactions as a verification method, either through credit or debit cards or other online payment systems, is "problematic for the 8.4 million households in the United States that do not have any accounts at a bank or other financial institution."[177] In 2019, the Brookings Institution estimated that the number of undocumented immigrants living in the United States ranges from 10.5 million to 12 million, many of whom lack the identification necessary to complete most VPC requirements involving use of ID.[178]

Some commenters argue that children should not be prevented from enjoying the internet's considerable benefits simply because they cannot gain VPC for reasons out of their or their caregivers' control; in fact, this is contrary to COPPA's intent.[179] In its 2019 COPPA comments, Google notes that sometimes a parent or caregiver may not be readily accessible to engage in the VPC process, thereby hindering a child's ability to explore, learn, and engage online.[180]

Hesitancies, Privacy, and Security

When asked about particular COPPA-enumerated VPC methods, parents generally expressed discomfort with being asked to share sensitive information such as credit card information or their government ID and having that information linked to their children's online presence. The LEGO Group noted similar concerns in its 2019 COPPA comments, finding that implementing a robust VPC mechanism can "necessitate obtaining additional and often sensitive personal information from adults," posing privacy concerns.[181] Khan Academy noted that methods requiring parents to submit credit card or ID information, "create independent privacy concerns and increase[] compliance costs for service providers."[182] The Electronic Privacy Information Center noted that requiring parents to share credit card information would instead "expose parents to the same privacy risks that they are trying to protect their children from and deter them from using such online services in general."[183] One parent stated that if they were asked to provide credit card information or government ID, they would begin to question the appropriateness of content their child was trying to access.

Industry stakeholders also expressed concerns about parental confusion and discomfort, which often lead to reductions in users. For example, several companies noted that parents often mistakenly believe that providing credit card information to complete VPC means that services want them to pay to access a service or enable in-app purchases. These misconceptions can cause parents to distrust the service and its privacy practices, even if the service protects privacy well. Several parents noted that their degree of discomfort depended on their familiarity with the service requesting such information. If their family trusted, already used, or was familiar with the service, either through their personal life or through their child's school, they would feel more willing to share information to provide permission for their child. Academics also noted that "parents' privacy expectations are highly context dependent and contingent on perceptions of the different entities that collect personal information."[184]

Convenience and Cost Barriers

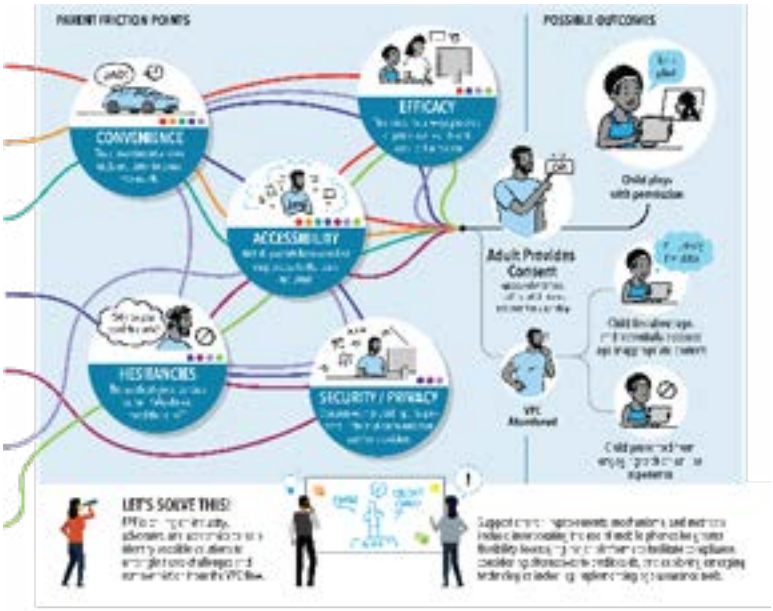
Several companies noted that implementing rigorous VPC requirements often leads to user drop-off, because the process introduces friction for users who want to engage a service. If a parent works from home and is in a meeting and their child wants to download an app, the aforementioned hesitation combined with a time-consuming VPC mechanism (such as inputting credit card information or engaging in a video call) may dissuade parents from completing the VPC authentication process. This friction may encourage children and parents to seek experiences that are easier to engage and may not comply with

COPPA's VPC requirement. Worse, this friction may cause children to either circumvent VPC or engage in age-inappropriate experiences online.[185]

According to the Developers Alliance, extra steps during a sign-on process "create[] a system where parents regularly forgo COPPA benefits in favor of easier to use (ie: COPPA non-compliant) or general audience apps."[186] Similarly, the LEGO Group reported "a significant dropout when VPC is required due to the arduous and time consuming sign-in process," and, consequently, risks that children turn to games with lower barriers to entry and that "are not necessarily designed for the child's age."[187] Khan Academy noted that VPC methods that require "more intensive human interaction" including consent forms sent via fax or scan, or telephone or video calls, are "labor intensive," "time-consuming," inconvenient for parents, and costly to implement.[188]

Furthermore, industry stakeholders note that this friction also deters innovation regarding online sites and services for children. The associated costs of implementing a COPPA-compliant VPC mechanism also discourage developers from creating products for children. ACT, the App Association, argues that the lack of "effective, easy-to-implement, and affordable mechanisms" means that companies risk "unnecessary liability without meaningfully enhancing children's privacy."[189] In fact, ACT notes that "the COPPA Rule's burdensome compliance costs have resulted in many children-directed app and software developers closing down their businesses or deciding to target a general audience."[190] The high cost of getting VPC right can create an inequitable burden for midsized and smaller developers, making compliance affordable only for the largest platforms.

The Developer's Alliance noted in 2019 that "[a]n anonymous Developers Alliance poll of developers that design apps for children, or whose apps children could be using, indicated that many developers felt that designing a COPPA-compliant app places them at a competitive disadvantage amongst their peers. COPPA regulations by design have created increased friction between end-users and platforms, and thus impacts the way users chose to interact with certain apps."[191]



The ESRB and SuperAwesome identified a similar issue. According to ESRB, "many operators have chosen either not to create online services directed to children—an unintended negative consequence—or to restrict their collection of personal information so they do not trigger COPPA's direct notice and verifiable parental consent (VPC) requirements."[192] SuperAwesome notes that "the high bar for verified parental consent means it has also deterred some new and existing operators from launching innovative new services for kids. For many, the complexity is simply too daunting and the cost too high. The result is fewer dedicated kid-safe digital destinations, which arguably leads to children spending more time on general audience platforms, where their privacy and safety is less protected."[193]

The Toy Association notes that "it is costly to implement robust VPC and doing so results in significant drop-off of interest by parents. More restrictions that force companies to set up pay walls or other parental consent mechanisms will reduce, not foster, children's content online."[194] According to the Internet Association, while "COPPA and its implementation through the Rule has served the statute's goals . . . obtaining verifiable parental consent remains costly and complex and has materially affected the availability of child-directed content and services and the manner in which those services are delivered. Upfront costs, registration friction, and difficulties associated with securing approval for streamlined methods for providing notice and documenting parental consent may account for the fact that there has been very little innovation with respect to consent acquisition mechanisms. This, in turn, discourages new entrants and inhibits innovation in the interactive child-directed content space – which is ultimately a disservice to children, families, educators, and others who care for and about children."[195]

Government actors have also noted concerns about the cost of COPPA's VPC requirement. In its 2019 COPPA filings, the Office of the Arizona Attorney General stated that "the cost of obtaining verifiable parental consent can be unduly burdensome on small businesses, and the consent process can be frustrating for both businesses and parents alike."[196]

Unique Considerations

Research and conversations with stakeholders uncovered a gray area regarding when and how VPC should be implemented. For example, comments submitted by CTIA, the Wireless Association, argue that the FTC needs to "clarify that verifiable parental consent can be obtained through the set-up process for services that collect personal information from children at the direction of their parents."[197] For example, parents may rely on online tools to ensure that their children are safe, such as a smartwatch that tracks their child's location or an add-on phone service that monitors and filters their child's internet usage. Although these tools are marketed to parents and parents direct their children to use them, the tools may require operators to collect personal information from children under 13 and therefore may trigger COPPA's VPC requirements. As CTIA states, "under the FTC's current Rule and guidance, COPPA could be interpreted to require operators of these services to use a separate notice and consent process specifically to collect information from children under the age of 13 – even though that is precisely the reason that parents sign up for these services in the first place."[198]

How VPC Challenges Can Impact Children

If current VPC methods fail to effectively ensure that parents have an opportunity to weigh in on whether their child uses a site or service, many of the concerns that drove legislators to introduce and pass COPPA remain. In practice, research shows that children frequently circumvent VPC requirements to gain access to age-restricted sites and services.[199] What does that mean for children? In 2021, The University of Michigan Health C.S. Mott Children's Hospital conducted a national poll of parents of children ages 7-12 years old and found that a majority of parents are concerned that their children are inappropriately engaging with social media, sharing sensitive personal information without realizing it, accessing adult content, and unable to distinguish whether the information they engage with is true or false.[200]

These parental concerns are supported by research, which indicates that children struggle to identify credible sources and understand when an image is altered, leading to distorted perceptions of body image, or encouraging the replication of dangerous behaviors.[201] Although there is no research indicating that increased exposure to such risks definitively results in increased harms to children, according to UNICEF, "some studies show a positive association between internet use, risk encounters and negative outcomes... includ[ing] anxiety, depression, suicidal thoughts and panic disorder." Legislators enacted COPPA with the goal of enhancing parental involvement in their childrens' online activity "to help protect the safety of children in online fora."[202] If VPC—which mechanizes this enhanced parental involvement—is riddled with significant challenges, meeting this goal only becomes more difficult.

The Future of VPC

Although the FTC does not require operators subject to COPPA to use the FTC-enumerated verification methods for obtaining VPC, most operators rely (as a cautionary measure) on those methods for gaining consent. In 2013, COPPA was updated to allow the submission of VPC proposals to the FTC for review and formal approval.[203] Some operators employ novel methods for obtaining VPC, which often incorporate emerging technologies. This section describes how the FTC approves VPC proposals; proposed solutions to the VPC conundrum; emerging technologies and VPC; and the impact of state-level laws on children's privacy.

Considerations for Submitting VPC Proposals

The FTC does not require operators to use the approval mechanism. The commission added the approval mechanism in 2013 as a way to develop new approaches to VPC and receive formal assurance that their approach complies with COPPA. Successful VPC proposals must include 1) a detailed description of the proposed method and 2) an analysis of how the method is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.[204] The FTC approves non-proprietary methods that "can be used by the applicant or any other party."[205] Once an applicant files the VPC proposal with the FTC, the commission seeks and considers public comments and then issues a determination.[206]

The FTC has only approved two VPC proposals.

APPROVED VPC PROPOSALS

Since 2013, applicants have submitted VPC proposals six times, with only two successful approvals: "knowledge-based authentication" (KBA) in 2013 and "face match to verified photo identification" (FMVPI) in 2015.[207] Through the commission's determination process, it was clear that the FTC found it compelling that both methods have been used to verify identities in other rigorous settings. Although the FTC approved these two proposals, they are rarely implemented as people perceive them as onerous, expensive, or invasive of privacy.

KBA entails the use of dynamic, multiple-choice questions, including a "reasonable number" of questions with an "adequate number" of possible answers, which mitigate the risk of a non-parent user guessing the correct answer and accessing a site or service without obtaining parental consent.[208] The questions must be sufficiently difficult so that "a child age 12 or under in the parent's household could not reasonably guess or access the answers."[209] The commission noted that Imperium, the VPC applicant, used "out-of-wallet" questions whose answers were not located in the contents of an individual's wallet.[210] In its approval, the FTC noted that financial institutions and credit bureaus rely on KBA as a secure, effective mechanism for user authentication.[211]

FMVPI is a two-step facial recognition process that compares an image from a parent's photo ID (for example, a driver's license or passport) to a photo of the parent taken with the parent's phone or device camera.[212] The FTC found that although the process included elements of the current VPC method that checks government-issued ID against databases, the proposal was "more rigorous" because it involves verifying that the individual undergoing the VPC process is the person to whom the ID was issued.[213] The FTC pointed to several use cases in which facial recognition technology verifies identities: "retailers, financial institutions, and technology companies use facial recognition technology for safety and security purposes."[214]

REJECTED VPC PROPOSALS

The other four proposals were denied for various reasons: lack of novelty, prematurity, legal insufficiency, and asymmetry with COPPA. The FTC denied two proposals for their lack of novelty. One proposal incorporated two approved methods: verifying the parent's social security number and responding to knowledge-based questions. The FTC's response to iVeriFly's application suggests that the approval mechanism is for genuinely new mechanisms rather than to ensure that a company's method complies with COPPA.[215] Similarly, the FTC denied AgeCheq's initial application because the proposal incorporated already approved methods.[216] AgeCheq proposed a "common consent mechanism," which verified identity in two ways: verifying a parent's identity with a financial transaction and having the parent printing, signing, and returning a declaration form to AgeCheq.

The FTC rejected one method for prematurity. AssertID proposed a "social-graph verification" method that relied on a parent's network to verify the parent's identity and the parent-child relationship.[217] Since AssertID was unable to substantiate the proposal with sufficient research demonstrating that social graphs accurately determine a parent's identity, the method was rejected as premature.[218]

The FTC denied AgeCheq's second proposed VPC method, "Device-Signed Parental Consent Form," because it did not comply with COPPA. The proposed methos involved the parent registering with an intemediary company that handle certification, then entering personal information on a perental identity declaration form. The intermediary would then send a code to the parent's form, where the parent would enter the code and then digitally sign a certification verifying they owened the device.[219] Because the method involved sending a code via text message to the parent's phone, AgeCheq argued this was an adaptation of the approved method of physically signing and mailing or faxing a paper form.[220] AgeCheq also argued that the proposed method improved the existing method because it was more difficult to circumvent: when submitting paper forms, parents receive no record of the transmission, so a child could secretly send a form. However, the FTC found that a child could intercept the text message code and bypass the security requirement.[221] Thus, the FTC claimed that the method did not meet prong 2 of its requirement: it was not reasonably calculated to ensure that the person providing consent is the child's parent. The FTC noted that in the 2013 Rule, digital signatures were specifically excluded in the list of enumerated VPC methods because a digital signature alone is not a reliable method of obtaining VPC, and AgeCheq's "Device-Signed Parental Consent Form" did not "add indicia of reliability to the digital signature."[222]

The FTC also determined that this method did not comply with COPPA. COPPA permits an operator seeking VPC to collect a parent's contact information, defined as an email address, an instant messaging user identifier, a voice-over internet protocol identifier, or a video chat username. AgeCheq's proposed method required the collection of a mobile phone number and home address, which is not categorized as online contact information and, therefore, not suitable for the consent initiation process.[223]

No operators have submitted formal VPC proposals to the FTC since 2015, which means that the commission has not considered or approved new methods in approximately six years. As discussed, there is no requirement that operators receive approval before relying on an unenumerated VPC method—the approval process allows an operator to ensure their VPC method meets COPPA standards. However, because the FTC has denied methods when operators believed the method was "reasonable in light of available technology," operators may be reluctant to innovate and invest in developing new methods. Additionally, as technology improves, the FTC might consider methods denied in 2013, 2014, or 2015 as reasonable or sufficiently advanced such that previous concerns are no longer prohibitive. For example, in 2013 the FTC denied an

application of VPC that would involve "social-graph verification" because the technology did "not yet [have] adequate research or market testing" to demonstrate the technology's effectiveness.[224]

Suggested Solutions to VPC Challenges

Industry, advocates, and academics have been grappling with VPC requirements since COPPA's inception and have observed the successes, challenges, and other implications of VPC. Their perspective on the efficacy and enforceability of VPC is thus unique and valuable. This section outlines selected stakeholder proposals to address some of the challenges discussed above. Many of the proposed solutions introduce significant additional privacy and policy concerns that, if implemented, would have to be addressed. For example, many proposed solutions include the introduction of new methods or technology to facilitate VPC, which often include requiring operators to collect or facilitate the collection of additional personal information about children or their parents.

NEW REGULATORY APPROACHES TO VPC

Some stakeholders suggested alternative approaches to how the FTC currently lists appropriate VPC methods. Yoti, for example, suggested that the FTC eliminate the list and, instead, enumerate criteria for obtaining VPC. Yoti states that "the FTC could determine criteria that assures a minimum level of security and robustness, and any method that meets all the criteria could be acceptable," and even identifies potential criteria.[225] Yoti's examples include ensuring that the person providing consent is an adult, that identity documents belong to the individual undergoing VPC, and confirming that the person has "authority to act for the child."[226] The Center for Information Policy Leadership also supports an "outcome- or criteria-based approach to VPC instead of a specified list of consent methods."[227]

The Toy Association also favored an approach that gives operators flexibility regarding VPC methods: "Flexibility in allowing a variety of VPC methods tailored to different circumstances remains vital. It is costly to implement robust VPC and doing so results in significant drop-off of interest by parents. More restrictions that force companies to set up pay walls or other parental consent mechanisms will reduce, not foster, children's content online."[228] They urged the FTC to "allow operators the flexibility to choose among various VPC methods that work for their respective situations, as long as the approaches are reasonably calculated, in light of available technology."[229]

In contrast, SuperAwesome suggested "expanding the list of permitted verification methods to create a sliding scale that balances the risk of data processing against the intrusiveness and certainty of verification."[230] SuperAwesome also recommended "introducing a concept of 'proportional verification' which allows publishers (or service providers) to match the risk level of data processing to a verification method that ranges in certainty and intrusiveness. Rather than presenting three categories of verification (email, email+ and VPC), we propose introducing a 'sliding scale' that includes other, less intrusive methods. The FTC would be able to place their currently accepted verification means on this scale, while making it easier (and encouraging) the development of new methods."[231]

Some organizations urged the FTC to foster the development of additional methods through collaboration. The LEGO Group expressed a desire to "[c]onvene[] relevant stakeholders to further explore effective Verifiable Parental Consent (VPC) mechanisms that result in stronger protections for

children, are not disruptive to access or experience, and give parents clear control over what content their children are viewing."[232] The Association of National Advertisers expressed their hope that the commission would "leave avenues open for the development of new approaches to verifiable parental consent, such as a multi-stakeholder, one-stop-shop approach to facilitating consent online."[233]

The Center for Information Policy Leadership also supported a stakeholder engagement process, particularly because it could foster equity. The center urged the commission to "continue to examine additional parental consent methods that take into account important principles such as data minimization, equity and parental ease . . . it is important to consider methods for parents who are either unbanked, underbanked, or undocumented. The commission may want to consider convening stakeholders to consider new methods of VPC that are less disruptive to the sign-up or onboarding process, better informs parents and gives children stronger privacy protections while also providing easier access to online opportunities."[234]

ALTERNATIVE VPC METHODS

The VPC feedback reflected several common threads in stakeholders' suggestions. First, current methods of obtaining VPC may not achieve COPPA's goals in terms of efficacy and enforcement. Second, additional methods of obtaining VPC, particularly to allow more flexibility, should be explored. Several groups have proposed such methods or described what they should not be. Some of the proposals introduce additional privacy or policy risks that, if implemented, stakeholders must consider.

Mobile Phones

Many supported the use of mobile phones to obtain VPC. The Toy Association stated, "[t]oday's parents use their mobile phones. We urge the FTC to reconsider the option of asking children to furnish a parent's cell phone number as a way of offering notices to parents and initiating VPC where needed."[235] The FTC previously denied the use of mobile phones to collect VPC because it is difficult to verify, via a mobile parental consent form, that a parent or guardian is the one actually providing consent.[236] A child using the mobile phone could sign in lieu of their parents, and since there is no way to verify the signer's identity, the method does not meet COPPA requirements.[237] Additionally, the FTC found that such a process did not comply with COPPA regarding the type of information to be collected to verify parental identity.[238]

Regardless of these challenges, several other organizations agree that mobile phones are viable methods for obtaining VPC. The NCTA, The Internet & Television Association, supported the use of SMS text messages for VPC to allow approved methods to keep pace with technology developments, noting "the proposal for SMS/text messaging should not have been rejected by the commission because it would be useful today."[239] The Association of National Advertisers also supported text messages as a permissible method of obtaining VPC under the Rule.[240]

ESRB also recommended that the FTC consider expanding acceptable alternatives to email plus that allow text messages or electronic signatures, stating that even though "the commission has deemed text messages and electronic signatures unsuitable as standalone VPC mechanisms, it is worth revisiting them as alternatives to email plus."[241] ESRB also recommended that the FTC modernize VPC mechanisms by allowing the incorporation of fingerprint and facial recognition, especially because those features are often on a parent's mobile device.[242]

Platform-Mediated VPC

Several organizations urged the FTC to consider whether and how platforms can mediate the VPC process. Princeton University's Center for Information Technology Policy (CITP) suggested, "One way in which platforms could assist with COPPA compliance is by uniformly flagging users who are under 13,"[243] arguing that this process "could mitigate the need for app developers and content creators to implement their own audience management or age gating" while also "providing verifiable parental consent mechanisms."[244] CITP also noted that "major mobile operating systems already provide for linked parent and child accounts; if they also provided a software interface for child accounts to submit permission requests to parent accounts, apps and content could have a convenient and free means of obtaining verifiable parental consent."[245]

Similarly, the Developers Alliance indicated that "many developers believe that the burden for verification should instead be on the platforms, rather than the individual companies themselves. This would ensure a more coherent compliance mechanism and cut down the amount of overall friction between the end-users and the apps."[246] ESRB also pointed to platforms as a possible solution, and urged the FTC to "explore steps to engage platforms in the VPC process."[247] ESRB reasoned that "parents will continue to push back on VPC collected on a service-by-service basis" but may be more amenable to providing VPC "if they can provide the necessary verification once to a trusted party, and that verification can be shared with other third-party operators." Beyond platforms mediating VPC itself, safe harbor PRIVO suggested that the commission encourages the development and adoption of a "a uniform signal by which a device or browser can give operators notice that the primary user of the device is a child" which would also assist operators in complying "in jurisdictions that implement protections for children 13 years of age or older."[248]

VPC During Setup When at the Direction of a Parent

With regard to products purchased by adults for the use of children, The Toy Association noted that "if consent is needed, it can be provided only by the adult purchaser of the connected children's product," and urged the FTC to "formally recognize that parental consent by the parent who purchased a connected children's product fully satisfies the operator's COPPA obligations."[249] CTIA suggested that VPC should be obtained through the set-up process for services that collect personal information from children at the direction of their parents.[250] CTIA posited that "[s]pecifically, the FTC should recognize that a notice that is made available to consumers prior to purchase or use (e.g., on product packaging or during product set-up) and clearly discloses that the product or service may collect information from a child, may give rise to verifiable parental consent."[251]

Alternatives to Credit Card

Several commentators criticized the currently approved VPC method involving use of a credit or debit card or other online payment system whereby the card holder receives notification of each separate transaction. The NCTA opined that the FTC should "revisit its decision to limit use of payment cards only to situations where a monetary transaction is completed" because "[h]aving the added requirement that an actual transaction must occur is an obstacle for companies trying to provide free child-friendly content, including in a paid-for subscription service, from adopting this method of verifiable parental consent."[252] Pokemon, too, favored looking into additional ways to obtain VPC, beyond credit card verification. Their feedback stated that the commission "should explore methods of obtaining VPC without the use of credit card verification and the costs/benefits on non-credit card based consent."[253]

The Association of National Advertisers indicated its support for an expansion of the credit card VPC method but noted that the current method is inequitable, specifically noting the complications that the unbanked

population faces.[254] ANA argued that the method "should be broadened to allow parents to use other kinds of financial instruments. At a minimum, companies should be able to obtain verifiable parental consent by requesting a valid credit card from a parent even if the consent is not obtained in connection with a monetary transaction."[255]

AMENDING THE PROPOSAL PROCESS

Some organizations' feedback focused on the mechanism of the VPC proposal process itself. To incentivize operators to submit VPC proposals, The Software and Information Industry Association encouraged the commission to "consider shortening the current determination window from 120 days and allow for more robust feedback and communication between the applicant and the commission during consideration of new parental consent methods."[256]

Other submissions proposed new frameworks altogether. Yoti posited that "[r]ather than the typical public consultation period for new methods of consent, the FTC may also wish to consider the merits of either an independent review panel to assess and give feedback to potential new COPPA approaches or a regtech sandbox approach where COPPA approaches could be 'tested' over a controlled period."[257] Although safe harbors do play this role in the existing framework, this proposal would create an entirely separate mechanism for raising VPC proposals. FOSI proposed an additional framework, after describing how the "lack of effective, easy-to-implement, and affordable mechanisms expose companies to unnecessary liability without meaningfully enhancing children's privacy"—FOSI "strongly urge[d] the commission to promote the development of additional mechanisms to obtain consent where required and then swiftly approve them."[258]

Emerging Technologies, State Law Considerations, and VPC

Some companies have started to incorporate age verification and age-estimation methods into the age screening and VPC processes. By doing so, companies can provide additional verification that a user is or is not a child and that an adult is providing the required consent. For example, Yoti's age-estimation tool uses machine learning to scan a user's face to determine whether the user falls within a certain age range, for example, over or under the age of 13.[259] According to the company, such technology can help remove barriers that people without government-issued identification face in the VPC process, in terms of verifying their age. Yoti also introduced Age Scan technology, which uses facial analysis to identify whether an individual is over or under 18.[260]

Some companies have announced the use of in-house age verification or estimation technology as an additional measure, to ensure that young people who may circumvent traditional age gates or screens have safe, age-appropriate experiences. For example, in July 2021, Facebook announced updates to Instagram and Facebook (which prohibit users under 13) that incorporate artificial intelligence to ensure a user's actual and stated ages match.[261]

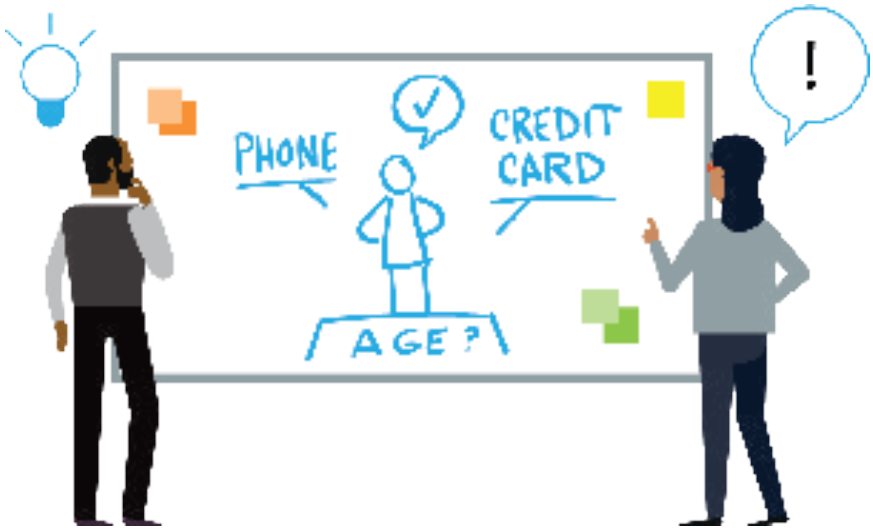
The FTC has yet to comment on the privacy implications of age assurance mechanisms. In October 2021, the United Kingdom's data protection regulator, the Information Commissioner's Office, issued an opinion on how implementation of age assurance mechanisms can align with the UK's Age Appropriate Design Code (discussed on p. __). However, the Code differs significantly from COPPA and explicitly discusses the use of age assurance tools, along with other, more modern approaches to designing safe online environments for children.[262] The ICO recognized the value of age assurance as a method for protecting children's privacy. Nonetheless, as the ICO states, although age assurance methods are useful for ensuring age-appropriate online experiences for children, age assurance solutions also have risks, including additional intrusiveness, bias, inaccuracy, and circumvention.[263]

Companies could soon use this technology to verify whether an individual is over or under 13, but risks of age assurance based on profiling or biometrics include algorithmic bias for non-white and disabled people as well as privacy risks based on the technique's intrusiveness—concerns noted by the ICO's 2021 opinion on age assurance technology.[264] In 2021, the ICO formally approved an age assurance certification scheme.[265] Certification schemes act similarly to the FTC's COPPA safe harbors, by providing companies with a framework for and assurance of compliance with the country's data protection requirements. The ICO's approved "Age Check Certification Scheme" tests whether certain age assurance products can effectively estimate or verify a user's age.[266]

State-level restrictions may hinder providers from innovating regarding VPC in the United States. For example, Illinois's Biometric Information Privacy Act (BIPA) requires companies to obtain consent before collecting or disclosing biometric identifiers.[267] If a company attempts to innovate with a method for obtaining VPC that includes collecting biometric information, the company's risk analysis would need to consider BIPA. BIPA also includes a private right of action that allows individuals to sue companies for violating the law.

In its 2019 COPPA Rule Review, the FTC requested responses to whether the Rule should be "more specific about the appropriate methods for determining the age of users." In its response, both CARU and PRIVO, COPPA safe harbors, noted the importance of strengthening age gates and screens. CARU noted that existing age gates and screens "should be the lowest bar for compliance with the law."[268] Both safe harbors also expressed significant concerns about children circumventing age gates and screens. CARU finds that "techniques that effectively restricted access and prevented children from breaching protections are quickly becoming obsolete" due to children circumventing existing methods, by, for example "back-buttoning and changing their age" once they are prevented from accessing a site, which goes against FTC guidance.[269] In alignment with the FTC's guidance, in its Self-Regulatory Guidelines, CARU requires that use of age-screening mechanisms must be "in conjunction with technology" and provides the example of session cookies, which helps "prevent underage children from going back and changing their age to circumvent age-screening."[270] In addition, PRIVO noted that "the only way that age could be changed is if the user were to delete the app and download it again entering different details."[271] Further, PRIVO suggested there should be higher standards for screening children out of services depending on the risk associated with certain data: "if the service collects and processes personal data that would be considered high risk, i.e. public sharing of images, video, free text and communications, then age gates are not robust enough of a mechanism and a secondary authentication level should be required."[272] Beyond this suggestion, PRIVO also noted that mechanisms which allow parents to register a child's device and signal that a device is used by a child can be used to limit children circumventing age gates or screens.[273]

Concluding Thoughts



Our findings identify significant challenges to getting VPC right in the current regulatory and legislative environment. Not only do these challenges present complications regarding how operators comply with the law, they also present potential barriers to children accessing online experiences with their caregivers' knowledge and approval, thereby risking exposing children to unsuitable experiences. Several stakeholders have presented potential solutions to the current landscape, including modernizing current approved VPC methods, updating the current VPC proposal process, and the FTC conducting broad stakeholder engagement to understand and develop workable solutions.

However, these challenges are not happening in isolation; children's privacy protections are rapidly developing around the world, to include fundamental digital rights and protections for children online. As U.S. legislators and regulators consider modernizing COPPA or new children's privacy frameworks, the question of how to appropriately and effectively obtain VPC remains essential. To develop solutions to the current challenges of VPC, stakeholders must consider the perspectives of children, parents, industry representatives, advocates, and academics.

ENDNOTES

1 15 U.S.C. § 6501.
2 Common Sense Media, *The Common Sense Census: Media Use by Kids Age Zero to Eight* (2020), https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-kids-age-zero-to-eight-2020.
3 UNICEF, *How many children and young people have internet access at home?; Estimating digital connectivity during the COVID-19 pandemic* (December 2020), https://data.unicef.org/resources/children-and-young-people-internet-access-at-home-during-covid19/
4 Lisa M. Given, Denise Cantrell Winkler, Rebekah Wilson, Christina Davidson, Susan Danby, and Karen Thorpe, *Documenting young children's technology use: Observations in the Homem* Proceedings of the American Society for Information Science and Technology (2015), 51 (1): 1-9, https://asistdl.onlinelibrary.wiley.com/doi/full/10.1002/meet.2014.14505101028?casa_token=8n5NkFuu-42wAAAAA%3Ao0T7W3EeYuLBC0gpolOmMJjqeBU-kX4B7vUd9_nt_YIVzf_7m_ofHUzmEk2WvPk1Z05CsVEdcxDI
5 Family Online Safety Institute, *Connected Families: How Parents Think & Feel about Wearables, Toys, and the Internet of Things* (2017), http://fosi-assets.s3.amazonaws.com/media/documents/HartReport_d7_full_report_WEB.pdf.
6 Ibid.
7 Ibid.
8 Ibid.
9 Ibid.
10 38% of parents reported their child had their own social media account, and 28% of parents reported their child had their own email account. Ibid.
11 89% of parents of a child aged 5 to 11 say their child watches videos on YouTube; 81% of those who have a child ages 3 to 4 and 57% of those who have a child 2 years old or younger.
Pew Research Center, *Parenting Children in the Age of Screens* (July 28, 2020), https://www.pewresearch.org/internet/2020/07/28/parenting-children-in-the-age-of-screens/.
12 Ryan Tuchow, *Mobile gaming up 9% among kids,* Kidscreen (January 19, 2021), https://kidscreen.com/2021/01/19/mobile-gaming-up-9-among-kids/.
13 Duncan Stewart, Allan V. Cook, and Kevin Westcott, *From virtual to reality: Digital reality headsets in enterprise and education: TMT Predictions 2021*, Deloitte (December 7, 2020), https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2021/vr-immersive-technologies.html/#endnote-2.
14 Toca Boca, Apps, *Toca Hair Salon,* https://tocaboca.com/app/toca-hair-salon/.
15 Federal Trade Commission, *Taking Care: The American Approach to Protecting Children's Privacy* (2018), Accessed June 23, 2021, https://www.ftc.gov/system/files/documents/public_statements/1422695/phillips_-_taking_care_11-15-18_0.pdf.
16 Daniel J. Solove, *A Brief History of Information Privacy Law* in *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, Practising Law Institute (2006): 1-24.
17 Ibid, citing Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 44.
18 Ibid, citing U.S. Department of Health, Education, and Welfare, *Records, Computers,and the Rights of Citizens: Report of the Secretary's Advisory Comm. on Automated Personal Data Systems* (July 1973).
19 5 U.S.C. § 552a.
20 5 U.S.C. § 552a.
21 5 U.S.C. § 552a.
22 5 U.S.C. § 552a.
23 Amelia Vance and Casey Waughn, *Student Privacy's History of Unintended Consequences*, 44 Seton Hall Leg. J. 3, 520-2 (2020), https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1172&context=shlj.
24 Ibid.
25 Ibid.
26 Ibid.
27 Ibid.
28 Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.
29 Ibid.
30 https://web.archive.org/web/20030622142444/https://www.ftc.gov/os/1997/07/cenmed.htm
31 https://web.archive.org/web/20030622142444/https://www.ftc.gov/os/1997/07/cenmed.htm
32 Federal Trade Commission, Press Releases, *FTC Staff Sets Forth Principles for Online Information Collection from Children* (July 16, 1997), https://www.ftc.gov/news-events/press-releases/1997/07/ftc-staff-sets-forth-principles-online-information-collection
33 Ibid.
34 Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.
35 Ibid.
36 Ibid.
37 Ibid.
38 Ibid.
39 Ibid.
40 Ibid.
41 Ibid.
42 Ibid.
43 Ibid.
44 Ibid.
45 105 Cong. Rec. S8482 (July 17, 1998).
46 105 H.R. H.R.4667.

ENDNOTES

47 105 Cong. Rec. S8482 (July 17, 1998).
48 105 Cong. Rec. S8482-3 (July 17, 1998).
49 105 Cong. Rec. S8482 (July 17, 1998).
50 105 Cong. Rec. E1861 (Oct. 1, 1998).
51 105 Cong. Rec. S8482 (July 17, 1998).
52 105 Cong. Rec. S8482 (July 17, 1998).
53 105 Cong. Rec. S8483 (July 17, 1998).
54 United Nations Human Rights Office of the Commissioner, *Convention on the Rights of the Child* (November 1989), Accessed September 17, 2021, https://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx.
55 UNICEF, *Frequently Asked Questions on the Convention on the Rights of the Child*, Accessed September 16, 2021, https://www.unicef.org/child-rights-convention/frequently-asked-questions .
56 United Nations Treaty Collection, *Convention on the Rights of the Child* (November 1989), Accessed September 17, 2021, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11&chapter=4&clang=_en.
57 The Organisation for Economic Co-operation and Development, *About the OECD*, Accessed September 17, 2021, https://www.oecd.org/about/.
58 Ibid.
59 The Organisation for Economic Co-operation and Development, *Recommendation of the Council on Children in the Digital Environment,* OECD Legal Instruments (May 30, 2021), Accessed September 17, 2021, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389.
60 The UK Information Commissioner's Office (ICO) explained that, post-Brexit, "the GDPR is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review." Information Commissioner's Office, *The UK GDPR,* https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/.
61 GDPR Recital 38, *Special Protection of Children's Personal Data.*
62 Tay Nguyen, GDPR Matchup: The Children's Online Privacy Protection Act, IAPP Privacy Tracker (April 5, 2017), https://iapp.org/news/a/gdpr-matchup-the-childrens-online-privacy-protection-act/.
63 GDPR Article 8(1).
64 GDPR Article 8(2).
65 GDPR Article 6(1)(f).
66 European Commission, *Guidelines on Transparency Under Regulation 2016/679*, European Commission Newsroom (November 29, 2017), https://ec.europa.eu/newsroom/article29/items/622227; Information Commissioner's Office, *Children and the GDPR* (March 22, 2018), https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf.
67 European Commission, *Communication From the Commission of the European Parliament and the Council* (June 24, 2020), https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v6_1.pdf.
68 Ibid.
69 Jasmine Park, *The European Commission Considers Amending the General Data Protection Regulation to Make Digital Age of Consent Consistent*, Future of Privacy Forum (July 21, 2021), https://fpf.org/blog/the-european-commission-considers-amending-the-general-data-protection-regulation-to-make-digital-age-of-consent-consistent/.
70 European Commission, *Pilot Program: Outline and trial an infrastructure dedicated to the implementation of child rights and protection mechanisms in the online domain*, Call for Proposals (2020), https://ec.europa.eu/digital-single-market/en/news/pilot-project-outline-and-trial-infrastructure-dedicated-implementation-child-rights-and.
71 euCONSENT (2021), https://euconsent.eu/
72 "The GDPR is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the [Data Protection Act of 2018]." Information Commissioner's Office, *The UK GDPR*, https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/.
73 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/.
74 The Organisation for Economic Co-operation and Development, *Recommendation of the Council on Children in the Digital Environment*, OECD Legal Instruments (May 30, 2021), Accessed September 17, 2021 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389.
75 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.
76 Ibid.
77 Information Commissioner's Office, *Online Tools,* 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/15-online-tools/.
78 Jihong Chen, *China: Data Protection & Cyber Security*, The Legal 500 Country Comparative Guides (2021), https://www.legal500.com/guides/chapter/china-data-protection-cyber-security/?export-pdf.
79 Hunter Dorwart, Gabriela Zanfir-Fortuna, and Clarisse Girot, *China's New Comprehensive Data Protection Law: Context, Stated Objectives, Key Provisions*, Future of Privacy Forum (August 20, 2021), https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/.
80 Jihong Chen, *China: Data Protection & Cyber Security*, The Legal 500 Country Comparative Guides (2021), https://www.legal500.com/guides/chapter/china-data-protection-cyber-security/?export-pdf.
81 Liu Jiaxin, *Newly revised law on minors protection highlights online safety*, CGTN (June 1, 2021), https://news.cgtn.com/news/2021-06-01/Newly-revised-law-on-minors-protection-highlights-online-safety-10JK9ZuSCLS/index.html.

ENDNOTES

82 Ibid.
83 《关于进一步严格管理 切实防止未成年人沉迷网络游戏的通知，National Press and Publication Administration, (August 30, 2021), http://www.nppa.gov.cn/nppa/contents/719/98785.shtml.
84 Kevin Webb, *Kids in China are trying every trick in the book to beat the facial recognition software that puts a mandatory time limit on popular video games*, Business Insider (December 15, 2018), https://www.businessinsider.com/china-facial-recognition-video-games-2018-12.
85 《关于进一步严格管理 切实防止未成年人沉迷网络游戏的通知，National Press and Publication Administration, (August 30, 2021), http://www.nppa.gov.cn/nppa/contents/719/98785.shtml.
86 Mr Lim Chong Kin, *Singapore: Data Protection & Cyber Security*, The Legal 500 Country Comparative Guides (2021), https://www.legal500.com/guides/chapter/singapore-data-protection-cyber-security/?export-pdf.
87 Ibid.
88 Cho Mu-Hyun, *South Korea strengthens child data protection laws*, ZDNet (June 24, 2019), https://www.zdnet.com/article/south-korea-strengthens-child-data-protection-laws/.
89 Ibid.
90 Ibid.
91 Doil Son, Sun Hee Kim, and Chris H. Kang, *South Korea: Data Protection & Cyber Security*, The Legal 500 Country Comparative Guides (2021), https://www.legal500.com/guides/chapter/south-korea-data-protection-cyber-security/?export-pdf.
92 Ana Carolina Cagnoni, *How Brazil regulates children's privacy and what to expect under the new data protection law*, International Association of Privacy Professionals (October 29, 2019), https://iapp.org/news/a/how-brazil-regulates-childrens-privacy-and-what-to-expect-under-the-new-data-protection-law/.
93 *Brazil: Statute of the Child and Adolescent, Law n° 8.069* (July 13, 1990), https://www.refworld.org/docid/4c481bcf2.html.
94 Ricardo Barretto Ferreira de Silva, Lorena Pretti Serraglio. Camilla Lopes Chicaroni, Nariman Ferdinian Gonzales, and Isabella da Penha Lopes Santana, *Brazil: Data Protection & Cyber Security*, The Legal 500 Country Comparative Guides (2021), https://www.legal500.com/guides/chapter/brazil-data-protection-cyber-security/?export-pdf.
95 Ana Carolina Cagnoni, *How Brazil regulates children's privacy and what to expect under the new data protection law*, International Association of Privacy Professionals (October 29, 2019), https://iapp.org/news/a/how-brazil-regulates-childrens-privacy-and-what-to-expect-under-the-new-data-protection-law/.
96 International Association of Privacy Professionals, *Brazilian General Data Protection Law (LGPD, English Translation*) (2019), https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/.
97 Ibid.
98 "Over the last two decades, COPPA has defined children's online experience around the globe and COPPA-like provisions have been exported into all digital markets, including the UK's." 5Rights Foundation, *But how do they know it is a child? Age Assurance in the Digital World*, (October 2021), https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf.
99 Information Commissioner's Office, *Age Appropriate Application,* 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/3-age-appropriate-application/.
100 Simone van der Hof, *I Agree... Or Do I? – A Rights-Based Analysis of the Law on Children's Consent in the Digital World*, Wisconsin International Law Journal (2016), 34 (2): 101-136, Accessed June 24, 2021, https://scholarlypublications.universiteitleiden.nl/access/item%3A2944101/view.
101 Ibid.
102 GDPR Article 8(2).
103 15 U.S.C. § 6501.
104 Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions* (2020), Accessed June 10, 2021, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0.
105 Ibid.
106 16 C.F.R. § 312.2
107 Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions* (2020), Accessed June 10, 2021, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0.
108 Ibid.
109 Ibid.
110 In the United States, age screening mechanisms are also used to determine whether a user does or does not qualify to participate in a particular service.
111 Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions* (2020), Accessed August 10, 2021, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0.
112 16 CFR § 312.4
113 16 CFR § 312.4
114 16 CFR § 312.4
115 16 CFR § 312.4
116 Federal Trade Commission, *Verifiable Parental Consent and the Children's Online Privacy Rule*, Accessed June 10, 2021, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/verifiable-parental-consent-childrens-online-privacy-rule.
117 Supra, p. __.
118 Federal Trade Commission, *Verifiable Parental Consent and the Children's Online Privacy Rule*, Accessed June 10, 2021, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/verifiable-parental-consent-childrens-online-privacy-rule.
119 16 C.F.R. § 312.2: (definition of "collection")
120 Ibid.
121 Including but not limited to an IP address, a unique cookie ID, and a device ID.

ENDNOTES

122 16 C.F.R. § 312.2: (definition of "persistent identifier")
123 Thomas Germain, *How a Photo's Hidden "Exif" Data Exposes Your Personal Information,* Consumer Reports (December 6, 2019), https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data/.
124 Federal Trade Commission, *Federal Trade Commission Enforcement Policy Statement Regarding the Applicability of the Children's Online Privacy Protection Act Rule to the Collection and Use of Voice Recordings* (October 20, 2017), https://www.ftc.gov/public-statements/2017/10/federal-trade-commission-enforcement-policy-statement-regarding.
125 Ibid.
126 "Where a school has contracted with an operator to collect personal information from students for the use and benefit of the school, and for no other commercial purpose, the operator is not required to obtain consent directly from parents under COPPA, and can presume that the school's authorization for the collection of students' personal information is based upon the school having obtained the parents' consent." Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions* (2020), Accessed June 10, 2021, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0.
127 Ibid.
128 Ibid.
129 Ibid.
130 Ibid.
131 Ibid. *See also* Final Rule Amendments, 78 Fed Reg. 3972, 3981 (Jan. 17, 2013), https://www.govinfo.gov/content/pkg/FR-2013-01-17/pdf/2012-31341.pdf.
132 The FTC has also made it clear that a technical cookie flag can be sent to disengage targeting when a user is a child, without violating COPPA.
133 16 C.F.R. § 312.5(b)(2)
134 Infra, p. ___.
135 Lesley Fair, *Do your COPPA Safe Harbor claims hold water?,* Federal Trade Commission (May 19, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/05/do-your-coppa-safe-harbor-claims-hold-water.
136 Chris Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, (2016), Cambridge University Press.
137 Federal Trade Commission, *COPPA Safe Harbor Program,* https://www.ftc.gov/safe-harbor-program
138 In its 2013 rulemaking, the FTC reasoned that "it cannot be the responsibility of parents to try to pierce the complex infrastructure of entities that may be collecting their children's personal information through any one site. For child-directed properties, one entity, at least, must be strictly responsible for providing parents notice and obtaining consent when personal information is collected through that site." See Federal Trade Commission, 16 C.F.R. Part 312: Children's Online Privacy Protection Rule: Final Rule Amendments and Statement of Basis and Purpose (Dec. 19, 2012), available at https://www.ftc.gov/system/files/2012-31341.pdf.
139 Infra p. ___.
140 Some social media platforms may provide "child directed" configurations. (see e.g., Information for Child-Directed Sites and Service, https://developers.facebook.com/docs/plugins/restrictions/; https://support.twitter.com/articles/20171365;) while other social media platforms do not (see e.g., https://dev.twitter.com/web/wordpress).
141 Mobile App Child Privacy Settlements, Accessed August 10, 2021, https://web.archive.org/web/20210414202400/https://mobileappchildprivacysettlements.com/.
142 Google Ad Manager Help, *Tag an ad request for child-directed treatment (TFCD),* Accessed August 10, 2021, https://support.google.com/admanager/answer/3671211?hl=en.
143 ironSource Knowledge Center, *COPPA and child-directed apps,* Accessed August 10, 2021, https://developers.is.com/ironsource-mobile/general/ironsource-mobile-child-directed-apps/#step-2.
144 Google Ad Manager Help, *Tag an ad request for child-directed treatment (TFCD),* Accessed August 10, 2021, https://support.google.com/admanager/answer/3671211?hl=en.
145 Steve Bellovin, *COPPA and signaling*, Federal Trade Commission (January 2, 2013), Accessed August 10, 2021, https://www.ftc.gov/news-events/blogs/techftc/2013/01/coppa-signaling.
146 16 C.F.R. § 312.8
147 Federal Trade Commission, Press Releases, *FTC Requires Zoom to Enhance its Security Practices as Part of Settlement* (November 9, 2020), Accessed July 7, 2021, https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement.
148 Lesley Fair, *VTech settlement cautions companies to keep COPPA-covered data secure*, Federal Trade Commission (January 8, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/01/vtech-settlement-cautions-companies-keep-coppa-covered-data.
149 Federal Trade Commission, *VTech Case File,* Case No. 1:18-cv-114 (2018), https://www.ftc.gov/system/files/documents/cases/vtech_file_stamped_stip_order_1-8-18.pdf.
150 Ibid.
151 Federal Trade Commission, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, (2017), Accessed June 10, 2021, https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step4.
152 There are certain exceptions where enforcement has touched on the distinctions between the types of groups. Federal Trade Commission, *Cases Tagged with Children's Online Privacy Act (COPPA),* https://www.ftc.gov/enforcement/cases-proceedings/terms/336.
153 Ariel Fox Johnson, *13 Going on 30: An Exploration of Expanding COPPA's Privacy Protections to Everyone*, Seton Hall Legislative Journal (2020), 44 (3): 419-455, Accessed June 23, 2021, https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1168&context=shlj.
154 Sheila F. Anthony, *Statement on The Subcommittee on Telecommunications, Trade and Consumer Protection,* Federal Trade Commission, (July 21, 1998), https://www.ftc.gov/public-statements/1998/07/statement-subcommittee-telecommunications-trade-consumer-protection.
155 Federal Trade Commission, *Taking Care: The American Approach to Protecting Children's Privacy*, (2018), Accessed June 23, 2021, https://www.ftc.gov/system/files/documents/public_statements/1422695/phillips_-_taking_care_11-15-18_0.pdf.

ENDNOTES

156 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.
157 Federal Trade Commission, *Taking Care: The American Approach to Protecting Children's Privacy* (2018), Accessed June 23, 2021, https://www.ftc.gov/system/files/documents/public_statements/1422695/phillips_-_taking_care_11-15-18_0.pdf.
158 Ibid.
159 Lauren A. Matecki, *Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era,* Northwestern Journal of Law & Social Policy (2010), 5 (2): 369-402, Accessed June 23, 2021, https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1058&context=njlsp.
160 Ariel Fox Johnson, *13 Going on 30: An Exploration of Expanding COPPA's Privacy Protections to Everyone*, Seton Hall Legislative Journal (2020), 44 (3): 419-455, Accessed June 23, 2021, https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1168&context=shlj.
161 Emily DiRoma, *Kids Say the Darndest Things: Minors and the Internet*, Cardozo Law Review (2019): 43-75, Accessed June 23, 2021, http://cardozolawreview.com/wp-content/uploads/2019/08/DiRoma.pdf.
162 Ariel Fox Johnson, *13 Going on 30: An Exploration of Expanding COPPA's Privacy Protections to Everyone*, Seton Hall Legislative Journal (2020), 44 (3): 419-455, Accessed June 23, 2021, https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1168&context=shlj.
163 Lauren A. Matecki, *Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era,* Northwestern Journal of Law & Social Policy (2010), 5 (2): 369-402, Accessed June 23, 2021, https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1058&context=njlsp.
164 Simone van der Hof, *I Agree... Or Do I? – A Rights-Based Analysis of the Law on Children's Consent in the Digital World*, Wisconsin International Law Journal (2016), 34 (2): 101-136, Accessed June 24, 2021, https://scholarlypublications.universiteitleiden.nl/access/item%3A2944101/view.
165 Ibid.
166 5Rights Foundation, *But how do they know it is a child? Age Assurance in the Digital World*, (October 2021), https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf.
167 Ibid.
168 Ibid.
169 Ibid.
170 Federal Trade Commission, Public Submission, *Yoti Response to the Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule* (March 22, 2020), https://www.regulations.gov/comment/FTC-2019-0054-113202.
171 Id.
172 Federal Trade Commission, Public Submission, *Comments of Computer & Communications Industry Association* (March 25, 2020), https://www.regulations.gov/comment/FTC-2019-0054-117085.
173 Federal Trade Commission, Public Submission, *SuperAwesome Comments on Public Consultation on the Effectiveness of COPPA* (December 11, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25091.
174 Herb Weisbaum, *How young is too young for a kid to have a credit card?,* NBC News (August 6, 2019), https://www.nbcnews.com/better/lifestyle/how-young-too-young-kid-have-credit-card-ncna1039536.
175 Federal Trade Commission, Public Submission, *SuperAwesome Comments on Public Consultation on the Effectiveness of COPPA* (December 11, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25091.
176 These are prevalent methods, but not the only methods -- the FTC also offers other methods, such as a signed consent form or phone call.
177 Federal Trade Commission, Public Submission, *Comments of Internet Association* (March 25, 2020), https://www.regulations.gov/comment/FTC-2019-0054-117011.
178 Elaine Kamarck and Christine Stenglein, *How many undocumented immigrants are in the United States and who are they?*, Brookings Policy 2020 (November 12, 2019), https://www.brookings.edu/policy2020/votervital/how-many-undocumented-immigrants-are-in-the-united-states-and-who-are-they/.
179 Infra, p. __.
180 Federal Trade Commission, Public Submission, *Google's Response to Request for Comments on the FTC's Implementation of the Children's Online Privacy Protection Rule* (December 9, 2019), https://www.regulations.gov/comment/FTC-2019-0054-21661.
181 Federal Trade Commission, Public Submission, *LEGO's Response to Request for Comments on the FTC's Implementation of the Children's Online Privacy Protection Rule* (December 12, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25188.
182 Federal Trade Commission, Public Submission, *Khan Academy's Response to Request for Public Comment on COPPA* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116444.
183 EPIC, *Children's Online Privacy Protection Act (COPPA)*, https://epic.org/privacy/kids/.
184 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.
185 Federal Trade Commission, *Transcript of The Future of the COPPA Rule: An FTC Workshop Part 2* (October 7, 2019), https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_part_2_1.pdf.
186 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.
187 Federal Trade Commission, Public Submission, *LEGO's Response to Request for Comments on the FTC's Implementation of the Children's Online Privacy Protection Rule* (December 12, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25188.
188 Federal Trade Commission, Public Submission, *Khan Academy's Response to Request for Public Comment on COPPA* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116444.
189 Federal Trade Commission, Public Submission, *Comments of the Family Online Safety Institute* (March 22, 2020), https://www.regulations.gov/comment/FTC-2019-0054-113172.
190 Ibid.

ENDNOTES

191 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.
192 Federal Trade Commission, Public Submission, *Entertainment Software Rating Board COPPA Rule Review Comments* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116012.
193 Federal Trade Commission, Public Submission, *SuperAwesome Comments on Public Consultation on the Effectiveness of COPPA* (December 11, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25091.
194 Federal Trade Commission, Public Submission, *Comments Submitted by The Toy Association re: COPPA Rule Review* (December 9, 2019), https://www.regulations.gov/comment/FTC-2019-0054-21672.
195 Federal Trade Commission, Public Submission, *Comments of Internet Association* (March 25, 2020), https://www.regulations.gov/comment/FTC-2019-0054-117011.
196 Federal Trade Commission, Public Submission, *Comment Submitted by Office of the Arizona Attorney General* (April 8, 2020), https://www.regulations.gov/comment/FTC-2019-0054-118870.
197 Federal Trade Commission, Public Submission, *Comments of CTIA* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116136.
198 Ibid.
199 L. Pasquale et al., *Digital Age of Consent and Age Verification: Can They Protect Children?*, IEEE Software, (December 2020), Accessed October 21st, 2021, https://ieeexplore.ieee.org/document/9295422.
200 C.S. Mott Children's Hospital, *Sharing Too Soon? Children and Social Media Apps*, Mott Poll Report (2021) 39 (4) Accessed October 21st, 2021, https://web.archive.org/web/20211018120937/https://mottpoll.org/sites/default/files/documents/101821_SocialMedia.pdf.
201 Beata Mostafavi, *A Third of Children Ages 7-9 Use Social Media Apps*, Michigan Health, (October 18, 2021), Accessed October 21st, 2021, /web/20211025222835/https://healthblog.uofmhealth.org/childrens-health/a-third-of-children-ages-7-9-use-social-media-apps.
202 144 Cong. Rec. S12787 (October 21, 1998).
203 16 C.F.R. § 312.12
204 16 C.F.R. §§ 312.12(a).
205 Federal Trade Commission, *FTC Grants Approval for New COPPA Verifiable Parental Consent Method* (December 23, 2013), Accessed June 10, 2021, https://www.ftc.gov/news-events/press-releases/2013/12/ftc-grants-approval-new-coppa-verifiable-parental-consent-method.
206 16 C.F.R. §§ 312.12(a).
207 Federal Trade Commission, *Verifiable Parental Consent and the Children's Online Privacy Rule*, Accessed June 10, 2021, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/verifiable-parental-consent-childrens-online-privacy-rule.
208 Federal Trade Commission, *FTC Grants Approval for New COPPA Verifiable Parental Consent Method* (December 23, 2013), Accessed June 10, 2021, https://www.ftc.gov/news-events/press-releases/2013/12/ftc-grants-approval-new-coppa-verifiable-parental-consent-method.
209 Ibid.
210 Ibid.
211 Ibid.
212 Ibid.
213 Ibid.
214 Ibid.
215 Federal Trade Commission, *FTC Concludes Review of iVeriFly, Inc.'s Application for Approval as a COPPA Verifiable Consent Mechanism* (February 24, 2014), https://www.ftc.gov/system/files/attachments/press-releases/ftc-concludes-review-iveriflys-proposed-coppa-verifiable-parental-consent-method/140225iveriflyapplicationletter.pdf.
216 Federal Trade Commission, *FTC Concludes Review of AgeCheq Inc.'s Application for Approval of Verifiable Parental Consent Method* (November 21, 2014), https://www.ftc.gov/system/files/attachments/press-releases/ftc-concludes-review-agecheqs-initial-proposed-coppa-verifiable-parental-consent-method/141121agecheqapplication.pdf.
217 Federal Trade Commission, *FTC Denies AssertID's Application for Proposed COPPA Verifiable Parental Consent Method*, (November 13, 2013), Accessed June 10, 2021, https://www.ftc.gov/news-events/press-releases/2013/11/ftc-denies-assertids-application-proposed-coppa-verifiable.
218 Ibid.
219 Federal Trade Commission, *AgeCheq Inc.'s Application Pursuant to Section 312.12(a) of the Final Children's Online Privacy Protection Rule for Approval of Parental Consent Method Not Currently Enumerated in §312.5(b)* (October 1, 2014), https://www.ftc.gov/system/files/documents/public_statements/621461/141119agecheqapplication-2.pdf.
220 Federal Trade Commission, *AgeCheq Inc.'s Application Pursuant to Section 312.12(a) of the Final Children's Online Privacy Protection Rule for Approval of Parental Consent Method Not Currently Enumerated in §312.5(b)* (October 1, 2014), https://www.ftc.gov/system/files/documents/public_statements/621461/141119agecheqapplication-2.pdf.
221 Federal Trade Commission, *FTC Concludes Review of AgeCheq's Second Proposed COPPA Verifiable Parental Consent Method* (January 29, 2015), Accessed June 10, 2021, https://www.ftc.gov/news-events/press-releases/2015/01/ftc-concludes-review-agecheqs-second-proposed-coppa-verifiable.
222 Ibid.
223 Ibid.
224 Federal Trade Commission, Press Releases, *FTC Denies AssertID's Application for Proposed COPPA Verifiable Parental Consent Method* (November 13, 2013), https://www.ftc.gov/news-events/press-releases/2013/11/ftc-denies-assertids-application-proposed-coppa-verifiable.
225 Federal Trade Commission, Public Submission, *Yoti Response to the Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule* (March 22, 2020), https://www.regulations.gov/comment/FTC-2019-0054-113202.
226 Ibid.

ENDNOTES

227 Federal Trade Commission, Public Submission, *Centre for Information Policy Leadership Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule* (March 25, 2020), https://www.regulations.gov/comment/FTC-2019-0054-117235.
228 Federal Trade Commission, Public Submission, *Comments Submitted by The Toy Association re: COPPA Rule Review* (December 9, 2019), https://www.regulations.gov/comment/FTC-2019-0054-21672.
229 Ibid.
230 Federal Trade Commission, Public Submission, *SuperAwesome Comments on Public Consultation on the Effectiveness of COPPA* (December 11, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25091.
231 Ibid.
232 Federal Trade Commission, Public Submission, *LEGO's Response to Request for Comments on the FTC's Implementation of the Children's Online Privacy Protection Rule* (December 12, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25188.
233 Federal Trade Commission, Public Submission, *Comments of the Association of National Advertisers on the COPPA Rule Review* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116130.
234 Federal Trade Commission, Public Submission, *Centre for Information Policy Leadership Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule* (March 25, 2020), https://www.regulations.gov/comment/FTC-2019-0054-117235.
235 Federal Trade Commission, Public Submission, *Comments Submitted by The Toy Association re: COPPA Rule Review* (December 9, 2019), https://www.regulations.gov/comment/FTC-2019-0054-21672.
236 Federal Trade Commission, *FTC Concludes Review of AgeCheq's Second Proposed COPPA Verifiable Parental Consent Method* (January 29, 2015), Accessed June 10, 2021, https://www.ftc.gov/news-events/press-releases/2015/01/ftc-concludes-review-agecheqs-second-proposed-coppa-verifiable.
237 Ibid.
238 Ibid.
239 Federal Trade Commission, Public Submission, *Comments of NCTA - The Internet and Television Association* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-115944.
240 Federal Trade Commission, Public Submission, *Comments of the Association of National Advertisers on the COPPA Rule Review* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116130.
241 Federal Trade Commission, Public Submission, *Entertainment Software Rating Board COPPA Rule Review Comments* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116012.
242 Ibid.
243 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.
244 Ibid.
245 Ibid.
246 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.
247 Federal Trade Commission, Public Submission, *Entertainment Software Rating Board COPPA Rule Review Comments* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116012.
248 Privo, *Comments of Privo* (December 11, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25092.
249 Federal Trade Commission, Public Submission, *Comments Submitted by The Toy Association re: COPPA Rule Review* (December 9, 2019), https://www.regulations.gov/comment/FTC-2019-0054-21672.
250 Federal Trade Commission, Public Submission, *Comments of CTIA* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116136.
251 Ibid.
252 Federal Trade Commission, Public Submission, *Comments of NCTA - The Internet and Television Association* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-115944.
253 Federal Trade Commission, Public Submission, *Comments Submitted by The Pokemon Company International, Inc.,* (December 12, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25196.
254 Federal Trade Commission, Public Submission, *Comments of the Association of National Advertisers on the COPPA Rule Review* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116130.
255 Ibid.
256 Federal Trade Commission, Public Submission, *The Software & Information Industry Association's COPPA Rule Review Comments* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116429.
257 Federal Trade Commission, Public Submission, *Yoti Response to the Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule* (March 22, 2020), https://www.regulations.gov/comment/FTC-2019-0054-113202.
258 Federal Trade Commission, Public Submission, *Comments of the Family Online Safety Institute* (March 22, 2020), https://www.regulations.gov/comment/FTC-2019-0054-113172.
259 Yoti, *Anonymous Age Estimation: A Deep Dive*, Yoti (May 2021), Accessed August 16, 2021, https://www.yoti.com/wp-content/uploads/Yoti-age-estimation-White-Paper-May-2021.pdf.
260 Ibid.
261 Pavni Diwanji, *How Do We Know Someone Is Old Enough to Use Our Apps?*, Facebook (July 27, 2021), Accessed August 16, 2021, https://about.fb.com/news/2021/07/age-verification/.
262 Infra, p. __.
263 Information Commissioner's Opinion, *Age Assurance for the Children's Code,* Information Commissioner's Office (October 14, 2021), https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf.

ENDNOTES

264 Ibid.
265 Information Commissioner's Office, *New certification schemes will "raise the bar" of data protection in children's privacy, age assurance and asset disposal* (August 19, 2021), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/08/ico-approves-the-first-uk-gdpr-certification-scheme-criteria/.
266 Information Commissioner's Office, *Age Check Certification Scheme (ACCS)* (July 13, 2021), https://ico.org.uk/for-organisations/age-check-certification-scheme-accs/.
267 Illinois Biometric Information Privacy Act 740 ILCS 14 (2008), available at https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.
268 Children's Advertising Review Unit, *Comments on COPPA Rule Review* (December 11, 2019), https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/default-source/caru/caru-coppa-rule-comment-12-9-19-final.pdf.
269 Ibid.
270 Children's Advertising Review Unit, *Self-Regulatory Guidelines for Children's Online Privacy Protection, Better Business Bureau National Programs*, https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/default-source/caru/caru_onlineprivacy.pdf.
271 Privo, *Comments of Privo* (December 11, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25092.
272 Privo, *Comments of Privo* (December 11, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25092.
273 Privo, *Comments of Privo* (December 11, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25092.


FUTURE OF
PRIVACY
FORUM