American University Washington College of Law
Digital Commons @ American University Washington College of Law

Joint PIJIP/TLS Research Paper Series

8-1-2024

Child Privacy in the Digital Era: Is COPPA Enough?

Melannie Sandoval

Follow this and additional works at: https://digitalcommons.wcl.american.edu/research

 Part of the Communications Law Commons, and the Internet Law Commons

Abstract

Children growing up in the digital age are experiencing an entirely different world than their parents once did. While most adults' first online experience occurred on a bulky desktop computer, today's children are born into a society that is largely digitized and where online accessibility is at the swipe of a pocket-sized smartphone. Despite the many benefits that this generation of children enjoys due to the increased access to the internet and innovative technology, parents, child advocates, and privacy experts caution against the dangers that arise when children enter the digital landscape.

Part I of this paper delves into children's interaction with the internet and the surrounding online technology, while also highlighting the different risks they are exposed to today with their online presence. Part II of this paper explores the United States' current regulatory framework, the Children's Online Privacy Protection Act ("COPPA"), which was enacted in 1998 with the intention of safeguarding children's personal information from being collected when using online services, websites, games, or apps. Part II continues by examining the FTC's proposed amendments for the COPPA Rule in response to the evolving landscape of online platforms that now largely involves social media, video-sharing websites, and IoT devices. Lastly, Part III evaluates whether, even with full compliance, the COPPA Rule or its proposed revisions can effectively mitigate privacy risks and subsequent privacy harms children are exposed to in the digital age.

Part I. Kids Online and the Risks They Face

A. Children's Usage of the Internet and Technology

With each passing year, children are spending more time on the internet because it accounts for a large part of their social life, entertainment, and educational experience.[1] A 2024 Report by *Internet Matters* highlighted children's well-being in a digital world, showcasing the ways in which children use the internet today, which include: chatting with friends, streaming movies or shows, and playing online video games.[2] This is enabled by the growing number of children, of all ages, owning smartphones.[3]

Since the pandemic, children have also increasingly taken advantage of study applications that supplement their traditional school learning in a way that gamifies their studying and provides instantaneous feedback.[4] Additionally, today's internet landscape not only includes digital content consumption but also incorporates a rapid growth in digital content creation,[5] with children of Generation Alpha entering the influencer space.[6] A potentially inadvertent use of the internet by children involves Internet of Things ("IoT") devices, as more ordinary devices are converted to Smart devices by being connected to the internet.[7]

Ultimately, the digital landscape plays a core part of youths' lives by providing a space to express and explore their identities.[8] However, even with the significant convenience and

---

[1] *See generally Child and Youth Safety Online*, UNITED Nations, https://www.un.org/en/global-issues/child-and-youth-safety-online.

[2] *See* Internet Matters, *Children's Wellbeing in a Digital World: Year 3 Index Report 2024* at 25 (2024).

[3] *See* Federica Laricchia, *Share of U.S. Children Owning a Smartphone 2015-2021 By Age*, STATISTA (Oct. 26, 2023) https://www.statista.com/statistics/1324262/children-owning-a-smartphone-by-age-us/ (revealing that 31% of 8-year-olds surveyed owned a smartphone, which was a stark increase from 2015, where it was only 11%).

[4] *See* Louise Wylie, *Education App Revenue and Usage Statistics*, BUS. OF APPS, https://www.businessofapps.com/data/education-app-market/ (last updated Jan. 8, 2024).

[5] *See* Ali Asku, *The Future Belongs to Impact-Driven Creators: The Shift in the Creator Economy*, ROLLING STONES (Dec. 15, 2023) https://www.rollingstone.com/culture-council/articles/future-belongs-to-impact-driven-creators-the-shift-creator-economy-1234928851/.

[6] *See* Gillian Follett*, Gen Alpha Influencer Marketing–How Brands Can Work with Young Creators*, ADAGE (Jan. 19, 2024), https://adage.com/article/digital-marketing-ad-tech-news/gen-alpha-influencer-marketing-how-brands-can-work-young-creators/2537591.

[7] *See* Eldar Haber, *The Internet of Children: Protecting Children's Privacy in a Hyper-Connected World*, 2020 U. ILL. L. REV. 1209, 1212 (2020).

[8] Kathryn C. Montgomery et, al., *Children's Privacy in the Big Data Era: Research Opportunities*, 140 PEDIATRICS 117, 118 (Nov. 01, 2017).

benefits that technological advances and internet accessibility bring, children's online presence poses substantial risks to their data privacy that they may not fully grasp.[9]

B. Risks to Children Online Today

i. Data Breach and Identity Theft

Platforms often collect and retain personal data from its users, voluntarily or passively provided.[10] This information may include a phone number, email, and physical address, though it can also extend to real-time location, biometrics, and Social Security numbers.[11] However, if a platform fails to securely collect and retain the data, a data breach can occur.[12] A data breach is defined as "the release of confidential, private, or otherwise sensitive information into an unsecured environment."[13] These breaches can occur in several ways. For example, the Federal Trade Commission ("FTC") explains it can ensue when: an unauthorized person hacks into a company's corporate server and unlawfully takes personal information; an insider of the entity steals the company's consumer information; or if it was unintentionally shared as a leak.[14]

Although all people, regardless of age, are exposed to this risk by engaging in the online space, children are particularly vulnerable to targeted data breaches.[15] A study performed by *Javelin Strategy and Research* discovered that in 2022 "one in every 43 children had their personal information exposed and potentially compromised in the past year by a data breach,[16]" and another report found that over 50% of children are more prone to be victim of

---

[9] *See* Samuel M. Roth, *Data Snatchers: Analyzing TikTok's Collection of Children's Data and Its Compliance With Modern Data Privacy Regulations*, 29 J. HIGH TECH. L. 1, 35 (2021).

[10] *What is PII (personally identifiable information)?*, CLOUDFARE, https://www.cloudflare.com/learning/privacy/what-is-pii/ (exemplifying collected personally identifiable information to include a physical address, email, or phone number directly linked to an identity, or linkable information that when combined with other data elements identifies a person to the information).

[11] *See* Kelly Graham, et al., *Privacy Risks and Harms*, COMMON SENSE MEDIA 9 (2019), *available at* https://privacy.commonsense.org/content/resource/privacy-risks-harms-report/privacy-risks-harms-report.pdf.

[12] *See id.*

[13] *See What is a Data Breach?*, CLOUDFARE, https://www.cloudflare.com/learning/security/what-is-a-data-breach/# (last visited Apr. 25, 2024).

[14] *See Data Breach Response: A Guide for Business*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business.

[15] *See* Graham, *supra* note 11.

[16] *See* Javelin Strategy & Research**,** *1.7 Million U.S. Children Fell Victim to Data Breaches, According to Javelin's 2022 Child Identity Fraud Study*, PRWEB (Oct. 26, 2022), https://www.prweb.com/releases/1-7-million-u-s-children-fell-victim-to-data-breaches-according-to-javelin-s-2022-child-identity-fraud-study-851086633.html#:~:text=Javelin%20found%20that%20beyond%20suffering%20from%20identity%20fra

identity theft compared to adults.[17] Cybercriminals recognize that children are valuable targets, because they are less likely to identify a scam and also hold access to sensitive information, sometimes including that of their parents.[18] Many adults have received training or some sort of exposure to what scams may look like and thus are not as easily tricked by beguiling efforts to divulge their sensitive data. Thus, cybercriminals target websites and platforms popular among children and pretend to offer attractive features, like free access to online games or content, in exchange for data from children – exploiting their lack of awareness regarding the sensitivity of the information they provide.[19] This can also be done by convincing them to download malware that would breach their device to access confidential info.[20]

ii. Online Child Predators

As discussed in Part I (A), children today utilize the internet to socialize and communicate with family and friends they know in person, or connections they make online.[21] For some children, it is easier to socialize online than in person because the device's screen alleviates the pressure from face-to-face interactions with people.[22] However, this dynamic may be abused by adult predators looking to interact with children through fake accounts, and pretending to share the same interests and hobbies, offering them gifts, or complimenting them.[23]

The ongoing concern about child predators, which was a critical component of discussion for the creation of COPPA, continues to be a significant issue in present-day

---

ud%2C,every%2043—having%20personal%20information%20exposed%20and%20potentially%20compromised.

[17] *See* Avery Wolfe, *How Data Breaches Affect Children*, AXIOM CYBER SOL. (Mar. 15, 2018), https://axiomcyber.com/data-breach/how-data-breaches-affect-children/ [https://web.archive.org/web/20231028012852/https://axiomcyber.com/data-breach/how-data-breaches-affect-children/]; *see also id.* ("children under the age of 7 were most likely to be victimized by ID theft and subsequent ID fraud").

[18] *See* Andrey Sidenko, *Kids and Cybersecurity: What Parents Should be Aware of in 2024*, KASPERSKY (Jan. 17, 2024), https://www.kaspersky.com/blog/cybersecurity-threats-for-kids-2024/50188/.

[19] *See id.*

[20] *See id.*; *see also How Scammers Target Kids Online*, ONPOINT CMTY. CREDIT UNION, https://www.onpointcu.com/blog/how-scammers-target-kids-online/.

[21] *See Children and Grooming / Online Predators*, CHILD CRIME PREVENTION & SAFETY CENTER, https://childsafety.losangelescriminallawyer.pro/children-and-grooming-online-predators.html.

[22] *See supra* note 2, at 10.

[23] *See Children and Grooming / Online Predators*, CHILD CRIME PREVENTION & SAFETY CENTER, https://childsafety.losangelescriminallawyer.pro/children-and-grooming-online-predators.html (last visited Apr. 24, 2024).

discussions surrounding children's online safety.[24] Regarding children's data, this concern primarily revolves around: 1) fear of sexual predators communicating with minors to gather personal information, including the solicitation of explicit photos; and 2) that the sexual predators use the information to initiate direct contact with the child and potentially harm them.[25]

iii. Monetization of Children's Data

Data is generated by users while surfing the web, using mobile apps, and engaging with IoT devices.[26] By partaking in activities that are connected to the internet, online platforms can collect information on users such as websites visited, past purchases, browsing habits, and personal identifiers.[27] When further refined, processed, and combined, such data becomes monetizable, making its collection a revenue opportunity,[28] and an attractive commodity to advertisers and third-party companies for targeted advertising, or to be used by the operators themselves to increase duration and frequency use of their platform and sell in-app purchase options.[29]

Children's data in particular is highly prized for operators because they are more susceptible to influence than adults and are more vulnerable to the collection as some companies develop commercial relationships with them and take advantage of their trust or lack of judgment.[30] There are now more opportunities for the collection of children's data

---

[24] *See* Melanie L. Hersh*, Is COPPA a Cop Out? The Child Online Privacy Protection Act As Proof That Parents, Not Government, Should Be Protecting Children's Interests on the Internet*, 28 FORDHAM URB. L.J. 1831, 1854 (2001); *see also* Laura Draper, *Protecting Children in the Age of End-to-End Encryption, JOINT PIJIP/TLS RSCH. PAPER SERIES* at 9 (2022), https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1082&context=research.

[25] *See* Draper *supra* note 24, at 12 (describing a notable trend where children are "enticed, induced, or exploited into taking [explicit] images by someone they. . . met online"); *see also* Dan Frechtling*, Is the U.S. Government Doing Enough to Protect Children Online?*, OPEN ACCESS GOV'T (June 20, 2023), https://www.openaccessgovernment.org/u-s-government-doing-enough-protect-children-online/160137/ ("[B]ad actors and predators online may access children's data and use it for nefarious purposes, even contacting them directly").

[26] *See* Fangwei Zhao, et al., *Data Collection Practices of Mobile Applications Played by Preschool-Aged Children*, JAMA PEDIATRICS (Sept. 8, 2020), https://jamanetwork.com/journals/jamapediatrics/fullarticle/2769689.

[27] *See id.*

[28] *See* Yonego Joris Toonders, *Data is the New Oil of the Digital Economy*, WIRED, https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last visited Apr. 25, 2024),

[29]*See* Jenny Radesky, et al., *Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children's*, JAMA NETWORK OPEN at 2 (June 17, 2022).

[30] *See* Federal Trade Commission, *Statement of Commissioner Alvaro M. Bedoya On the Issuance of the Notice of Proposed Rulemaking to Update the Children's Online Privacy Protection Rule,* 6-8 (Dec. 20, 2023) (exemplifying a website that was Batman-themed to ask children to complete a

stemming from children's increased use of social media, online games, educational apps, as well as IoT devices.[31] Moreover, persistent identifiers may permit operators to track a user's activities over time and across different devices, even without the user actively using the platform.[32] This makes the collection of a child's data from platforms, including those child-directed and those directed to a general audience, hard to detect or understand how extensive it really is.[33]

Since children's data is deemed valuable, operators may turn to generating manipulative design features, also referred to as "dark patterns," as a tactic to 1) encourage kids' prolonged use of an app; 2) incite them to re-engage via persuasive push notifications; or 3) pressure the child user to make purchases or watch advertisements.[34] Further, a 2020 study revealed that two-thirds of apps used by children collected digital identifiers and a different study suggested that more child-directed apps contained third-party trackers than adult apps, ultimately demonstrating that operators are still able and willing to collect and monetize off of children's data at the child's privacy expense.[35]

iv. Cyberbullying and Mental Health Harm

Though not a prominent concern at the time COPPA was drafted, a legitimate issue children face when entering the online landscape today is cyberbullying.[36] Cyberbullying is defined as harassing, threatening, embarrassing, or targeting another individual online through different

---

form by instructing them: "Become a valued citizen of Gotham and complete this census") *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/BedoyaStatementonCOPPARuleNPRMFINAL12.20.23.pdf

[31] *See* Olufunmilayo B. Arewa, *Data Collection, Privacy, and Children in the Digital Economy*, *in* FAMILIES AND NEW MEDIA 199 (2023); *see also* Zhao, *supra* note 28.

[32] *See The Shadow Market: How Big Tech Exploits Children's Data*, KIDS INC. (Dec. 8, 2023), https://www.kidsinc.cc/the-shadow-market-how-big-tech-exploits-children-s-data

[33] *See generally id.*

[34] *See* Jenny Radesky, et al., *Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children's*, JAMA NETWORK OPEN (June 17, 2022), https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2793493?utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=061722; (noting that the exploitive nature of these designs, in conjunction with the creation of profiles based on kids' data, can pick up on and exploit on their vulnerabilities).

[35] *See* S. Liao & Claudia Ferreira, *Kids Deserve Privacy Online. They're Not Getting It.*, THE ATL. (Sept. 14, 2023), https://www.theatlantic.com/ideas/archive/2023/09/kids-online-data-privacy-tracking-apps/675320/.

[36] *See* Usha Munukutla-Parker, *Unsolicited Commercial E-mail, Privacy Concerns Related to Social Network Services, Online Protection of Children, and Cyberbullying*, 2 I/S: J.L. & POL'Y FOR INFO. SOC'Y 627, 628 (2006); *see also* Stephen Beemsterboer, *COPPA Killed the Video Star: How the YouTube Settlement Shows that COPPA Does More Harm Than Good*, 25 ILL. BUS. L.J. 63, 75, n.106 (2020).

mediums like social media, online games, and instant messaging.[37] Cyberbullying can include the posting, sending, or sharing of content (i.e., comments, photos, posts) that is negative or harmful to another, whether the content itself is true or not.[38] In contrast to the traditional form of bullying, cyberbullying occurs online and thus transcends physical barriers, allowing bullies to target their victims in a relentless and very public manner.[39] Another difference is that a cyberbully can choose to perform harmful conduct while hiding their identity behind the internet.[40] Additionally, on social media platforms, the level of embarrassment or humiliation is exacerbated by the fact that cyberbullying can reach a much larger audience, including not only the victim and their acquaintances, but also by strangers online.[41] Lastly, as a result of the harmful content posted by a cyberbully the unsolicited content of a child victim becomes part of their digital footprint even if the original post is removed.[42]

Moreover, the mental health of children, including teens, has also drawn concern from parents and child advocates with the rise in social media use.[43] Although earlier versions of social media was set up to showcase primarily the accounts that one followed – typically intimate content from friends and family – today's platform exposes its users to heavily curated content that targets each individual with the aim of increasing user retention and screen time.[44] The use of algorithm-backed automated systems has gained popularity; and although the type of algorithms varies per platform, at its core it is comprised of a set of rules and signals that generate a programmed ranking of content based on data collected by the user, including their tracked likes, comments, and other online behavior.[45] Ultimately, since more engagement

---

[37] *See What Is Cyberbullying*, STOPBULLYING, https://www.stopbullying.gov/cyberbullying/what-is-it (last visited Apr. 24, 2024).
[38] *See id.*
[39] *See id.*
[40] *See* Munukutla-Parker, *supra* note 36, at 645.
[41] *See* Munukutla-Parker, *supra* note 36, at 644-45.
[42] *See On Social Media, Delete Does Not Really Exist,* EVOLVE (Oct. 08, 2020), https://evolvetreatment.com/blog/social-media-consequences/ (noting that even if your press the delete button a second after posting, its existence is not scrubbed from the internet and may still be accessible).
[43] *See* Jesse Greenspan, *Social Media Can Harm Kids. Could New Regulations Help?*, SCI. AM. (May 26, 2023), https://www.scientificamerican.com/article/social-media-can-harm-kids-could-new-regulations-help/ ("adolescent rates of depression, anxiety, loneliness, self-harm and suicide have skyrocketed in the U.S. and elsewhere since around the time that smartphones and social media became ubiquitous").
[44] *See generally* Juan Lodoño*, Assessing the Impact of the Widespread Adoption of Algorithm-backed Content Moderation in Social Media*, AM. ACTION F. (Jan. 25, 2022), https://www.americanactionforum.org/insight/assessing-the-impact-of-the-widespread-adoption-of-algorithm-backed-content-moderation-in-social-media/#ixzz89ZNpYimF.
[45] *See* Hannah Trivette, *A Guide to Social Media Algorithms and SEO*, FORBES (Oct. 14, 2022), https://www.forbes.com/sites/forbesagencycouncil/2022/10/14/a-guide-to-social-media-algorithms-and-seo/?sh=78c8973052a0 (delving into the different factors social media platforms like Facebook and Twitter use that impact how quickly a post will be noticed and the size of the audience it will reach); Will

essentially equates to more profit, social media companies' algorithmic designs may overlook whether the content it is recommending is harmful or not to its receiver.[46]

Despite some applications being age restricted, children still manage to get on social media platforms and thus are exposed to its algorithmic designs.[47] In a study performed by *the Center for Countering Digital Hate*, researchers discovered that an algorithm can recognize vulnerability and rather than exercising caution with it, the algorithm identifies it as a "a potential point of addiction … [and a way] to maximize time on the platform for [a] child.[48]" The study, based on youth users, found that: in less than 3 minutes, the TikTok algorithm recommended content about suicide; in under 8 minutes, the algorithm recommended content surrounding disordered eating; and approximately every 39 seconds, content surrounding body image and mental health would be suggested.[49] This study indicated that platforms with algorithmic designs that prioritize engagement over safety makes its environment toxic to youth, impacting their mental and even physical health.

Part II. An Overview of COPPA

A. What Led to COPPA?

The 1990s marked the commencement of a more interconnected world as the *World Wide Web* became publicly accessible and revolutionized the way people interacted with others in an

---

Oremus, *Social Media Can Be Polarizing. A New Type Of Algorithm Aims to Change that*., WASH. POST (Jan. 11, 2023), https://www.washingtonpost.com/politics/2023/01/11/social-media-can-be-polarizing-new-type-algorithm-aims-change-that/ (flagging that "algorithm amplification" rewards all engagements and thus finding that generated recommended content also arises from negative interactions with user-content, be that with angry comments or discontent reactions).

[46] *See* Olivia Carville, *TikTok's Algorithm Keeps Pushing Suicide to Vulnerable Kids*, BLOOMBERG, https://www.bloomberg.com/news/features/2023-04-20/tiktok-effects-on-mental-health-in-focus-after-teen-suicide; *Social Media Algorithms Amplify Misogynistic Content to Teens*, UNIV. COLL. LONDON (Feb. 25, 2024), https://www.ucl.ac.uk/news/2024/feb/social-media-algorithms-amplify-misogynistic-content-teens#:~:text=Social%20media%20algorithms%20amplify%20extreme,led%20by%20a%20UCL%20researcher.

[47] *See* Kevin Rawlinson, *How TikTok's Algorithm 'Exploits the Vulnerability' of Children*, THE GUARDIAN (Apr. 4, 2023), https://www.theguardian.com/technology/2023/apr/04/how-tiktoks-algorithm-exploits-the-vulnerability-of-children ("1.4 million children under the age of 13 have been allowed access to TikTok")

[48] *See id.*

[49] *See Deadly By Design: Tiktok Pushes Harmful Content Promoting Eating Disorders and Self-Harm Into Young Users' Feeds*, CTR. FOR COUNTERING HATE (Dec. 15, 2022), https://counterhate.com/research/deadly-by-design/.

online format.[50] The FTC observed the exponential marketplace growth that came with an online medium and flagged the noteworthy number of children online that were now susceptible to targeted marketing techniques and personal data collection when they used online chatrooms, videogames, and even homework assistance sites.[51] In 1997, following an investigation into KidsCom–a website directed to children and whose data collection practices were considered to likely violate Section 5 of the FTC Act–the FTC issued a letter outlining the limits of what info can be collected from children online.[52] Through this letter, the FTC laid down principles of adequate disclosures of a site's data collection practices and its intended use, as well as the need for prior parental consent when dealing with children's data in particular.[53]

In 1998 the FTC reiterated its concern about the collection of children's data in its report "*Privacy Online: A Report to Congress*.[54]" The report highlighted that, unlike adults, children are not as apprehensive about the risks associated with sharing their personal information, whether voluntarily when prompted by a site or incidentally through the use of cookies.[55] The report revealed that eighty-nine percent of the child-directed online sites they surveyed collected children's personal and identifiable information (i.e., names, physical addresses, phone numbers, and date of birth); in certain cases, the sites also collected a parent's information through the children, where the children were asked questions prompting them to disclose whether the parent owns a mutual fund.[56]

The FTC's letter in response to KidCom's data collection practices, in conjunction with the FTC's 1998 report findings, were among the major factors that led Congress to enact the Children's Online Privacy Protection Act ("COPPA" or "the Act") in 1998.[57] The Act served to increase parental involvement and control over the collection and dissemination of children's

---

[50] *See World Wide Web (WWW) Launches in the Public Domain*, HISTORY https://www.history.com/this-day-in-history/world-wide-web-launches-in-public-domain (last updated Apr. 29, 2024).
[51] *See* Federal Trade Commission, *Privacy Online: A Report to Congress* at 4, 33 (June 1998) (hereinafter "1998 FTC Report") https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.
[52] *See* Press Release, Fed. Trade Comm'n, FTC Staff Sets Forth Principles For Online Information Collection From Children (July 16, 1997), https://www.ftc.gov/news-events/news/press-releases/1997/07/ftc-staff-sets-forth-principles-online-information-collection-children*; see also How COPPA Came About,* INFORMATION WEEK (Jan. 14, 2004), https://www.informationweek.com/it-leadership/how-coppa-came-about (describing KidsCom's practices for collecting children's data include soliciting information via registration forms, contests, and for participation in their pen-pal programs).
[53] *See* Fed. Trade Comm'n *supra* note 52.
[54] *See* 1998 FTC Report, *supra* note 51, at 4.
[55] *See* 1998 FTC Report, *supra* note 51, at 3.
[56] *See* 1998 FTC Report, *supra* note 51, at 31-34, 39.
[57] *See How COPPA Came About,* INFORMATION WEEK (Jan. 14, 2004), https://www.informationweek.com/it-leadership/how-coppa-came-about.

data.[58] Through COPPA, Congress delegated authority to the FTC to adopt regulations that implemented online privacy protections over the personal information of children under 13.[59] On April 21, 2000, the FTC's Children's Online Privacy Protection Rule ("the Rule" or "the COPPA Rule") became effective and included enforcement power under which action may be brought if a site or app was found non-compliant.[60] In 2013, the FTC introduced changes to the Rule to broaden and clarify the Rule's application with new technological developments in mind, such as geolocation information and social networking.[61]

B. A Breakdown of the COPPA Rule and Its Requirements

The Rule places limitations on operators of child-directed commercial websites and online services[62] that collect personal data from and about children aged 12 and under.[63] The FTC identified factors for determining whether a website or service is directed, or targeted, to children, which include 1) if upon extrinsic examination of the site it contains child-oriented incentives and activities, and 2) if empirical evidence regarding its audience composition notably reflects children.[64] Although the Rule does not normally apply to websites or services that serve a general audience, if an operator were to gain actual knowledge of children using their website or service they then become subject to COPPA's Rule for compliance.[65]

The Rule requires two obligations for operators with sites and services under its scope. The first obligation is that a child-directed site or service must publish on its landing page or screen an effective notice that clearly and comprehensively describes its practice for data use and

[58] *See* 15 U.S.C.A §§ 6501- 6505; *see also Children's Privacy*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/issues/data-protection/childrens-privacy/ (last visited Apr. 19, 2024).
[59] *See* 15 U.S.C.A § 6502(b)(1).
[60] *See* 16 C.F.R. § 312 (2013).
[61] *See* Final Rule Amendments, 78 Fed. Reg. 3972 (Jan. 17, 2013) (reflecting changes in five significant areas, including updating definitions of "personal information," "operator" and "collection," among other key terms; clarifying what satisfies the parental notice obligation; enumerating new approved parental consent mechanisms; extending the operator's responsibility when maintaining and discarding child data to inquire a third party's, with whom they share the data, confidentiality and security assurances; and specifying requirements for approved safe harbor programs).
[62] *See Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited Apr. 19, 2024) (noting that services covered under COPPA are inclusive of mobile apps and IoT devices such as smart speakers, Internet-enabled gaming platforms, and voice-over-Internet protocol services).
[63] *See* 16 C.F.R. § 312.
[64] *See* 16 C.F.R. § 312.2.
[65] *See Children's Online Privacy Protection Rule: Not Just for Kids' Sites*, FED. TRADE COMM'N https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-not-just-kids-sites (last visited Apr. 19, 2024).

collection from children.[66] The notice requirement additionally demands that the operator provide direct notice to the child's parent, via reasonable efforts, to ensure the parent is aware of the data collection practices to which the child would be exposed to when using the site or service.[67]

Secondly, operators of child-directed sites or services are obligated to comply with the verifiable parental consent requirement of the Rule.[68] According to the Rule, before any personal data can be collected from a child under 13, an operator must give the parent the choice of consenting to the collection and use of their child's personal data.[69] It additionally mandates that the operator attain the parent's verifiable consent.[70] Section 312.5(b) of the Rule lays out existing methods deemed as acceptable means that are reasonably calculated for sites to obtain verifiable parental consent in light of existing technology.[71] Nonetheless, the Rule explicitly clarifies that in consenting to the data collection, the parent is not explicitly giving the operator permission to disclose the data to third parties.[72]

Aside from the two main obligations of notice and parental consent, the Rule also establishes other rights, responsibilities, and restrictions under its scope. For example, the Rule grants a parent access to review their child's collected personal data, with the option to have the information deleted by the operator upon request.[73] Further, the Rule expresses a strict prohibition against sites or services conditioning a child's participation in an activity (i.e., games, contests, prize giveaways) on the child providing further personal data than is "reasonably necessary" to partake in the activity.[74] Operators subject to the Rule also must establish procedures to keep collected data confidential and secure, which extends to their ability to share the data only with parties that can keep the same assurances.[75] Lastly, they are limited to retaining the data only for the time necessary to fulfill its collection's purpose and are responsible for discarding the data in a way that prevents unauthorized access to or use of it. [76]

---

[66] *See* 16 C.F.R. § 312.4 (d).
[67] *See* 16 C.F.R. § 312.4 (b).
[68] *See* 16 C.F.R. § 312.5 (a)(1).
[69] *See* 16 C.F.R. § 312.5 (a)(1).
[70] *See* 16 C.F.R. § 312.5 (a)(2).
[71] *See* 16 C.F.R. § 312.5 (b)(2) (listing the methods, which includes consent via: a parent-signed consent form that is returned to the operator via postal mail, fax, or electronic scan; a parent call to a toll-free number that is controlled by trained staff; a parent video-conference call with trained staff; the use of a credit card that alerts the primary account holder of a transaction; and a cross-check of the parent's government-issued ID, of which would be discarded after verification).
[72] *See* 16 C.F.R. § 312.5 (a)(2) (demonstrating that consent to the data collection does not extend to consent to its disclosure; however, the Rule also does not require the operator to seek separate consent to disclose the information to third parties).
[73] *See* 16 C.F.R. § 312.6.
[74] *See* 16 C.F.R. § 312.7.
[75] *See* 16 C.F.R. § 312.8.
[76] *See* 16 C.F.R. § 312.10.

C. The FTC's Proposed Amendments for the COPPA Rule

In January of 2024, the FTC issued a Notice of Proposed Rulemaking ("NPRM") to update the COPPA Rule, once again, in response to the rapid evolution of available technology.[77] Although the FTC does not have the power to make changes to the Act itself, the congressionally delegated authority within the Act does permit the agency to make substantial modifications to the Rule through which the Act is enforced.[78] While COPPA initially focused on giving parents more control to ensure children are safe digitally, now through the proposed changes to the Rule, the FTC aims to shift that burden onto online service operators.[79]

The NPRM details what it has declined to review or change of the Rule, as well as many proposals to modify the Rule; however, eight key modifications stand out. First, the Rule's proposed revisions include expanding the definitions of the Act's key terms. The FTC proposes to expand the definition of "online contact information," which is utilized in the Act to describe the type of information an operator can obtain from a child that permits direct contact with a person online for a particular purpose (i.e., to begin the process of obtaining parental consent).[80] Although the Act already includes a non-exhaustive list of permissible identifiers for limited purposes, the suggested modification would add mobile telephone numbers as a form of online contact information, but limit it to only sending a text message, ultimately presenting operators with a new form of obtaining parental consent for data collection.[81] The FTC also proposes broadening the definition of "personal information," to include biometric data since technological advancements have facilitated consumer products' increasing use of this type of sensitive personal data for identification. [82] "Website or online service directed to children," is another term that the FTC proposes to alter for clarity in its interpretation, particularly about the factors the FTC will consider in determining whether a site is child-directed.[83] The new suggested factors would include a site's "marketing or promotional materials or plans,

[77] *See* Notice of Proposed Rulemaking, 89 Fed. Reg. 2034 (Jan. 11, 2024).
[78] *See* 15 U.S.C.A. § 6502(b).
[79] *See* Press Release, Fed. Trade Comm'n, FTC Proposes Strengthening Children's Privacy Rule to Further Limit Companies' Ability to Monetize Children's Data (Dec. 20, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens?utm_source=govdelivery (". . . [the] proposal places affirmative obligations on service providers and prohibits them from outsourcing their responsibilities to parents").
[80] *See* 89 Fed. Reg. 2034 at 2040.
[81] *See id.*
[82] *See* 89 Fed. Reg. 2034 at 2041 (defining biometric data as "[a] biometric identifier that can be used for the automated or semi-automated recognition of an individual, including fingerprints or handprints; retina and iris patterns; genetic data, including a DNA sequence; or data derived from voice data, gait data, or facial data.).
[83] *See* 89 Fed. Reg. 2034 at 2046-47.

representations to consumers or third parties, reviews by users or third parties, and the age of users on similar websites or services".[84]

The FTC's second proposal extends the existing consent obligation concerning an operator's site or service collection of a child's data by requiring separate parental consent if the gathered data were to be shared with third parties, including third-party advertisers.[85] The Rule's third proposal reaffirms its prohibition on collecting more data than is needed for a child to be able to participate in a game or activity by clarifying that this ban is not waivable even if the company were to acquire verified parental consent.[86] Further, by building upon current FTC guidance allowing schools and educational agencies to consent to children's data collection in the place of parents, the FTC's fourth recommendation in the NPRM suggests formalizing this exception by conditioning it on the establishment of a contractual relationship between an operator and the school.[87] The proposal also explicitly clarified that the school's consent to the collection is limited to school-authorized education purposes and not commercial purposes.[88]

The NPRM also emphasizes strengthening data security. Thus, the fifth key suggested change relates to requiring the operator to implement and maintain a written comprehensive children's personal information security program.[89] Such a program would need to incorporate appropriate safeguards proportional to the type of collected data and the operator's size and scope of activities.[90] Moreover, the NPRM also emphasized changes to the Rule's data retention section in its sixth key proposal, prohibiting indefinite data retention or use for any secondary purpose, and requiring operators to disclose their written data retention policies on their site for data collected from and about children.[91]

Currently, under COPPA, there is an exception where parental consent is not necessary if the collected persistent identifiers are solely to support a site's internal operations and if the operator does not collect any other personal information.[92] However, the NPRM's seventh proposal would require operators using this exception to adhere to a notice requirement that

---

[84] *See id.*

[85] *See* 89 Fed. Reg. 2034 at 2049, 2051 (noting this would not apply where the data collection is integral to the nature of the site (i.e., an online messaging forum)).

[86] *See* 89 Fed. Reg. 2034 at 2060.

[87] *See* 89 Fed. Reg. 2034 at 2055-57.

[88] *See id.*

[89] *See* 89 Fed. Reg. 2034 at 2061.

[90] *See id.* (requiring that the program "at least annually performing additional assessments to identify risks to the confidentiality, security, and integrity of personal information collected from children; designing, implementing, and maintaining safeguards to control any identified risks, as well as testing and monitoring the effectiveness of such safeguards; and, at least annually, evaluating and modifying the information security program").

[91] *See* 89 Fed. Reg. 2034 at 2062 (highlighting a new proposed obligation for data retention similar to the current obligation to disclose the collection practices under the notice requirement).

[92] *See* 16 C.F.R. § 312.2.

1) declares the specific internal operations and 2) details measures taken to secure the identifiers from unauthorized use or disclosure for individual contact.[93] Lastly, the eighth key proposal detailed in the NPRM concerns operators' practice of using personal identifiers to prompt a user to use an app or service more to maximize engagement and user attention.[94] The FTC suggestion would explicitly disallow the collection of data for engagement optimization purposes to qualify under the internal operations exception, ultimately demanding parental consent if the operator would like to optimize a child's engagement on their site by using or disclosing their persistent identifiers.[95]

Part III. Does Full Compliance with the COPPA Rule, or Even a Recalibrated Rule, Sufficiently Mitigate the Online Risks to Children?

Although COPPA was designed to safeguard children's online privacy by placing barriers to the collection of their data, even if those subject to the Rule fully comply with the obligations, it still leaves gaps that do not adequately cover the risks that children face in today's digital landscape. Although the FTC has rolled out proposals to the Rule to mitigate these issues, it may not be enough.

A. The Gaps in COPPA

i. A Flawed Child-Directed Standard

Under Section 312.3 of the COPPA Rule, an operator whose site or service is knowingly child-directed, whether intentional or not and collects data from children is required to comply with the Rule's obligations.[96] Thus, websites that are unmistakably child-directed because they exclusively tailor their service or site to children can be squarely identified as needing to be compliant with the Rule. Moreover, the FTC states that sites or apps that have a "mixed audience", meaning that children are considered a part of the audience even if not the *primary* audience, the site would also be considered child-directed.[97] However, many services or apps that are technically accessible to children fall into a grey area where they may or may not be categorized as child-directed. For example, according to FTC guidance, a site that may be directed to a general audience but used by children does not automatically make it child-

[93] *See* 89 Fed. Reg. 2034 at 2045.
[94] *See id.; see also FTC Seeks to Bridge Gaps with Proposed COPPA Rulemaking*, IAPP (Jan. 2, 2024), https://iapp.org/news/a/ftc-seeks-to-bridge-gaps-with-proposed-coppa-rulemaking (referencing the practice as being commonly referred to as "online nudging").
[95] *See id.*
[96] *See* 16 C.F.R. § 312.3.
[97] *See* Federal Trade Commission, *supra* note 62.

directed, except if the operator gains actual knowledge of child users, then the COPPA Rule obligations are triggered.[98] The issue with this is that absent gaining actual knowledge, operators may be collecting children's data because they may be under the impression, or allege to be under the impression, that their site or app is not targeted to children and hence bypass the need to get verified parental consent.

YouTube channels like Cocomelon[99] likely meet COPPA's child-directed factors (i.e., considering the subject matter, visual representation, empirical audience evidence, and children-oriented activities); however, YouTube channels that produce content appealing to both adults and children are more difficult to evaluate.[100] This is exacerbated by the fact that children's interests are not monolithic and can shift frequently as they discover new curiosities.[101] Thus, with COPPA's essentially objective standard for what is child-directed based on what children ordinarily find attractive, there are apps or websites technically outside that group that are still able to collect and monetize off a child's data.[102] Even with the amendments proposed by COPPA to expand the factors[103] for determining whether something is child-directed and thus requires compliance, the proposal still emphasizes what objectively would attract kids to the platforms, overlooking platforms that do not outwardly fit that standard.

A less obvious example of this issue relates to IoT devices. The convenience and efficiency of having IoT devices like Smart TVs, speakers, and wearables, appear to have consumers gloss over the fact that the devices can collect and transmit their data consistently and possibly inadvertently.[104] Moreover, some of these devices now default to automatically opting users into data collection, thus requiring a deliberate opt-out if you wish to prevent your data from being collected. This differs from previous settings where users would opt into such a choice.[105] While IoToys, which are children-targeted IoT devices, are governed by the Rule, normal IoT devices targeting the general audience are not, even if they are in the homes with children, thus enabling the operators to collect, retain, and potentially sell data from adults

---

[98] *See* Federal Trade Commission, *supra* note 62.

[99] *See About*, COCOMELON, https://cocomelon.com/pages/about (last visited Apr. 24, 2024).

[100] *See* Todd Spangler, *What You Need to Know About YouTube's New COPPA Child-Directed Content Rules*, VARIETY (Jan. 3, 2020), https://variety.com/2020/digital/news/ftc-rules-child-directed-content-youtube-1203454167/ ("even attorneys who have worked in the area for years say it's not a clear-cut process").

[101] *See* Beemsterboer, *supra* note 36, at 71.

[102] *See* Beemsterboer, *supra* note 36, at 70.

[103] *See supra* text accompanying note 85.

[104] *See generally Internet of Things and Privacy – Issues and Challenges*, OVIC, https://ovic.vic.gov.au/privacy/resources-for-organisations/internet-of-things-and-privacy-issues-and-challenges/ (last visited Apr. 24, 2024).

[105] *See* Eldar Haber, *The Internet of Children: Protecting Children's Privacy in a Hyper-Connected World*, 2020 U. ILL. L. REV. 1209, 1215 (2020) (describing always-on IoT devices and their datamining-by-default characteristic).

and children.[106] Since non-child-directed IoT devices do not fall within the scope of COPPA, this leaves a gap in the consensual collection of children's data.

Moreover, since it is less costly and cumbersome for a company to adjust their practices to comply with COPPA's obligations, the child-directed standard produces a loophole that creates incentives operators to assert that they are not child-directed or that they are not aware that they are collecting data from children so as to avoid compliance.[107] Though the operator may be placing themselves at risk by giving into the incentive, many companies find it worthwhile considering that 1) individuals lack a private right to action against the operator under COPPA and 2) to date, the FTC has only brought forth approximately forty enforcement actions since the Rule went into effect, creating an assumption that the likelihood of persecution is arguably nominal.[108]

Ultimately, the child-directed standard loophole endangers children since this would mean operators of these type of sites or services would not have to comply with the Rule's obligations. This would include circumventing data retention and deletion obligations as well as the need to establish reasonable standards for safeguarding the personal data gathered from children, which in turn exposes them to risks of data breach and identity fraud.[109]

ii. Age Falsification

A core component of the Rule's application is that it governs data collected from children aged 12 and under.[110] Since this heavily impacts the earning capacity of an operator in comparison to another operator who did not have to comply with the COPPA Rule, many companies serving general audiences elect to ban children from the application or site altogether to circumvent COPPA Rule compliance.[111] One of the mechanisms used by operators to collect user data and restrict children's access is an age assurance process, though not required by the Rule itself.[112] Despite incorporating an age assurance method like age-gating[113] to prohibit children 12 and under, these systems often do not stop underage children from creating fake profiles or profiles with a false age to access general audience sites that are age-

[106] *See id.* at 1219, 1229.
[107] *See* Dercem Kaya, *Ignoring COPPA: An Industry Standard*, SETON HALL UNIV. (2023).
[108] *See id.*
[109] *See id.*
[110] *See* 16 C.F.R. §312.2.
[111] *See* Federal Trade Commission, *supra* note 62 (noting that banning children under 13 is permissible under COPPA for sites tailored to general audiences).
[112] *See* Scott B. Brennen & Matt Perault, *Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?* CTR. FOR GROWTH & OPPORTUNITY UTAH STATE UNIV. 11 (June 2023), *available at* https://www.thecgo.org/wp-content/uploads/2023/06/Age-Assurance_02.pdf.
[113] *See Age Verification vs. Age Gating: How to Protect Minors Online*, INCODE (Dec. 12, 2022), https://incode.com/blog/age-verification-age-gating/.

restricted.[114] Thus, COPPA's effectiveness becomes undermined as children who successfully bypass the age verification through false pretenses are no longer protected from the collection of their personal information.

There is a supplemental method, known as algorithmic estimation, that operators may implement as an age assurance process to attempt to ensure the age was not fabricated for the account's creation.[115] This is a practice popular among social media platforms like Facebook who, under COPPA's "internal operations" exception, can use an algorithm to track alleged minor users' data to examine their pattern of behavior to determine their probable age.[116] However, the very nature of the practice is not only "creepy", as stated by Representative Carter, but also anti-privacy as it is inconspicuously spying on a user's conduct, and that user can likely be a child whom COPPA aims to protect in the first place.[117]

A less invasive practice would be to use age-estimation technology instead, as it 1) does not retain any information because the data collected is instantly deleted and 2) it can be used without being linked to a particular identity or personal information, avoiding the classification of personal data under COPPA's current state altogether.[118] Despite capturing a live facial image to complete the age estimation process, this tool is more privacy protective and less invasive than facial recognition technology or other age assurance tools available because its only output is the estimate age of a *non-identifiable* person.[119] Although the FTC does not prohibit using this practice, the agency refuses to extend its application as a new form of parental consent under COPPA, despite its potential effectiveness of remedying the age falsification issue or even consent falsification issue since children can technically fabricate parental consent by affirming permission themselves through other COPPA suggested or

---

[114] *See* Kiara Ortiz, *Underage Social Media Usage and COPPA*, AM. U. J. GENDER & SOC. POL'Y L., https://jgspl.org/underage-social-media-usage-and-coppa/ (last visited Apr. 24, 2024)

[115] *See generally Unpacking Age Assurance: Technologies and Tradeoffs*, FUTURE OF PRIV. F., https://fpf.org/wp-content/uploads/2023/06/FPF_Age-Assurance_final_6.23.pdf (last visited Apr. 29, 2024); *see also* Pavni Diwanji*, How Do We Know Someone Is Old Enough to Use Our Apps?*, FACEBOOK (July 27, 2021) https://about.fb.com/news/2021/07/age-verification/.

[116] *See* Brennen, *supra* note 112, at 4.

[117] *See* Brennen, *supra* note 112, at 5.

[118]*See* Lorna Cropper, *Age Assurance: A Modern Coming of Age Approach to Ensure the Safety of Children Online and an Age Appropriate Experience*, FIELDFISHER (Jan. 12, 2024), https://www.fieldfisher.com/en/insights/age-assurance-a-modern-coming-of-age-approach-to-ensure-the-saftey-of-children-online; *see also* 16 C.F.R. § 312.2.

[119] *See* Stacy Feuer, *How Facial Age-Estimation Tech Can Help Protect Children's Privacy for COPPA and Beyond*, IAPP (July 20, 2023), https://iapp.org/news/a/how-facial-age-estimation-technology-can-help-protect-childrens-privacy-for-coppa-and-beyond (emphasizing that in present day there is no existing child age assurance method that is not privacy invasive).

proposed methods consequently leaving kids exposed to online harms without the protections of COPPA in place.[120]

iii. Challenges with Meaningful Verifiable Parental Consent and Effective Notice

As discussed in Part II, a core obligation of an operator of a website or online service under the COPPA Rule includes the need for verifiable parental consent.[121] However, the efficacy of the consent is undermined when it is not meaningfully provided.[122] The evolving digital landscape in 2024 starkly contrasts that of 1998 when the Act was enacted and when consent was first demanded for collecting children's data.[123] In the early years of when the Act took effect, requests for parental consent were minimal and thus feasible for operators to attain because although children's online presence increased, it had yet to reach the level of presence they hold today.[124] For example, accessibility to the internet used to be heavily dependent on the access to a home computer, and often one shared with other family members, or a school computer, both of which had limited and frequency of its use.[125] Ultimately a true presence of being offline was achievable when stepping away from the computer; however, the same cannot be said today.[126]

Smart devices, many equipped with a myriad of capabilities and constant access to the online world, have become common place amongst children and adults–largely distinct from its previous categorization as luxury items during their earlier stages, which typically members of higher socio-economic levels could likely afford.[127] This difference depicts the drastic shift in

---

[120] *See* Press Release, Fed. Trade Comm'n, FTC Denies Application for New Parental Consent Mechanism Under COPPA (Mar. 29, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-denies-application-new-parental-consent-mechanism-under-coppa

[121] *See* 16 C.F.R. § 312.5 (a).

[122] *See* Daniel J. Solove, *Murky Consent: An Approach To The Fictions Of Consent In Privacy Law*, 104 B.U. L. REV. 593, 614 (2024).

[123] *Compare supra* notes 1-9 and accompanying text *with* Sara Uusimaki & Rebecca Da Cruz Tiderman, *The First Child-Generation on the Internet: A Qualitative Study on Childhood Experiences of Internet Use in the Early 2000s*, LINKOPING UNIV. 34 (2021) available at https://www.diva-portal.org/smash/get/diva2:1597355/FULLTEXT01.pdf

[124] *See Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, ELECTRONIC PRIV. INFO. CTR. at 177 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.

[125] *See* Uusimaki *supra* note 123, at 25.

[126] *See* Uusimaki *supra* note 123, at 34 (describing children in the early 2000s to have experienced a childhood with an offline mode and where the internet did not play an important part of their lives, nor did it replace or reduce social interactions with peers in person).

[127] *See* Uusimaki *supra* note 123, at 25 ("When the use of the internet became available on phones, the groups argued that they very rarely used the 'i' button for internet since it was 'very expensive' and slow"); *see also Home Computers and Internet Use in the United States: August 2000,* U.S. CENSUS BUREAU

providing meaningful consent as parents may find it more cumbersome or inconvenient to carefully review the extensive privacy policies of every single app, online game, and website their child uses.[128] As a result, it can lead to either parental consent that is not meaningful or no consent at all.

Consequently, even if a parent refrains from providing consent, children have successfully circumvented the requirement by other means such as age falsification or submitting consent from a non-parent or custodian since none of the current or additional suggested methods for obtaining verifiable parental consent actually confirm parental relationship.[129] Moreover, other prominent parental consent methods, like credit card verification[130], that the FTC finds sufficient for compliance, may not be as effective as it once was.[131] A 2019 survey noted that seventeen percent of parents reported that their kids, some as young as 4 years of age, had credit cards and thus may bypass the parental consent requirement when using their own credit card despite being a minor that COPPA intends to protect.[132]

Another challenge with obtaining meaningful consent arises when the original notice, though technically COPPA-compliant, may still be insufficient for a parent to be properly informed and provide consent to. Operators who need to comply with the Rule's notice requirement must directly express their privacy practices to parents when seeking to collect a child under 13's data.[133] Such notice must sufficiently detail the operator's collection, use and disclosure of children users' personal data; however, the notice requirement does not specify a particular manner to inform parents and users about its privacy practices and policies aside from being "clear and understandable."[134] The lack of clear guidelines on what constitutes "clear and understandable" notice simplifies compliance for operators but fails to ensure the user, or their parent's, genuine comprehension of the notice before any data collection, use, or

---

2 (Sept. 2001), https://www.census.gov/content/dam/Census/library/publications/2001/demo/p23-207.pdf

[128] *See supra* note 124, at 177; *see also* Luiz Montezuma & Tara Taubman-Bassirian, *How to Avoid Consent Fatigue*, IAPP (Jan. 18, 2019), https://iapp.org/news/a/how-to-avoid-consent-fatigue/ (emphasizing that digital privacy policies for platforms that parents are expected to review to provide consent typically range between 2500 and 4500 words which can result in consent fatigue).

[129] *See The State of Play: Is Verifiable Parental Consent Fit For Purpose?*, FUTURE OF PRIV. F. 11 (June 2023), https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf.

[130] *See* 16 C.F.R. § 312.5 (b)(2).

[131] *See supra* note 129, at 11 ("A parent even described [Verifiable Parental Consent] as privacy theater, because their children can get around [Verifiable Parental Consent] 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").

[132] *See id.*

[133] *See* 16 C.F.R. § 312.4 (b).

[134] *See* 16 C.F.R. § 312.4(b)-(c).

disclosure occurs.[135] What is understandable to some individuals might not be to others due to differences in education level, language proficiency, or background knowledge necessary to make an informed decision to consent to a privacy practice.[136] Thus if a parent who has inaccurate understandings and limited knowledge of digital privacy practices provides consent, such consent should be deemed meaningless as they did not fully grasp what they were agreeing to.[137]

The issue surrounding ineffective notice is only exacerbated when language barriers are present as non-English speakers' access to linguistically appropriate resources are either limited or absent.[138] Such constraint causes non-English speakers to be more vulnerable to cybercrime and in turn their children more susceptible to online harms when the parents are unable to meaningfully consent to practices that may place their vulnerable data at risk.[139]

As the COPPA Rule stands today, an operator's notice and consent obligations regarding their privacy practices may be easily checked off by obtaining a single consent from a parent-appearing adult.[140] The FTC's suggested modifications to the Rule attempts to strengthen the effectiveness of consent by de-bundling parental consent through requiring operators to obtain separate additional consent if they want to 1) disclose a child's collected data to third parties and 2) use the data to maximize the child user's engagement with the platform or site.[141]

---

[135] *See* Geoffrey A. Fowler, *I Tried to Read All My App Privacy Policies. It was 1 Million Words*, WASH. POST (May 31, 2022), https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/ (stating that operators' current disclosures of privacy practices create a flawed assumption that the info within them "will be digestible, intelligible, usable for people").

[136] *See* Irene Lee, *It's Not You; Privacy Policies Are Difficult to Read*, COMMON SENSE MEDIA (July 17, 2018), https://www.commonsense.org/education/articles/its-not-you-privacy-policies-are-difficult-to-read (noting that the average American reading level is lower than the level certain privacy policies are writing in to understand); Jocelyn Mackie, Privacy Policies and Language Choices, TERMS FEED, https://www.termsfeed.com/blog/privacy-policy-language/ (last visited June 2, 2024) (noting that most privacy practices are disclosed in English, and though it is the dominant language in the U.S. it does not account for American diversity and thus fails to consider the level of proficiency of its users and other common languages that its users may be able to comprehend better in); Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html ("Even policies that are shorter and easier to read can be impenetrable, given the amount of background knowledge required to understand how things like cookies and IP addresses play a role in data collection").

[137] *See* Solove, *supra* note 122, at 614 ("Privacy consent is not meaningful if it is not informed. If people lack an understanding of what they are agreeing to, they are not really consenting; they are just making decisions in the dark.")

[138] See *Research Reveals Language Barriers Limit Effectiveness of Cybersecurity Resources*, SCIENCEDAILY (Apr. 1, 2024), https://www.sciencedaily.com/releases/2024/04/240401142443.htm.

[139] *See id.*

[140] *See* 16 C.F.R. § 312.5 (a)(2).

[141] *See* 89 Fed. Reg. 2034 at 2045, 2049, 2051.

However, as discussed in this section, even if consent is deemed lawful under current or revised COPPA standards, it does not necessarily mean it was meaningfully provided with the child's best interests or a clear understanding of the consent's true implications. As a result, children remain exposed to the online harms and risks despite the Rule's notice requirement. Although the FTC aims for heightened transparency with parents, the expansion of more layers of parental consent overlooks consent fatigue, parents' unfamiliarity with privacy concepts, and growing ways children strategize to circumvent the Rule's requirement.

Part IV. Conclusion

COPPA has made strides in addressing the collection of children's personal data in an increasingly digitized society, and its proposed amendments appear to attempt to strengthen and modernize the Act with updated definitions and more stringent requirements by operators in terms of data collection limitations, retention, and security.[142] However, COPPA's effectiveness is limited by many factors that leave a gap in being able to suitably protect the interests of protecting children online. Aside from its flawed child-directed standard, lack of a solution for age falsification occurrences, and absent standard for effective notice and meaningful consent, COPPA also fails to address other legitimate harms kids face online (i.e., cyberbullying, access to and the amplification of harmful content, and communication from child predators), because the legislation focuses more on what a child shares rather than what they are exposed to. These gaps, combined with the challenging enforcement process[143], make the COPPA legislation and Rule, and its proposed modifications, presently unfit to protect children online fully and adequately.

[142] *See* 89 Fed. Reg. 2034 at 2040, 2044-45, 2061-62.

[143] *See* Irwin Reyes, et al., *Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale*, PROCEEDINGS ON PRIV. ENHANCING TECH. 1 (2018) ("enforcement is a painstaking process, as investigations generally rely on manual examination of programs and websites to observe violations").