THE STATE OF PLAY:
Is Verifiable Parental Consent Fit For Purpose?

JUNE 2023

FUTURE OF PRIVACY FORUM

SUMMARY

Today, many children's favorite playgrounds are found online, and verifiable parental consent, or VPC, is the digital version of giving a child permission to play.

When parents take their child to a physical playground, they can assess the risk of each activity and their child's readiness. When children play online, their parent or guardian makes that same assessment (e.g., which types of online experiences and content are appropriate for my child)? Parents make these decisions every day, and they often seem straightforward, but the risks of digital services can be different and less apparent than the risks posed by merry-go-rounds and slides. A simple question, "Dad! Can I play this online game?" can trigger a complex chain of events.

Before a kid can access a child-directed online service, parents might be asked to verify their identity via a phone call, asked to confirm sensitive financial details, or print and sign a paper form. Parents could be required to charge a fee to a credit card, submit government-issued ID, or use their mobile phone camera to submit a biometric identifier.

Guardians are often unaware of what "verifiable parental consent" is, why these requirements exist, or how best to provide VPC and give their children permission to play. Couple this with children who are eager to play with their friends and who ask for permission to play online while harried parents are cooking dinner, driving, working, or at other inopportune moments, and even the most seemingly straightforward process can be difficult to navigate.

When the Children's Online Privacy Protection Act (COPPA) enacted VPC requirements in the 1990s, the goals were straightforward: keep children safe online and ensure parents are informed and engaged. COPPA restricts the data companies can collect from children under 13 and requires providers of child-directed services—based either on the website's content or on an actual knowledge that children use the website—to obtain verifiable parental consent before collecting personal information from kids. This is intended to have several benefits: it provides baseline protections for children; 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.

COPPA established the VPC requirements that still govern child-directed services today. However, children now use more—and vastly different—connected devices and products. Parents, policymakers, and youth technology experts know that opportunities for online play (and online misadventures) have also expanded. Young people are expected to interact with technology in increasingly sophisticated ways. At the same time, states are enacting new rules intended to protect young people that extend protections to teens, place stricter requirements on digital products, and require online services to infer individuals' ages in new ways. These digital fences can compromise access, potentially pushing children to less regulated spaces. Furthermore, children are resourceful and frequently able to circumvent existing requirements. Therefore, it is important to find the balance between protecting children from online harm and allowing them to reap the benefits of the digital world and develop the tools they need to navigate online services as they grow.

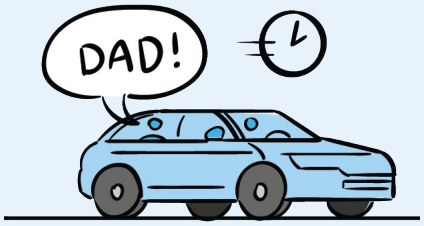
The challenges and opportunities posed by VPC have never been more important. Young people are using online services more than ever. Parents are grappling with how to best protect their children while teaching them to engage with technology in healthy ways. The Federal Trade Commission (FTC) is considering changes to the core federal law governing VPC. Companies are developing and implementing novel VPC technologies. New laws in California, Utah, and the United Kingdom require that a range of online services begin estimating or verifying the age of users, which will invariably impact the use of VPC methods. Indeed, some of the same technologies used to establish VPC also undergird age estimation technologies required by these new laws. Stakeholders have started a robust discussion about the potential benefits of age estimation and VPC tech, the privacy risks of estimating the ages of internet users, and the trade-offs between the accuracy and invasiveness of VPC and age estimation technologies. Therefore, it is an excellent time to assess the state of play regarding VPC.

With that ambition, the Future of Privacy Forum (FPF) convened industry, advocates, academics, parents, and policymakers to better understand how VPC works today, how it impacts kids' access to online play, and the unintended consequences of VPC laws and technologies. We prepared a discussion draft of this whitepaper last fall and circulated it widely to both stakeholders and the public, inviting commentary and feedback. This is the revised version of the discussion draft: an updated analysis of the state of play.

In this paper, we examine just how much children engage with the internet, explore the history of VPC and other similar approaches around the world, do a deep dive into the contours of VPC itself, identify challenges associated with VPC, and consider some possible solutions.

Although VPC requirements have enabled millions of parents to better understand and vet their children's online playgrounds, the VPC framework presents real challenges for young people and their guardians. The VPC process can:

- **Lack efficacy:** VPC often does not work as it should. Parents can get lost in the multiple steps required and attempts to provide bona fide VPC may fail if photos of a guardian's ID are blurry or there are other errors with VPC submissions. All too often, children figure out how to bypass VPC altogether, and parental consent is circumvented from the process intended to protect children.
- **Limit accessibility:** Common VPC methods such as providing a credit card number or government-issued identification reduce or preclude equitable access for millions of caregivers who are unbanked, undocumented, or lack government-issued identification for other reasons.
- **Generate hesitancy and privacy concerns:** a VPC requirement may give parents pause, causing them to worry about why the information to fulfill the requirement might be needed, or even causing them to be skeptical about the motives of the digital platform. Requirements to share sensitive financial or other personal information can also leave parents with concerns about potential security and privacy risks associated with that digital experience.
- **Inconvenient and poses cost barriers:** VPC can involve multiple steps and can be time consuming and cumbersome. As a result, many parents do not complete the VPC process, thereby locking their children out of engaging online experiences. There is evidence that many children are thus likely to either lie about their age, try to circumvent the VPC system, and/or redirect their online play to general audience services that provide fewer privacy protections—and expose children to more age-inappropriate content—than comparable child-directed services. From a developer standpoint, VPC can be such an implementation and cost barrier for operators that many are abandoning developing experiences for children altogether.



Next Steps: Let's Solve This Together

This whitepaper identifies possible solutions that are worth further discussion. These include:

- New regulatory approaches, including a transition of the FTC's approved-VPC methods list to a criteria-based framework;
- Alternative VPC methods, such as mobile phone text messaging, platform-mediated VPC, VPC during setup at the direction of a parent, and other alternatives to credit card VPC methods, including methods based on other financial instruments; and
- Amending the FTC approval process for VPC methods to promote more timely review, create an independent review panel, or implement a "regulatory sandbox" where VPC approaches could be tested and assessed.

This whitepaper is intended to help identify the challenges raised by VPC and determine what the future of parental consent could be. It is also an invitation for us to find a solution together. Let's explore the future of play!

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

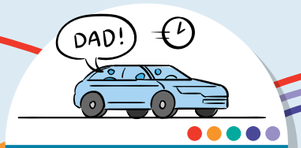
Credit/Debit Card

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

VPC Abandoned

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

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.

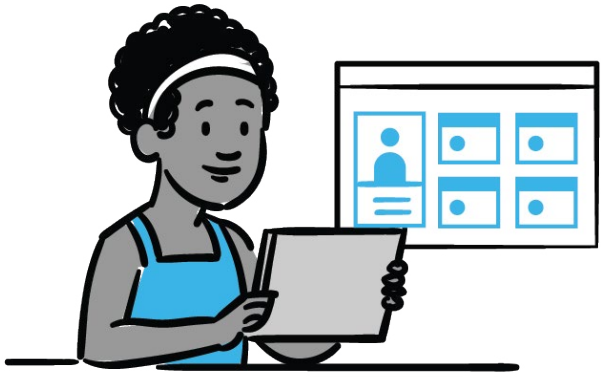
TABLE OF CONTENTS

Introduction: Why Verifiable Parental Consent?

Why are parents asked for verifiable parental consent (VPC) in the first place? VPC is a requirement of the Children's Online Privacy Protection Act (COPPA)—the primary federal child privacy law.[1] COPPA requires operators of online services directed to children under 13 (or with actual knowledge that a child under 13 uses the service) to provide parents with detailed, direct notice and to obtain parents' affirmative express consent—verifiable parental consent—before operators collect children's personal information.

COPPA does not regulate online content directly; rather, the intent of VPC is to give parents some control over what content their children access and what data may be collected from them. Although VPC has been legally required since COPPA's enactment in 1998, operators subject to the law have faced challenges in its implementation. As the FTC conducts its COPPA Rule review and legislators continue to introduce bills that would update COPPA or create new children's privacy frameworks, this paper seeks to inform those efforts by exploring the current status of VPC and identifying opportunities to improve VPC mechanisms with the hope of informing fresh approaches to protecting children online.

Children Today Are Increasingly Connected



The internet is as much a part of the daily lives of American children as school, toys, and friends. In the United States, children from birth to age eight engage in about two-and-a-half hours of "screen media" per day on average.[2] Internet use became even more essential during the COVID-19 pandemic and the social isolation that ensued as it is easy to social distance on the internet. During the pandemic, children have used the internet to communicate; keep in touch with their friends, families, and teachers; go to school; maintain their social skills; and play online.[3]

From education to gaming to art, the landscape of children's online products has exploded in recent years. Children interact with mobile applications, including gaming and creation applications; extended reality experiences; edutainment; and other devices within the Internet of Things (IoT) directed to children. However, even when media is not explicitly directed to children, recent studies have shown that children are heavily connected online through use of their parents' devices.[4] To help stakeholders better understand online access points for children, this section explores the many media through which children connect to the internet and popular methods of their engagement online.

Kids are online, *a lot*. A recent study from the Family Online Safety Institute (FOSI) shows just how connected children are. 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 41 percent of parents reported that their children have one or two of their own connected devices.[6] This same study found that the most common devices children ages 12 and younger use to connect to the internet are tablet computer/iPads (89% of children either own or have access to), cell phones and smartphones (89%), desktops or laptop computers (86%), and video game consoles (83%). Less common devices included other handheld devices or iPods with WiFi capability (60%), connected toys (35%), and wearable devices (smart watches, fitness trackers; 31%).[7] Since these devices have vastly different interfaces, they can create different challenges when collecting VPC.

[=]But children don't just use their own personal connected devices. In the age of the smart home, children use the internet through devices that are common household items for many families. The FOSI study identified connected or smart TVs and internet-connected speakers as the connected devices that children most commonly use.[8] A majority of parents participating in the study own connected or smart TVs (67%). Of parents who own a smart TV, 96% indicated that their children use it. Of parents who own a voice-controlled, internet-connected speaker (23%), 94% reported that their children use it. Parents even reported that their children use devices such as their internet-enabled thermostats and internet-enabled security systems; 67% of parents who own internet-enabled devices and 64% of parents who own internet-enabled security systems devices reported that their children use the devices.[9]

The ways that children use the internet are as varied as the media through which they access it. They may post their take on the latest viral dance to their TikTok account, send snaps to their Snapchat friends using the zaniest filters, or communicate with their friends from email or messaging accounts.[10] Over 80 percent 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.[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, XR headset sales are projected to increase 14% in 2023 with a compound annual growth rate of 32.6% between 2023–2027.[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]

With so much to do online and so many ways to connect to the internet, it comes as no surprise that children today are heavily connected, but with this increase in connectivity comes the potential for increased risks driven by data collection, use, and disclosure. Although concerns remain about children's well-being, safety, and privacy, parents and education institutions alike have largely 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.

A Deep Dive into Veriable Parental Consent

In the United States, the prevailing route to regulating children's internet behavior has been to ensure that parents or caregivers mediate their children's online interactions. The FTC's COPPA enforcement reflects a legal, political, and social 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 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, various VPC techniques and technologies have emerged and formed the roadmap from which we are navigating VPC today.

Many websites are categorized as "general audience" services—they are not targeted to children, and the operators have no actual knowledge that a particular child uses the site. COPPA does not typically require general audience services to infer users' ages, but does mandate that sites act when children, parents, or others notify the operator that a particular child uses the service. COPPA spells out a list of requirements for covered operators.[16] It requires an operator of a commercial online service directed to children under 13, or with actual knowledge a child under 13 uses the service, 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.[17]

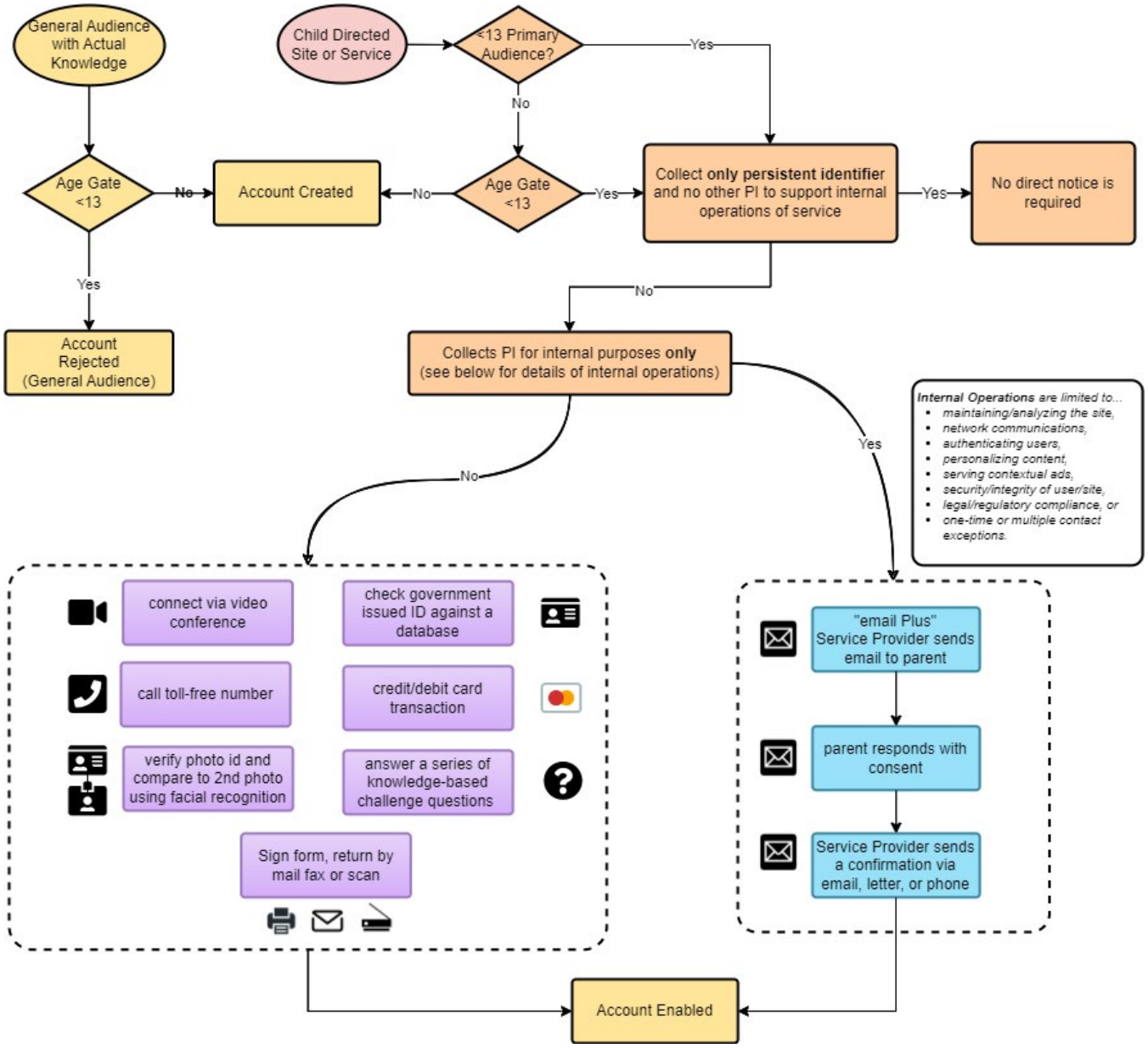
KNOWLEDGE STANDARDS UNDER COPPA

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.[18] 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.[19] 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."[20]

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."[21]

Knowledge standards are the subject of evolving policy debates. Some state laws, such as the California Consumer Privacy Act (CCPA), have expanded on the "actual knowledge" standard to include businesses who willfully disregard a consumer's age.[22] Some laws, such as the California Age-Appropriate Design Code Act (California AADC), take an even broader approach. The California AADC applies to all online services that are "likely to be accessed" by users under 18.[23]

Before collecting, using, or disclosing a child's personal information, an operator must provide direct notice of privacy practices to parents (more detail about direct notice and other COPPA requirements can be found in the Appendix). 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. 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

It is important to consider the question: how do we even know when an operator should obtain VPC regarding a particular user? Operators cannot compel kids to ask "Mom, can I play this game online?", if website operators don't already know a child is interacting with their interface and thus do not prompt the child to ask. 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 these 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.

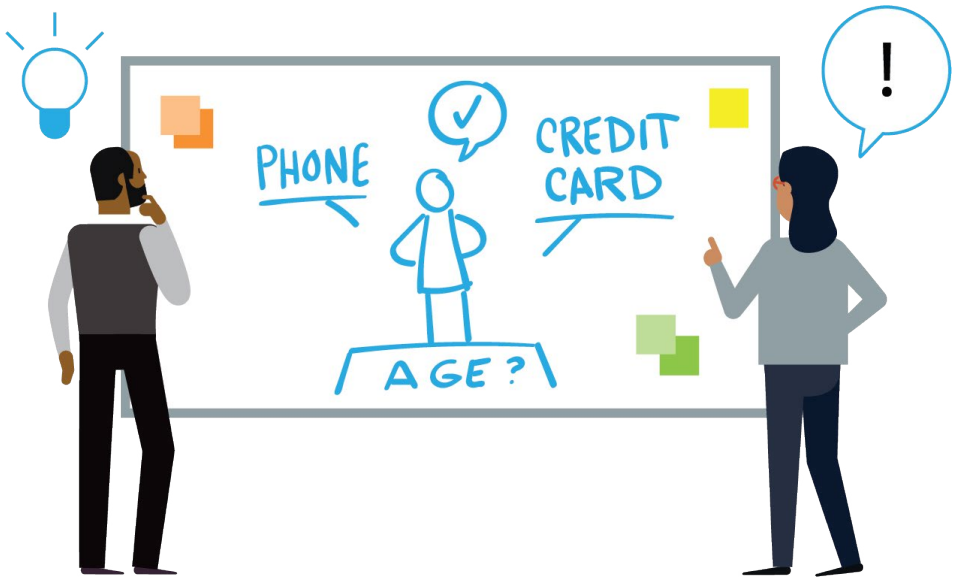
Per FTC guidelines, age screening systems must be "neutral."[24] They must prompt users to provide their age by asking their month and year of birth, rather than simply asking if they are 13 or older. This approach seeks to prevent child users from understanding that they need to input a particular birth 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.[25]

The chart below summarizes age screening applicability under COPPA:

Directed?	Is Child Directed?	Is <13 Primary Audience?	May Age Screen?	May Reject <13?
General Audience	No	No	Yes	Yes
Mixed Audience	Yes	No	Yes	No
Child Directed	Yes	Yes	No	No

When Is VPC Required?

After age screening, operators must provide direct parental notice and potentially obtain VPC, that digital "permission to play." And COPPA tells us just when we need it. There are also situations where COPPA does not require VPC, and further considerations are detailed in the Appendix C. 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 in a number of ways, including 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).[38] If any of these circumstances are occurring, we need VPC.



FTC-Approved Verification Methods

Simply knowing parental permission to play is needed for a child to hang out in an online playground only gets you so far. COPPA-covered operators need to figure out *how* to get that required permission. And since COPPA does not prescribe any specific required methods to obtain VPC, you may think the sky's the limit when it comes to creating a VPC method that works for you. Unfortunately, it's not quite that easy.

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.[26] The FTC has determined that several methods meet the rule's standard. This seems straightforward enough. And the FTC has also provided guidance in this area, providing a non-exhaustive list of VPC methods that it has approved. 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.[27] Most recently, in 2013 and 2015, knowledge-based questions and facial recognition technology have been approved as VPC methods.[28]

Though the FTC's list is not exhaustive for acceptable methods of getting VPC, it's a valuable resource for discerning what types of methods have been approved. Using a method that has the FTC's stamp of approval can help alleviate some of the concern about compliance, but it is never a guarantee that you won't get in trouble for your data privacy practices. And while using other VPC methods that fit COPPA's standard is technically allowed under COPPA, it may not be up to par with FTC expectations.

Special Considerations: COPPA Safe Harbors

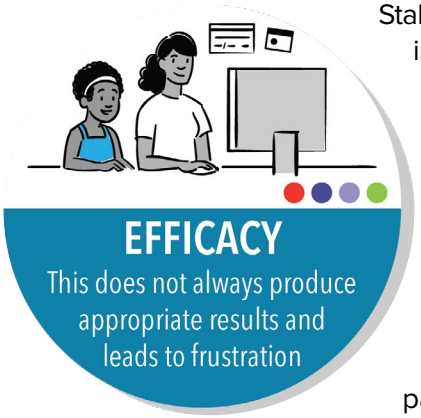
COPPA also allows operators to apply for certification as COPPA-compliant through a "safe harbor" program, which is consistent with one of the FTC's approaches to consumer privacy: industry self-regulation.[29] The safe harbor programs act as self-regulatory bodies. A company may comply with COPPA if it is a member of an FTC-approved safe harbor program and complies with the program's guidelines. 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.[30] In addition to certifying COPPA compliance, safe harbors can authorize VPC methods that operators may rely on to fulfill their COPPA obligations[31] (additional information about COPPA safe harbors can be found in the Appendix).

"Email plus": There are several exceptions to when an operator must obtain VPC, which are enumerated in Appendix C. One that is noteworthy from the stakeholder discussion is email plus, which operators may rely on if they do not disclose children's personal information to third parties or make that information publicly available. 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. 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 personal information under the COPPA Rule (e.g., username), email plus is not necessary. For example, if a cookie is only 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.

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

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

Efficacy



Stakeholders frequently stated that child users who complete the VPC process in lieu of their parents or lie about their age are able to 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."[32] 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.[33]

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."[34] 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.[35] 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 percent of parents reported that their children aged 4–19 had credit cards.[36] Further, there is no fail-safe, cost-effective way to verify parental identity.[37]

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.[38] 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."[39] 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.[40]

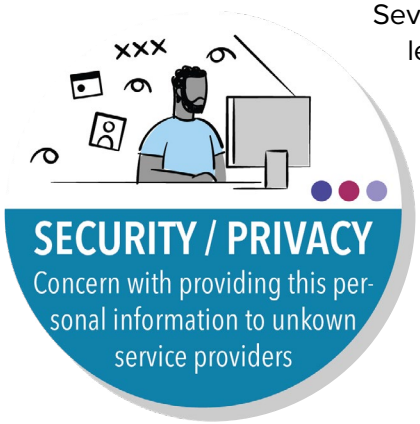
In its statement of basis and purpose of the original COPPA rulemaking in 1999, the FTC acknowledged several commenters' concerns regarding children's accessibility to the internet and that their goal was to create a rule that balanced this concern with protecting children online.[41] Twenty years later, the concerns still persist. For example, in its 2019 COPPA comments, Google notes that sometimes a parent or caregiver may not be readily available to engage in the VPC process, thereby hindering a child's ability to explore, learn, and engage online.[42]

Hesitancies, Privacy, and Security

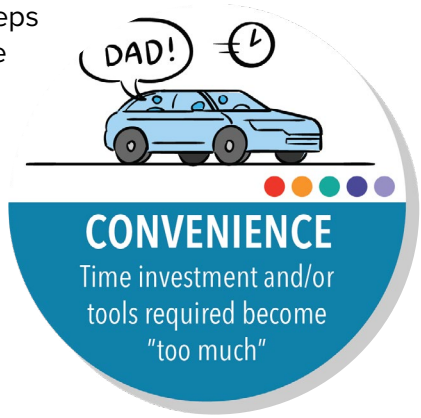
When asked about particular COPPA-enumerated VPC methods, parents generally expressed discomfort with being asked to share sensitive information such as credit card information or their government ID and having that information linked to their children's online presence. The LEGO Group noted similar 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.[43] 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."[44] 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."[45] 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 reduced numbers of 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 have also noted that "parents' privacy expectations are highly context dependent and contingent on perceptions of the different entities that collect personal information."[46]

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.[47]



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."[48] Similarly, the LEGO Group reported "a significant dropout when VPC is required due to the arduous and time consuming sign-in process," which, consequently, risks that children will turn to games with lower barriers to entry and that "are not necessarily designed for the child's age."[49] 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.[50]

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. The App Association (ACT) argues that the lack of "effective, easy-to-implement, and affordable mechanisms" means that companies risk "unnecessary liability without meaningfully enhancing children's privacy."[51] 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."[52] 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."[53]

ESRB and SuperAwesome identified a similar issue. According to ESRB:

> "[M]any 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."[54]

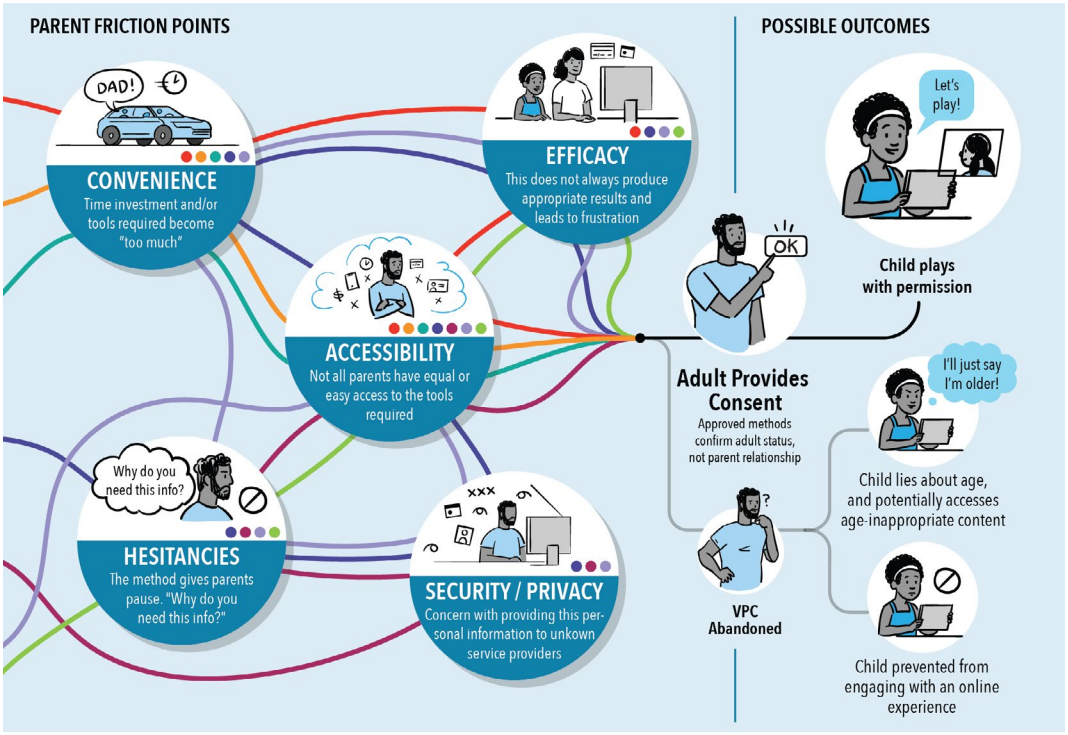
Further, SuperAwesome notes that:

> "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."[55]

The Toy Association notes that implementing strong VPC is incredibly costly, and such strong VPC also leads to a significant drop-off of parents' interest. It argues that adding additional VPC methods that force companies to set up pay walls will reduce, not foster, children's content online."[56] 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."[57]

Government officials 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."[58]



Implementation Challenges

In addition to the friction points, 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."[59] 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."[60]

Modernizing VPC: 2013 COPPA Updates & Beyond

The FTC does not require operators to use its enumerated verification methods for obtaining VPC, though as a cautionary measure most operators rely on those methods for gaining consent. In 2013, COPPA was updated to allow for the submission of VPC proposals to the FTC for review and formal approval.[61] 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 VPC 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.[62] The FTC approves non-proprietary methods that "can be used by the applicant or any other party."[63] Once an applicant files the VPC proposal with the FTC, the commission seeks and considers public comments and then issues a determination.[64]

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.[65] Through the commission's determination process, 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 because they trigger the friction points of convenience, hesitancies, security, and privacy.

KBA entails the use of dynamic, multiple-choice questions, including a "reasonable number" of questions with an "adequate number" of possible answers to mitigate the risk of a non-parent user guessing the correct answer and accessing a site or service without obtaining parental consent.[66] 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."[67] 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.[68] In its approval, the FTC noted that financial institutions and credit bureaus rely on KBA as a secure, effective mechanism for user authentication.[69]

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.[70] 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.[71] 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."[72]

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.[73] Similarly, the FTC denied AgeCheq's initial application because the proposal incorporated already approved methods.[74] 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 print, sign, and return 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.[75] 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.[76]

The FTC denied AgeCheq's second proposed VPC method, "Device-Signed Parental Consent Form." The proposed method involved the parent registering with an intermediary company that handles certification, then entering personal information on a parental identity declaration form. The intermediary would then send a code to the parent's phone, in which the parent would enter the code and then digitally sign a certification verifying that they owned the device.[77] The FTC found that this method was not reasonably calculated to ensure that the person providing consent is the child's parent because a child could intercept the text message code and bypass the security requirement.[78] 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."[79] Further, the FTC determined that AgeCheq's proposed method required the collection of a mobile phone number and home address, which is not categorized by COPPA as online contact information and, therefore, not suitable for the consent initiation process.[80]

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 eight 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.

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 perspectives on the efficacy of VPC is thus unique and valuable. This section outlines selected stakeholder proposals to address some of the challenges discussed above. Some 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 approved VPC methods. Yoti, for example, suggested that the FTC eliminate the list and, instead, enumerate criteria for obtaining valid 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.[81] Yoti's examples include ensuring that the person providing consent is an adult and that identity documents belong to the individual undergoing VPC and confirming that the person has "authority to act for the child."[82] The Center for Information Policy Leadership also supports an "outcome- or criteria-based approach to VPC instead of a specified list of consent methods."[83]

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."[84] 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."[85]

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."[86] 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."[87]

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."[88] 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."[89]

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."[90]

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 outcome. 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."[91] 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.[92] 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.[93] 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.[94]

Regardless of these concerns raised by the FTC, several other organizations agree that mobile phones should be 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."[95] The Association of National Advertisers also supported text messages as a permissible method of obtaining VPC under the Rule.[96]

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."[97] 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.[98]

Platform-Mediated VPC

Several organizations urged the FTC to consider whether and how platforms, such as operating systems, can mediate the VPC process instead of each individual application obtaining it. 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,"[99] 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."[100] CITP also noted that:

> "[M]ajor 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."[101]

Similarly, the Developers Alliance indicated that:

> "[M]any 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."[102]

ESRB also pointed to platforms as a possible solution and urged the FTC to "explore steps to engage platforms in the VPC process."[103] 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."[104] Beyond platforms mediating VPC itself, safe harbor PRIVO suggested that the commission encourages the development and adoption of:

> "[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."[105]

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."[106] CTIA suggested that VPC should be obtained through the setup process for services that collect personal information from children at the direction of their parents.[107] CTIA posited that

> "Specifically, 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."[108]

Alternatives to Credit Cards

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."[109] 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."[110]

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.[111] ANA argued that the method:

> "[S]hould 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."[112]

AMENDING THE VPC 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."[113]

Other submissions proposed new frameworks altogether. Yoti posited that:

> Rather 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.[114]

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."[115]

Looking Ahead Toward the Future State of Play

Companies may use age assurance methods to determine a user's age, if that user is a child, or to ensure that proper consent is obtained. "Age assurance" includes age verification or estimation methods that are a part of the VPC process for online services, including general or mixed audience services. COPPA does not require operators of general audience sites to infer users' ages, but some companies have adopted it voluntarily due to its flexibility.

Furthermore, newer laws, such as California's Age-Appropriate Design Code, the UK Age Appropriate Design Code, and Utah's Social Media Regulation Act, require age assurance as compliance obligations. These new requirements are also causing a shift toward using age assurance methods for all users, even for general audience sites, and contain no mention of parental consent. The UK and California Codes require that online services "likely to be accessed" by users under 18 estimate the age of users with "reasonable certainty" or alternatively apply required protections to all users, while the Utah Act explicitly requires companies to verify the age of all users. Newer and proposed legislation, like the Utah Act, are expanding age verification requirements to broader and older audiences. These legislative movements are likely to cause the issues raised by this paper to affect more individuals and exacerbate the impact of the existing friction points.

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 that a user's actual and stated ages match.[116]

Yoti's age estimation tool uses machine learning to scan a user's face and determine whether it is statistically likely that the user falls within a certain age range, such as under or over the age of 25.[117] According to the company, such technology can help remove barriers that people without government-issued identification face in the VPC process by giving a parent an additional way to verify their age to provide consent. Aside from the parental consent context, this technology is also being deployed to determine the age range of younger users in limited use cases, such as allowing adult users access to sites not intended for children or teens, like Facebook Dating. However, since the technology can only show that it is statistically probable that a user is a certain age, there will be false positives (and false negatives). There are also current limitations in the accuracy of this new technology for estimating age brackets for users under 25. Therefore, companies using these technologies may need secondary verification methods (such as showing a government-issued ID) depending on the risks.[118]

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 implementing age assurance mechanisms can align with the UK's Age Appropriate Design Code.[119] However, the Code differs from COPPA and explicitly discusses the use of age assurance tools, along with other approaches to designing safe online environments for children. The ICO recognized 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.[120] When considering the feasibility of new age assurance technologies, companies should evaluate these risks and determine the suitable balance of risk and accuracy before adoption. 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.[121] In 2021, the ICO formally approved an age assurance certification scheme.[122] 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.[123]

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 their responses, 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."[124] Both safe harbors 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.[125] Further, PRIVO suggested higher standards for screening children out of services depending on the risk associated with certain data, "i.e., public sharing of images, video, free text and communications."[126] Beyond this suggestion, PRIVO also noted that mechanisms that allow parents to register a child's device and signal that a child uses that device could be used to limit children circumventing age gates or screens.[127] The Commission's rule review has not significantly progressed and is ongoing.

Moreover, state-level restrictions may hinder providers from innovating VPC methods in the United States. For example, the Illinois Biometric Information Privacy Act (BIPA) requires companies to obtain consent before collecting or disclosing biometric identifiers.[128] BIPA also includes a private right of action that allows individuals to sue companies for violating the law. Companies must consider state law restrictions, like BIPA, and potential liability in their risk analyses when pursuing and creating innovative VPC methods.

The legal landscape is rapidly changing, particularly at the state level. The California Age-Appropriate Design Code Act is not enforceable until July 2024, and at least one pending lawsuit seeks to overturn the measure on constitutional grounds.[129] However, other states have introduced bills that would mimic California's age estimation requirements or even go further to require age verification. The age assurance conversation is shifting globally and increasingly requiring broad age estimation. Still, VPC is an existing COPPA obligation that is here to stay and necessitates continued efforts to find innovative solutions. It is unclear whether newer legislation will be struck down or expanded—the outcome will have substantial implications for organizations' VPC practices.

CONCLUSION

The state of play for kids online has evolved tremendously in recent years. With connected toys, smart products, and increased online experiences, many children's favorite playgrounds are now found online. We need regulations and legislation to keep up with the ever-changing and increasingly digital environment where our children play: this paper serves as a call to action to start a dialogue about how that should be done.

Our findings identify challenges to getting VPC right in the current regulatory and legislative environment. Companies, parents, and children are all struggling to navigate VPC in a way that is beneficial to kids. We identified issues with:

Efficacy: Many VPC methods are easily circumvented by children. A parent even described VPC as "privacy theater," because children can get around it easily, causing the parent to question its value. Many current VPC methods also allow for people who are not parents or caregivers to complete the VPC process, turning "verifiable parental consent" into "verifiable adult consent" and removing COPPA's intended parental rights. We have yet to see a truly fail-safe, cost-effective way to verify true parental identity.

Accessibility: Concerns about accessibility and equity also exist among stakeholders regarding the currently approved mechanisms for obtaining VPC. Prevalent methods of obtaining VPC include a parent providing credit card information or government identification information. These methods are problematic for millions of unbanked households in the United States, as well as for people without government-issued identification, including undocumented immigrants. Children with parents or caregivers who fall into these categories are thus prevented from enjoying the benefits of the internet simply because they cannot gain VPC for reasons out of their or their caregivers' control.

Hesitancy, 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 necessity of obtaining sensitive personal information from adults also poses privacy concerns and can increase compliance costs for service providers.

Convenience and Cost Barriers: Several companies noted that implementing rigorous VPC requirements often leads to user drop- off because the process introduces friction and inconvenience for users who want to engage a service. From the company standpoint, 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, and costly to implement. The high cost of getting VPC right can create an inequitable burden for mid-sized and smaller developers, making compliance affordable only for the largest platforms.

As U.S. legislators and regulators consider modernizing COPPA or crafting 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. Several stakeholders have presented potential solutions to address challenges in the current landscape, including:

- New regulatory approaches;
- Alternative VPC methods, such as mobile phone SMS or text messaging, platform-mediated VPC, VPC during set-up at the direction of a parent, and alternatives to credit card VPC methods; and
- Amending the FTC approval process for VPC methods.

Now that we know the state of play, it is time to take action. We invite you all to engage with the dialogue about how to solve VPC challenges. We believe solutions for improving the current system are out there, and we need to find them together!

APPENDIX A

A Detailed History of COPPA

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.[130] 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 citizen's 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.[131] 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 them is in a record and how it is used.
- There must be a way for an individual to prevent information about them 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.[132]

The FIPs laid the foundation for the Federal Privacy Act of 1974, enacted just one year after the HEW report's publication.[133] 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.[134] 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. 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.

Also in 1974, lawmakers enacted the Family Educational Rights and Privacy Act to protect the privacy of education records.[135] Lawmakers introduced FERPA amidst concerns about centralized computer systems amassing sensitive data about students, with little to no privacy or security protections.[136] 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.[137] 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."[138]

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."[139]

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.140 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.141

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."[142]

These principles were included in the FTC's response to a petition that the commission investigate KidsCom, an interactive website designed for kids aged 4–15.143 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.144

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.145 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.146 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.147 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."148 The report documents concerns about data collection practices bypassing parents, who "have traditionally protected children from marketing abuses."149 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.150

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.151 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.152

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."[153]

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."[154]

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."[155]

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."[156]

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.[157] 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.[158]

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.[159] 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."[160]

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:

> "[L]ess 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."[161]

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."[162]

> **"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.[163] 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."[164] 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.[165]

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.

APPENDIX B

Background on International Approaches

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 involve different 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, they 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.[166] While the United States has not ratified the CRC, UNICEF notes that it has become the most widely ratified human rights treaty in history.[167] Signatories include Australia, Brazil, France, Germany, Ireland, Mexico, Singapore, South Korea, and the UK.[168] 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.[169] Thirty-eight countries are members, including the United States.[170] 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."[171]

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: 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."[172]

Acknowledging that children require special protection, the GDPR includes instances in which privacy standards must be higher for data collected from children.[173] 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."[174] 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."[175] 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[176] 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.[177]

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's consent in relation to information society services."[178] 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.[179]

In addition to this flexibility in the GDPR, Member States' Data Protection Authorities (DPAs) may offer additional protections. For example, Germany's youth protection law focuses on content protection.[180] 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. Other Member States have similar initiatives, such as the French DPA (CNIL) prototype aimed at developing a privacy-friendly solution for age verification on pornographic websites.[181]

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.[182] 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."[183] 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.[184]

The United Kingdom

In addition to creating the guidelines set forth in the UK GDPR,[185] the UK 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."[186] 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 child-specific interpretive GDPR guidance.[187] 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:

> "Online 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."[188]

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."[189] 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.

China

China's Personal Information Protection Law (PIPL), which took effect in November 2021, deems the personal information of children under the age of 14 to be "sensitive personal information."[190] The PIPL includes strict rules regarding children's privacy, including requiring operators to obtain express consent from the parents or legal guardians of users under the age of 14.[191] Notably, this requirement does not include an exception for operators that are unaware or have no reason to be aware of the data subjects' young age.

The children's privacy landscape in China also includes the country's Law on the Protection of Minors, which was substantially amended in 2020.[192] As revised, the law restricts children under 16 from opening live broadcasting accounts.[193] 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."[194] In addition to the legal requirement, through regulation, the country's National Press and Publication Administration restricts online gaming to minors for one hour on Friday and Saturday, as well as on national holidays.[195] 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.[196] 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.[197]

Singapore

The Personal Data Protection Act of 2012 (PDPA) is the main law that governs protection of personal data in Singapore. The PDPA does not contain specific requirements regarding children's privacy. However, Advisory Guidelines issued by Singapore's Personal Data Protection Commission (PDPC) provide more detailed guidance on processing of the personal data of minors under the age of 21.[198] 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. Specifically, under the PDPC's guidelines, minors who are at least 13 years old would typically be considered to have sufficient understanding to be able to consent on their own behalf for the purposes of the PDPA.[199] However, if an organization has reason to believe or it can be shown that a minor does not have sufficient understanding, the organization may obtain consent from someone who can legally provide consent on the minor's behalf (e.g., parent or legal guardian).[200]

Similar to many countries' policies, the PDPC's guidelines recommend that operators obtain parental consent when they know, or ought to know, that they collect children's data. However, the PDPC'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

The Personal Information Protection Act (PIPA) is the main law that governs protection of personal data in South Korea. Under the PIPA,[201] operators must generally obtain parental consent before collecting and using the personal information of users under the age of 14.[202] Following amendments in 2020, the PIPA

also specifies several alternative methods through which operators must obtain written parental consent.[203] Parents may choose to consent "via text, payment, information, or authentication through smartphones."[204] After obtaining consent, the operators must send written confirmation to the parents through one of the aforementioned methods.[205]

Brazil

Brazil's General Personal Data Protection Law (LGPD) requires the processing of personal data of any child or adolescent data to be carried out in the child's "best interest" and with prior consent by at least one parent or legal guardian.[206] The country's Statute of the Child and Adolescent (ECA) defines "children" as individuals under 12 and "adolescents" as individuals between 12 and 18.[207] As one publication notes, the ECA asserts that "children and adolescents have a peculiar condition of being in development."[208] Reflecting this philosophy, the LGPD's parental consent requirements tend to be heavier than those in many other countries.[209]

Under the LGPD, the only time child or adolescent data collection does not require parental consent is when "collection is necessary to contact the parent or the legal guardian," and as long as the data are "used only once and without storage, or for their protection, and in no case may be passed on to a third party" without the consent of a parent or the legal guardian.[210] The law also prohibits controllers from conditioning children's and adolescents' participation on "games, internet applications or other activities" to providing personal information beyond what is "strictly necessary for the activity."[211]

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.[212] 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. 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, different 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.[213] 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. 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.[214] 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."[215] 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 authorized … taking into consideration available technology."[216]

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.

APPENDIX C

Additional COPPA Requirements

Direct Notice

Once users pass through an age gate, the next step in the flow is direct notice. The COPPA Rule outlines the information operators must include in the direct notice to parents.[217] 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."[218] We don't have to guess when direct notice is required: luckily, COPPA provides clear directions. 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.[219] 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.[220]

COPPA-Protected Information and Prohibited Practices

Above, we mentioned that COPPA applies to certain operators collecting personal information from children. But what counts as personal information? Surely there is some data that you can collect that is anonymous enough to not be in this category? COPPA defines personal information as "individually identifiable information about an individual collected online,"[221] a broad definition that includes "persistent identifier[s] that can be used to recognize a user over time and across different websites or online services."[222] 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

We know that not all data collected is created equal. Certain types and uses of data may trigger COPPA VPC obligations, and metadata that includes COPPA-protected personal information and audio files of a child's voice can trigger unique COPPA obligations. These distinctions are important for understanding when COPPA requires VPC.

If a child uploads a photo, for instance, that user-provided photo may include metadata that contains COPPA-protected personal information. Photos themselves are personally identifiable information when they contain a child's likeness or image. Digital cameras (like the ones on our phones) 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.[223] 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 the time necessary to fulfill that purpose, the FTC will not take an enforcement action against the operator for failing to obtain VPC.[224] The operator must, however, still provide clear online notice of its collection, use, and deletion policy regarding these audio files.[225] 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.

COPPA SAFE HARBORS

COPPA safe harbor 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.[226] In addition to certifying COPPA compliance, safe harbors can authorize VPC methods that operators may rely on to fulfill their COPPA obligations.

While COPPA safe harbor programs aim to increase COPPA-compliance through self-regulation, the system is not perfect. The FTC has removed an organization from the safe harbor list in the past for failing to meet their standards.[227]

EXCEPTIONS TO COPPA'S PARENTAL CONSENT REQUIREMENT

There are limited situations in which COPPA's general requirement that operators obtain parental consent before collecting children's personal information does not apply. The following are the eight narrow exceptions to COPPA:

Exception 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). This makes sense – in order to get parental consent in the first place, some information must be collected to go through that process.

Exception 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. In this case, no personal information is being collected, so no verifiable parental consent is required.

Exception 3: When an operator responds directly to a child's specific, one-time request. An example might be if a child wants to enter a contest; the operator cannot use information collected from that one-time request to contact the child again, and must delete the information afterwards.

Exception 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. The exception could apply, for example, if the child wants to receive a newsletter. Information about the child collected in this instance cannot be combined with any other information collected about the child.

Exception 5: When an operator is protecting a child's safety. If a child's safety is at stake, it is not necessary to obtain verifiable parental consent, but there are still plenty of rules about notifying the parents about what is happening, and the information collected cannot be used for other purposes.

Exception 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. Of course, COPPA does not require operators to interfere with security or legal processes.

Exception 7: 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 the COPPA Rule.

Exception 8: 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 the third-party operator collects only a persistent identifier and no other personal information; the user affirmatively interacts with the third-party site or service to trigger the collection; and the third-party operator has already screened and verified the person is 13 or older.[228]

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.[229] Such activities include 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.[230]

Contextual Advertising. 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.[231]

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.[232] 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.[233]

Special Considerations: Verifiable Parental Consent and Schools

When schools contract to use a site or service, the school may provide consent as the parent's agent.[234] 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."[235]

However, the school's ability to provide this consent is limited to the education 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.[236] In this context, the school can serve as the intermediary to help the operator obtain parents' consent.

Potential COPPA Violations

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.[237]

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.[238] 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,[239] into the network traffic to indicate to a third-party ad network that a website, service, or specific users[240] 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.[241]

While COPPA and other flags and signaling[242] 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 children."[243] 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. 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 software updates for security flaws, and ensure the updates will not hamper third-party security features.[244]

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.[245] 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 the sensitivity of the personal information." [246] 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.[247]

COPPA Enforcement

If companies get VPC (or other COPPA requirements) wrong, they will most likely answer to the Federal Trade Commission. 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.[248]

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.[249] The FTC has been enforcing COPPA violations for decades: early cases in the late 1990's and early 2000's include smaller dollar-amount settlements with companies like Lisa Frank, who

violated COPPA requirements for collection of children's data, and recent cases include multi-million dollar settlements for COPPA violations of large companies like Youtube, Tiktok and Weight Watchers.

However, this approach to COPPA enforcement has left many unanswered questions regarding the law's gray 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

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."[250] 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.[251]

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 guardians of children's online activity. The following excerpt from the FTC's 1998 report to Congress 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.[252]

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.[253] Congressional action in light of these concerns was, in the FTC's words, "deliberately paternalistic" while accounting for the "promise of technologies."[254] 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.[255] As some have noted, children, whose brains are still developing, are no match for advanced profiling and analytics techniques.[256] 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.[257] Such supervision would grant children the "right to grow, learn, and develop without surveillance, sorting, steering or suppression."[258]

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.[259] 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. An interesting perspective is offered by Professor Simone van der Hof, Professor of Law and Digital Technologies at Leiden University, who challenges 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.[260] She argues that if both assumptions are true, little opportunity remains to secure children's rights.[261]

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."[262]

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.[263] These advocates argue that parents, in a complex and quickly evolving digital environment, 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.[264] This holistic, rather than "deliberately paternalistic," approach most aligns with the European approach to regulating children's online activities.[265]

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%3Ao0T-7W3EeYuLBC0gpolOmMJjqeBU-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. Ibid. 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 International Data Corporation, *Slower Growth for AR/VR Headset Shipments in 2023 but Strong Growth Forecast Through 2027, According to IDC,* https://www.idc.com/getdoc.jsp?containerId=prUS50511523

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 15 U.S.C. § 6501.

17 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.

18 Ibid.

19 16 C.F.R. § 312.2

20 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.

21 Ibid.

22 Cal. Civ. Code §1798.120(c).

23 Cal. Civ. Code § 1798.99.30(b)(1),(4).

24 Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions* (2020), Accessed August 10, 2021, https://www.ftcgov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0

25 Ibid.

26 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.

27 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.

28 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.

29 16 C.F.R § 312.5(b)(2).

30 Ibid.

31 Ibid.

32 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.

33 Ibid.

34 Federal Trade Commission, Public Submission, *Comments of Computer & Communications Industry Association* (March 25, 2020), https://www.regulations.gov/comment/FTC-2019-0054-117085.

35 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.

36 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.

37 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.

38 These are prevalent methods, but not the only methods — the FTC also offers other methods, such as a signed consent form or phone call.

39 Federal Trade Commission, Public Submission, *Comments of Internet Association* (March 25, 2020), https://www.regulations.gov/comment/FTC-2019-0054-117011.

40 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/.

41 Children's Online Privacy Protection Rule; Final Rule, Fed. Reg. 59888(Nov. 3,1999) 16 CFR Part 312, https://www.ftc.gov/sites/default/files/documents/cases/2008/12/081211appa0823071.pdfhttps://www.ftc.gov/sites/default/files/documents/cases/2008/12/081211appa0823071.pdf

42 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.

43 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.

44 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.

45 EPIC, *Children's Online Privacy Protection Act (COPPA)*, https://epic.org/privacy/kids/.

46 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.

47 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.

48 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.

49 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.

50 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.

51 Federal Trade Commission, Public Submission, *Comment Submitted by ACT - Alexandra McLeod, COPPA Rule Review* (March 25, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116872

52 Ibid.

53 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.

54 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.

55 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.

56 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.

57 Federal Trade Commission, Public Submission, *Comments of Internet Association* (March 25, 2020), https://www.regulations.gov/comment/FTC-2019-0054-117011.

58 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.

59 Federal Trade Commission, Public Submission, *Comments of CTIA* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116136.

60 Ibid.

61 16 C.F.R. § 312.12

62 Ibid.

63 Ibid.

64 Ibid.

65 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.

66 Federal Trade Commission, *FTC Letter to Imperium* (December 23, 2013), Accessed May 25, 2023, https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf.

67 Ibid.

68 Ibid.

69 Ibid.

70 Federal Trade Commission, *FTC Letter to Jest8 Limited (Trading as Riyo)* (November 18, 2015), Accessed May 25, 2023, https://www.ftc.gov/system/files/documents/public_statements/881633/151119riyocoppaletter.pdf.

71 Ibid.

72 Ibid.

73 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-cop- pa-verifiable-parental-consent-method/140225iveriflyapplicationletter.pdf.

74 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-cop-pa-verifiable-parental-consent-method/141121agecheqapplication.pdf.

75 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-cop-pa-verifiable.

76 Ibid.

77 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.

78 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.

79 Ibid.

80 Ibid.

81 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.

82 Ibid.

83 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.

84 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.

85 Ibid.

86 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.

87 Ibid.

88 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

89 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.

90 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.

91 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.

92 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.

93 Ibid.

94 Ibid.

95 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.

96 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.

97 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.

98 Ibid.

99 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.

100 Ibid.

101 Ibid.

102 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.

103 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.

104 Ibid.

105 Privo, *Comments of Privo* (December 11, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25092.

106 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.

107 Federal Trade Commission, Public Submission, *Comments of CTIA* (March 24, 2020), https://www.regulations.gov/comment/FTC-2019-0054-116136.

108 Ibid.

109 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.

110 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.

111 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.

112 Ibid.

113 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.

114 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.

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

116 Pavni Diwanji, *How Do We Know Someone Is Old Enough to Use Our Apps?*, Facebook (July 27, 2021), Accessed August 16, 2021, https://about.b.com/news/2021/07/age-verification/.

117 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

118 Meta, *Introducing New Ways to Verify Age on Instagram* (April 13, 2023), https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram#:~:text=If%20someone%20attempts%20to%20edit,friends%20to%20verify%20their%20age.

119 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.

120 Ibid.

121 Ibid.

122 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-ap-proves-the-first-uk-gdpr-certification-scheme-criteria/.

123 Information Commissioner's Office, *Age Check Certification Scheme (ACCS)* (July 13, 2021), https://ico.org.uk/for-organisations/age-check-certification-scheme-accs/.

124 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.

125 Ibid.

126 Federal Trade Commission, Public Submission, *Comment of PRIVO, Inc.* (December 11, 2019), https://www.regulations.gov/comment/FTC-2019-0054-25092.

127 Ibid.

128 Illinois Biometric Information Privacy Act 740 ILCS 14 (2008), available at https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

129 *NetChoice LLC v. Bonta*, No. 5:22-cv-08861-B:F (N.D. CA).

[APPENDICES]

130 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.,

131 Ibid, citing Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 44.

132 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).

133 5 U.S.C. § 552a

134 5 U.S.C. § 552a

135 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

136 Ibid.

137 Ibid.

138 Ibid.

139 Ibid.

140 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.

141 Ibid.

142 Federal Trade Commission, Press Releases, *FTC Staf Sets Forth Principles for Online Information Collection from Children* (July 16, 1997), https://www.ftc.gov/news-events/press-releases/1997/07/ftc-staf-sets-forth-principles-online-information-collection

143 https://web.archive.org/web/20030622142444/https://www.ftc.gov/os/1997/07/cenmed.htm

144 Ibid.

145 Ibid.

146 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.

147 Ibid.

148 Ibid.

149 Ibid.

150 Ibid.

151 Ibid.

152 Ibid.

153 Ibid.

154 Ibid.

155 Ibid.

156 Ibid.

157 105 Cong. Rec. S8482 (July 17, 1998).

158 105 H.R. H.R.4667.

159 105 Cong. Rec. S8482 (July 17, 1998).

160 105 Cong. Rec. S8482-3 (July 17, 1998).

161 105 Cong. Rec. S8482 (July 17, 1998).

162 105 Cong. Rec. E1861 (Oct. 1, 1998).

163 105 Cong. Rec. S8482 (July 17, 1998).

164 105 Cong. Rec. S8482 (July 17, 1998).

165 105 Cong. Rec. S8483 (July 17, 1998).

166 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.

167 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 .

168 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.

169 The Organisation for Economic Co-operation and Development, *About the OECD*, Accessed September 17, 2021, https://www.oecd.org/about/.

170 Ibid.

171 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.

172 GDPR Article 8(1).

173 GDPR Article 8(2).

174 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/.

175 GDPR Article 8(2).

176 GDPR Article 6(1)(f).

177 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.

178 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.

179 Ibid.

180 Andreas Grünwald, Christoph Nüßing, *Youth Protection in Germany: Online Age Checks and Daytime Blackouts Ahead?* (May 23, 2019), https://www.mofo.com/resources/insights/190523-youth-protection-germany

181 Commission nationale de l'informatique et des libertés, *Contrôle de l'âge pour l'accès aux sites pornographiques* (February 21, 2023), https://www.cnil.fr/fr/controle-de-lage-pour-lacces-aux-sites-pornographiques

182 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/.

183 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.

184 euCONSENT (2021), https://euconsent.eu/

185 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/.

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

187 Data Protection Commission, *The Fundamentals for a Child-Oriented Approach to Data Processing* (December 2021) Accessed May 25, 2023. https://www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing

188 Ibid.

189 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/.

190 PIPL, Article 28. See Digichina, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021* (August 22, 2021). https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ .

191 PIPL, Article 31..

192 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.

193 Law on the Protection of Minors, Article 76. See China Law Translate, *Law of the P.R.C. on the Protection of Minors (2020 Edition)* (October 17, 2021). https://www.chinalawtranslate.com/en/protection-of-minors-2020/#_Toc53832363 .

194 Low on the Protection of Minors, Article 75. See China Law Translate, *Law of the P.R.C. on the Protection of Minors (2020 Edition)* (October 17, 2021). https://www.chinalawtranslate.com/en/protection-of-minors-2020/#_Toc53832363 .

195 Brenda Goh, *Three hours a week: Playtime's over for China's young video gamers,* Reuters (August 31, 2021) https://www.reuters.com/world/china/china-rolls-out-new-rules-minors-online-gaming-xinhua-2021-08-30/

196 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-vid- eo-games-2018-12.

197 Brenda Goh, *Three hours a week: Playtime's over for China's young video gamers,* Reuters (August 31, 2021) https://www.reuters.com/world/china/china-rolls-out-new-rules-minors-online-gaming-xinhua-2021-08-30/https://www.reuters.com/world/china/china-rolls-out-new-rules-minors-online-gaming-xinhua-2021-08-30/

198 PDPC, *Advisory Guidelines on the PDPA for Selected Topics* (October 4, 2021), paragraph 7.1. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-4-Oct-2021.pdf?la=en

199 id, paragraphs 7.6, 7.9, and 7.11

200 Ibid.

201 Korea Law Translation Center, *Personal Information Protection Act* (August 5, 2020). https://elaw.klri.re.kr/kor_service/lawView.do?hseq=53044&lang=ENG

202 PIPA, Articles 28(6) and 39-3(2).

203 PIPA, Article 39-3(4).

204 Ibid. See also Korea Law Translation Center, *Enforcement Decree of the PIPA* (August 4, 2020), Article 48-3. https://elaw.klri.re.kr/eng_service/lawView.do?hseq=54521&lang=ENG

205 Ibid.

206 LGPD, Article 14 § 1.

207 *Brazil: Statute of the Child and Adolescent, Law n° 8.069* (July 13, 1990), https://www.refworld.org/docid/4c481bcf2.html.

208 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-cybersecurity/.

209 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/.

210 LGPD, Article 14 § 3.

211 LGPD, Article 14 § 4.

212 LGPD, Article 14 § 6.

213 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/.

214 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.

215 Ibid.

216 GDPR Article 8(2).

217 16 CFR § 312.4

218 Ibid.

219 Ibid.

220 Ibid.

221 Ibid.

222 16 C.F.R. § 312.2: (definition of "persistent identifier")

223 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/.

224 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.

225 Ibid.

226 Federal Trade Commission, *COPPA Safe Harbor Program*, https://www.ftc.gov/safe-harbor-program.

227 Federal Trade Commission, *Aristotle Removed from List of FTC-Approved Childrens Privacy Self-Regulatory Programs* https://www.ftc.gov/news-events/news/press-releases/2021/08/aristotle-removed-list-ftc-approved-childrens-privacy-self-regulatory-programs

228 Ibid.

229 Ibid.

230 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.

231 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.

232 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.

233 Infra p. ___.

234 Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions N. COPPA and Schools,* https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#N.%20COPPA%20AND%20SCHOOLS

235 Ibid.

236 Federal Trade Commission, *FTC Says Ed Tech Provider Edmodo Unlawfully Used Children's Personal Information for Advertising and Outsourced Compliance to School Districts,* https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ed-tech-provider-edmodo-unlawfully-used-childrens-personal-information-advertising

237 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).

238 *Mobile App Child Privacy Settlements*, Accessed August 10, 2021, https://web.archive.org/web/20210414202400/https://mobileappchildprivacysettlements.com/.

239 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.

240 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.

241 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

242 Steve Bellovin, *COPPA and signaling, Federal Trade Commission* (January 2, 2013), Accessed August 10, 2021, http://web.archive.org/web/20140825170141/http://techatftc.wordpress.com:80/2013/01/02/coppa-and-signaling/.

243 16 C.F.R. § 312.8

244 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.

245 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.

246 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.

247 Ibid.

248 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/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#step4.

249 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.

250 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.

251 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.

252 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), available at http://www.ftc.gov/reports/privacy3/toc.shtm.

253 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.

254 Ibid.

255 Lauren A. Matecki, *Update: COPPA is Ine!ective 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.

256 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.

257 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.

258 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.

259 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.

260 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.

261 Ibid

262 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.

263 Ibid.

264 Ibid.

265 Ibid.


FUTURE OF
PRIVACY
FORUM