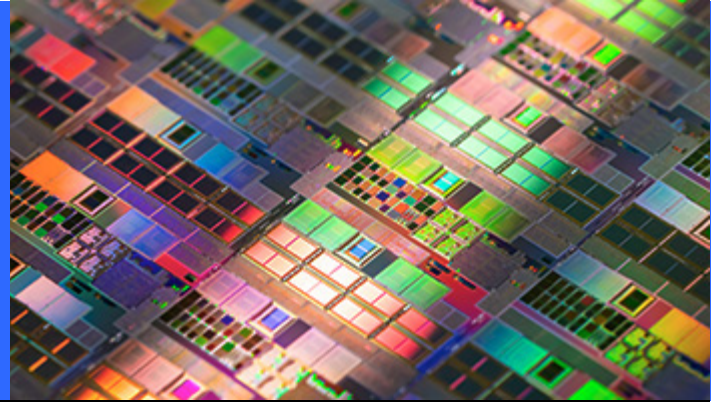


GIBSON DUNN



Privacy, Cybersecurity & Data Innovation Update

January 28, 2025

FTC Updates to the COPPA Rule Impose New Compliance Obligations for Online Services That Collect Data from Children

This update summarizes key amendments to the COPPA Rule and related FTC Commissioner statements, as well as key proposals that the FTC declined to adopt, and it positions these developments in the broader legal landscape related to children's privacy and safety online.

On January 16, 2025, the Federal Trade Commission (FTC or Commission) voted 5-0 to approve long-awaited updates to the Children's Online Privacy Protection Rule (COPPA Rule or Rule),^[1] which was last updated over a decade ago, in 2013. The FTC had proposed amendments to the COPPA Rule in a Notice of Proposed Rulemaking (NPRM) in January 2024,^[2] following a 2019 request for comment^[3] on the effectiveness of the 2013 amendments. While the updated COPPA Rule does not include some of the more sweeping amendments proposed, it imposes significant new obligations regarding the collection, use, and disclosure of personal information from children under 13. Many of these updates effectively codify positions that the Commission has taken in COPPA enforcement actions under the prior COPPA Rule.

As described in detail below, key updates to the COPPA Rule include:

- **Requiring separate parental consent for data sharing with third parties for targeted ads and other non-integral purposes.** Requiring covered operators to obtain separate verifiable parental consent to disclose children's personal information to third-party companies for targeted advertising or other purposes that are not "integral" to the operator's websites or online services;

- **Requiring data minimization and a data retention policy.** Limiting the retention of children’s personal information to only the time reasonably necessary to fulfill the specific purpose for which it was collected, prohibiting the retention of children’s personal information indefinitely, and requiring adoption of a written data retention policy;
- **Clarifying definitions of child-directed and mixed audience services.** Clarifying which online services may be covered by the Rule by amending the definition of “website or online service directed to children” to include a non-exhaustive exemplary list of evidence the FTC may consider in analyzing audience composition and intended audience, and adding a new, standalone definition of “mixed audience website or online service”;
- **Expanding the definition of covered information.** Expanding the definition of “personal information” to include biometric identifiers and government-issued identifiers beyond Social Security numbers;
- **Expanding parental notice requirements.** Clarifying and expanding the scope of disclosures required in direct notices and online privacy notices, including: the identities and categories of any third parties with which the operator shares children’s personal information; how specifically the operator uses persistent identifiers to support its internal operations and what measures are in place to avoid using persistent identifiers for unauthorized purposes; and when an operator collects an audio file of a child’s voice pursuant to the audio file exception, a description of how the operator uses audio files and a disclosure that such files are deleted immediately after responding to the request for which they were collected;
- **Enumerating additional methods to obtain verifiable parental consent.** Enumerating additional methods that satisfy the requirement to obtain verifiable parental consent before collecting personal information from children or using or disclosing such information, including using a text message coupled with an additional step, such as a confirmatory text message following receipt of consent (the “text plus” method);
- **Enhancing data security requirements.** Clarifying the reasonable security measures required to protect personal information from children, which include, at a minimum, establishing a written data security program; and
- **Increasing oversight and transparency of Safe Harbor programs.** Enhancing oversight of, and transparency regarding, Safe Harbor programs, including by requiring that such programs disclose their membership lists and report additional information to the FTC.

Significant proposals the FTC dropped include changes that would have codified requirements for educational technology companies operating in a school environment, and those that would have prohibited the use of push notifications and similar engagement techniques without separate parental consent.

The amended COPPA Rule will become effective 60 days after its publication in the federal register, and covered operators will have until one year after the publication date to comply, except with respect to certain provisions regarding Safe Harbor programs.^[4] We note, however, that businesses should continue to monitor updates regarding the publication of the updated Rule, given the possibility for delay or withdrawal under the Trump administration or the new FTC leadership.^[5] Although the FTC’s vote approving the final Rule was unanimous, then-incoming Chair Andrew Ferguson issued a strongly worded concurring statement identifying three “serious

problems” with the amendments that he ascribed to “the outgoing administration’s irresponsible rush to issue last-minute rules two months after the American people voted to evict them from office,” and calling for “[t]he Commission under President Trump [to] address these issues and fix the mess that the outgoing majority leaves in its wake.”^[6]

Despite some uncertainties, companies that knowingly provide services to children under 13 or that have offerings that could be considered attractive to children should revisit their existing compliance strategies to mitigate the substantial risk of liability for non-compliance with the updated COPPA Rule, which include civil penalties up to \$53,088 per violation for 2025.^[7] Given historical and continued bipartisan consensus that the privacy and safety of children online is a priority in light of developing technologies,^[8] we expect rigorous oversight and enforcement by the FTC, including under the new administration.

Gibson Dunn has extensive experience advising and defending multinational companies on COPPA and youth-related strategies, including regulatory investigations and engagement strategies, product counseling, and litigation matters. We stand ready to advise companies on compliance with the updated COPPA Rule, and on federal, state, and international youth privacy and safety laws more broadly.

A. COPPA Background

Congress enacted COPPA in 1998, and the FTC’s COPPA Rule implementing COPPA first went into effect in 2000 and was last amended in 2013.

Importantly, COPPA applies only to online services that are directed to children under 13 or that are collecting, using, or sharing personal information of a user with actual knowledge that a particular user is under 13. More specifically, COPPA applies to (1) “operators of commercial websites and online services” that are “**directed to children under 13** that collect, use, or disclose personal information from children”; (2) “operators of general audience websites or online services **with actual knowledge** that they are collecting, using, or disclosing personal information **from children under 13**”; and (3) to websites or online services that have **actual knowledge that they are collecting personal information directly from users of another website or online service directed to children**.”^[9] COPPA’s primary goal is to give parents control over their children’s personal information and how that information is collected and processed.^[10]

The COPPA Rule imposes several requirements on covered operators of websites and online services, including requirements to provide clear direct notice to parents and to obtain verifiable parental consent before collecting personal information from children or using or disclosing such information.^[11] The Rule also confers other rights on parents, including the right to request that covered operators delete their children’s personal information,^[12] and it imposes several additional obligations on covered operators, including for example with respect to security measures^[13] and data retention.^[14]

B. Key Amendments to the COPPA Rule

The following sections detail key amendments to the COPPA Rule.

a. Companies Covered By the COPPA Rule

The amended COPPA Rule “clarifies” the definition of “website or online service directed to children” by adding to the non-exhaustive exemplary list of evidence the FTC may consider in analyzing audience composition and intended audience “consideration of marketing or promotional materials or plans, representations to consumers or to third parties, reviews by users or third parties, and the age of users on similar websites or services.”^[15] The latter example may be particularly challenging for companies to address since it relies on extraneous information outside a service’s control (and for the same reason, would not appear to be probative of a company’s intent to direct its service to children).

The amended Rule also includes a new, standalone definition of “mixed audience website or online service,” which the FTC confirmed is not intended to expand the scope of child-directed websites and online services, and does not change which websites or online services are directed to children.^[16] The 2013 COPPA amendments and the FTC’s subsequent COPPA FAQ guidance introduced the concept of “mixed audience” websites and online services as a subcategory within the definition of “website or online service directed to children,” but did not define this term.^[17] Under the updated Rule, “mixed audience” websites and online services are defined as those directed to children but that do not target children as their *primary* audience, and that do not collect personal information from *any* visitor other than to assess whether a visitor is a child.^[18] Unlike other child-directed websites and online services, mixed audience websites and online services are permitted to collect information from visitors in a neutral manner in order to determine whether a visitor is a child.^[19] Once a mixed audience website or online service determines that a visitor is 13 or over, it may collect personal information from the visitor without obtaining verifiable parental consent. The mixed audience website or online service may not deny access to visitors who are under 13, but may require verifiable parental consent or offer an experience that does not collect their personal information.

b. Expanded Definition of “Personal Information”

As amended, “personal information” under COPPA now explicitly includes (1) biometric identifiers, defined as an “identifier that can be used for the automated or semi-automated recognition of an individual, such as fingerprints; handprints; retina patterns; iris patterns; genetic data, including a DNA sequence; voiceprints; gait patterns; facial templates; or faceprints”; and (2) government-issued identifiers beyond Social Security numbers, including state ID cards, birth certificates, and passport numbers.^[20]

c. Direct Notice & Verifiable Parental Consent

Direct Notice. The amended COPPA Rule clarifies and expands what companies must include in their direct notice disclosures to parents prior to collecting from and using their children’s personal information. Specifically, companies should ensure their direct notice disclosures:

- Include information on “how the operator intends to use [a child’s personal] information;”^[21]

- Disclose the identity or categories of third parties the company shares personal information with, the purposes for sharing with those third parties, and that a parent can consent to the collection of and use of the child’s information, without consenting to its disclosure;[\[22\]](#) and
- Are provided in every instance in which a company seeks parental consent.[\[23\]](#)

Online Privacy Notice. Companies must also post clear, prominent links to online notices of their information practices regarding children.[\[24\]](#) As with the direct notices, the COPPA Rule amendments expand what must be included in the online notices to include:

- The identities and categories of any third parties to which the operator discloses personal information and the purpose for such disclosure;[\[25\]](#)
- The specific internal operations for which the operator uses persistent identifiers, and the policies or practices the operator has in place to avoid using persistent identifiers for unauthorized purposes;[\[26\]](#)
- When an operator collects an audio file of a child’s voice pursuant to the audio file exception (discussed below), a description of how the operator uses the audio files, and that such files are deleted immediately after responding to the request for which they were collected;[\[27\]](#) and
- The operator’s data retention policies for personal information collected from children.[\[28\]](#)

Verifiable Parental Consent. The amendments enumerate additional methods that satisfy the requirement to obtain verifiable parental consent before collecting personal information from children or using or disclosing a child’s personal information,[\[29\]](#) including:

- Processing any transaction requiring a parent to use a credit card, debit card, or other online payment system, provided that the transaction “provides notification of each discrete transaction to the primary account holder”—not just those transactions which include a monetary fee, as previously required;[\[30\]](#)
- Using a knowledge-based authentication process (i.e., questions of sufficient number and difficulty that a child could not reasonably ascertain the answers);[\[31\]](#)
- Matching an image of a face to a verified photo identification, such as a driver’s license (with the image and photo ID being promptly deleted thereafter);[\[32\]](#) and
- Using a “text plus” method that may be used when an operator does not disclose personal information from children to a third party, where (similar to the “email plus” method already available) subject to certain disclosure and confirmation requirements, a company uses a text message to obtain consent.[\[33\]](#)

The amendments also modify and expand exceptions to the COPPA Rule’s verifiable parental consent requirement. Of particular note is an exception for when a company collects an audio file containing a child’s voice as a replacement for written words, and no other personal information, and uses the audio file only to respond to a child’s specific request such as to execute a search or implement a verbal instruction, and the file is deleted immediately thereafter.[\[34\]](#) This

exception is meant to provide flexibility for companies who rely on voice-assist technology.^[35] Such a practice must be disclosed in an online notice.^[36]

d. Separate Consent for Information Disclosures to Third Parties for Targeted Advertising and Other Non-Integral Purposes

The amended COPPA Rule requires separate parental consent for the disclosure of a child's personal information to a third party for targeted advertising or other uses, "unless such disclosure is integral to the website or online service" such as disclosures necessary to provide the product or service.^[37] Covered operators also cannot condition access to their website or service on obtaining such consent.^[38] This amendment, in particular, will have significant implications for online services that may be perceived to be attractive to children that leverage third-party advertising technologies in their services.

e. Data Retention and Deletion

The COPPA Rule includes directives regarding the retention and deletion of personal information from children, including that a covered operator may retain such information "for only as long as is reasonably necessary to fulfill the purpose(s) for which the information was collected."^[39] Notably, the amendments prohibit companies from retaining children's personal information indefinitely.^[40] As discussed below, there is disagreement within the Commission surrounding this requirement, including as to what "indefinitely" means in this context.

The amendments further instruct that companies must establish a written data retention policy that specifies the purposes for which a child's information is collected, the business need for retaining the information, and the timeframe for deleting it.^[41] These policies must now be provided in online notices, as described above.^[42]

f. Confidentiality, Security, and Integrity of Personal Information

COPPA requires covered operators to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children,"^[43] and the amendments clarify the steps covered operators can take to comply with this "reasonable procedures" standard.

At a minimum, a covered operator's safeguards must be "appropriate to the sensitivity of the personal information collected from children and the operator's size, complexity, and nature and scope of activities."^[44] To comply, an operator must, among other requirements, designate employees to manage the program, assess the program at least annually, and implement necessary safeguards based on those assessments.^[45] Notably, these requirements generally mirror the requirements contained in Commission orders requiring the implementation of a comprehensive information security program.

Additionally, covered operators that disclose children's personal information to third parties must "take reasonable steps to determine that such entities are capable of maintaining the

confidentiality, security, and integrity of the information” and obtain written assurances from the third parties that they will do so.[\[46\]](#)

g. Safe Harbor Programs

Under the COPPA Rule, the Commission may approve Safe Harbor programs—i.e., self-regulatory guidelines submitted by industry groups which implement the same or greater protections for children as in COPPA. The FTC amended the COPPA Rule to “enhance oversight of, and transparency regarding” these Safe Harbor programs by requiring they conduct annual independent assessments of their members’ compliance, including the members’ data privacy and security practices, disclose their membership lists, and maintain and submit to the FTC records of complaints about, and disciplinary actions against, the program’s members.[\[47\]](#) Existing COPPA Safe Harbor programs must submit proposed modifications within 6 months of the publication of the amended COPPA Rule in the federal register.[\[48\]](#)

C. Key Proposed Changes Not Adopted in Amended COPPA Rule

The amended COPPA Rule does not include certain amendments that the FTC proposed in its January 2024 NPRM, which were the subject of nearly 300 public comments, and which would have imposed significant compliance obligations relating to push notifications or engagement techniques and on educational technology companies.

a. Push Notifications/Engagement Techniques

The COPPA Rule includes an exception to obtaining verifiable parental consent “[w]here the purpose of collecting a child’s and a parent’s online contact information is to respond directly more than once to the child’s specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child.”[\[49\]](#) The NPRM’s proposal sought to prohibit companies from using this exception to “encourage or prompt use of a website or online service,” in order to address children’s overuse of online services due to engagement-enhancing techniques such as push notifications, in-game notices, or website pop-ups.[\[50\]](#)

Though the FTC stated it remains “deeply concerned” about push notifications and other techniques designed to prolong a child’s time spent online, the Commission was persuaded by concerns regarding the inconsistency between the proposed language and the COPPA statute, as well as First Amendment concerns regarding the breadth of the restriction, and thus did not amend COPPA to include this proposal.[\[51\]](#)

b. Educational Technology Requirements

The FTC also excluded several requirements proposed in the NPRM that would have been applicable to educational technology (ed tech) companies. The NPRM proposed including new definitions of “school” and “school-authorized education purpose,” as well as new provisions governing the collection of information from children in schools, and codifying the FTC’s existing guidance that allows ed tech companies to obtain consent from schools, rather than parents, to collect personal information from students for educational purposes.[\[52\]](#) The FTC chose not to

adopt these proposed amendments “[t]o avoid making amendments to the COPPA Rule that may conflict with potential amendments to [the Department of Education’s Family Education Rights and Privacy Act] regulations.”^[53] However, the Commission specifically noted that they “will continue to enforce COPPA in the ed tech context consistent with its existing guidance.”^[54]

c. Other Exclusions

The final COPPA Rule also excluded other proposed amendments, including one that would have modified the exception to the parental consent requirement when companies collect persistent identifiers (and no other personal information) to provide support for the internal operations of the website or online service, such as for contextual advertising or personalization.^[55] The FTC also declined to expand the definition of personal information to include avatars generated from a child’s image. And the FTC declined to amend the Rule to require companies disclose specifically the types of personal information collected, as well as details on how that personal information in particular is used, agreeing with commenters that “that level of detail could be superfluous.”^[56]

D. An Uncertain Future

While the Commission vote approving the final COPPA Rule was unanimous, the future of the Rule remains uncertain. Former-Chair Lina Khan and then-incoming Chair Andrew Ferguson issued separate concurring statements about the Rule, and Commissioners Alvaro Bedoya and Rebecca Slaughter issued a joint concurring statement.

Former-Chair Khan’s concurring statement emphasized that these updates were long-awaited, especially given the dramatic rise in children’s smartphone and social media use since the Rule was last amended.^[57] She characterized the updates as “complementing” the FTC’s enforcement efforts, potentially “boost[ing]” enforcement efforts by state attorneys general,^[58] and welcoming Congress’ efforts to legislate in this area.^[59]

In his concurring statement, Commissioner Ferguson characterized the amendments as “the culmination of a bipartisan effort initiated when President Trump was last in office” and voted to issue the final Rule because the amendments “contain several measures improving data privacy and security protections for children”—but he identified “three major problems” with the amendments.^[60] He argued against the requirement that all new third-party data sharing should require a separate consent from parents, and against the prohibition on indefinite retention of data.^[61] He also advocated for an exception for collecting children’s information for the limited purpose of age verification.^[62] He was blunt in his critique that “these issues are the result of the Biden-Harris FTC’s frantic rush to finalize rules on their way out the door” and foreshadowed an intent to revisit the amendments in stating that “[t]he Commission under President Trump should address these issues and fix the mess that the outgoing majority leaves in its wake.”^[63]

In their joint concurring statement, Commissioners Bedoya and Slaughter disagreed with Commissioner Ferguson regarding the prohibition against indefinite data retention, arguing such a requirement is necessary for companies that take the position that it is “reasonably necessary” to keep personal information indefinitely.^[64]

E. FTC Enforcement Risks

Notwithstanding disagreement among Commissioners on certain details of the COPPA Rule amendments, companies can expect the FTC to continue to vigorously scrutinize data practices involving children. The FTC historically has focused its enforcement efforts on potential harms to children online, even where business practices are not subject to COPPA, under Section 5 of the FTC Act (Section 5). The FTC has also enforced against companies for violations of both COPPA and Section 5, often resulting in steep monetary penalties.

For example, in 2022, the FTC secured an agreement with Epic Games, Inc. (the creator of the video game Fortnite) to pay a record-breaking \$520 million to settle allegations that Epic violated both COPPA and Section 5.^[65] More recently, on January 17, 2025, another video game developer agreed to pay \$20 million and make various product and other changes to settle FTC allegations that its practices related to loot boxes violated COPPA and Section 5^[66]—although notably, Commissioners Ferguson and Holyoak dissented on three of four counts brought under Section 5.^[67]

Further, some in Congress continue to push for federal legislation, including the Children and Teens' Online Privacy Protection Act (COPPA 2.0),^[68] which would extend the application of COPPA to youth under 16, ban targeted advertising to minors, and place more responsibility on companies to ensure children's online safety. Senator Markey, the author of the bill and an author of COPPA, noted in a statement applauding the updated COPPA Rule that "Congress must still pass [COPPA 2.0] to extend these protections to teenagers, block targeted advertising to kids and teens, and give young people an eraser button to delete their personal information."^[69]

F. Additional Youth Privacy and Safety Developments and Enforcement Risks

These federal changes reflect a broader trend toward enhancing privacy and safety protections for children. Various U.S. states and jurisdictions worldwide are also increasingly focused on children and youth, implementing laws and taking actions under existing laws against companies with a substantial youth user base.

a. State Youth Laws and Enforcement

State lawmakers have made clear that protecting children's online privacy and safety is a top priority, including by amending omnibus state privacy laws to include youth-specific provisions, enacting broader "age-appropriate design" laws applicable to any online service "reasonably likely to be accessed by children," and enacting social media-specific laws requiring enhanced protections and often parental consent to children under 18 who use social media services. Many of these laws have been challenged successfully on First Amendment and other grounds, but other laws are spawning aggressive enforcement.

Among these state laws are Texas' Securing Children Online Through Parental Empowerment Act (SCOPE Act), the majority of which came into effect on September 1, 2024,^[70] and the California Protecting Our Kids from Social Media Addiction Act, only parts of which are currently set to take effect on March 6, 2025.^[71] The Texas SCOPE Act takes a restrictive approach to collection and use of children's data, while the California law is the first aiming to protect children

from social media “addiction.” Both laws are shaping the youth legal landscape, setting templates for other states to follow, but the California law is currently being challenged, and we anticipate continued constitutional challenges asserting that other such laws restrict expressive speech. Even so, regulators are not slowing down their efforts pending these challenges.

For example, in October 2024—just one month after the Texas SCOPE Act came into effect—the Texas Attorney General’s Office announced its first action under the law seeking up to \$10,000 per violation.^[72] The Texas Attorney General’s Office also recently announced the launch of investigations into over a dozen companies in connection with the SCOPE Act and Texas’ omnibus privacy law that includes youth-specific provisions.^[73]

Enforcement authorities also have sought to hold companies liable for alleged online harms to children under general state consumer protection laws prohibiting unfair and deceptive practices, which are not subject to the same constitutional concerns. Additionally, parents and families of children, as well as school districts, have similarly leveraged general consumer protection and other laws to pursue claims against online companies relating to purported youth harms, resulting in extensive multidistrict and class action litigation in this area.

b. Global Focus on Youth Privacy and Safety

Global lawmakers and regulators are also focused on youth privacy and safety online. Omnibus privacy laws outside the U.S. do not accord special treatment to children’s data, but some contain some similar restrictions to COPPA, such as requiring parental consent to process children’s data (e.g., the European Union (EU)’s General Data Protection Regulation) or prohibiting online platforms from targeting ads to children under 18 (e.g., the EU’s Digital Services Act (DSA), a sweeping EU regulation). As in the U.S., there is a similar global trend towards more prescriptive and aggressive laws concerning youth online activity.

For example, under the DSA, in-scope platforms can be fined up to 6% of global annual turnover by the European Commission (EC), which is the primary enforcing authority, for failing to conduct required risk assessments considering the impact of new features and service on harm to minors, among other concerns. The EC has already requested information from, and in some instances launched investigations into several companies in connection with, the collection and use of minors’ data under the DSA.^[74] Similarly in the UK, Ofcom has been appointed to enforce the UK Online Safety Act (OSA) and has published drafts for consultation and finalized versions of its mandatory Codes of Practice. In addition, in recent years, many EU privacy regulators have been focused on enforcing against companies whose services can be accessed by children, and the UK Information Commissioner’s Office steadily continues to enforce its Children Code, also known as its Age Appropriate Design Code, which it published in 2020. And in APAC, Australia recently took steps to ban youth under the age of 16 from creating social media accounts—although implementing regulations have yet to be published.^[75]

These laws underscore the challenges global companies will face in restructuring their compliance plans within tight timeframes.

The privacy and safety of children online are top concerns for the FTC, other enforcement authorities, lawmakers, and families worldwide. To that end, companies that conduct business

online should take care to assess their legal obligations and practical risks under the amended COPPA Rule, as well as under youth-related laws across jurisdictions, given increased regulatory attention to child-directed services and features under an expanding landscape of child-focused regulation.

Again, Gibson Dunn has extensive experience advising multinational companies operating online services on a wide variety of regulatory and law enforcement investigation, enforcement, strategic counseling, litigation, and appellate matters relating to child and teen privacy and safety. We are closely monitoring developments within the youth legal landscape, and we are available to discuss these issues as applied to your particular situation.

[1] Press Release, Fed. Trade Comm'n, FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data (Jan. 16, 2025), <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data>; see also Fed. Trade Comm'n, Children's Online Privacy Protection Rule, Final Rule Amendments (Jan. 16, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/coppa_sbp_1.16_0.pdf.

[2] Children's Online Privacy Protection Rule, 89 Fed. Reg. 2034 (proposed Jan. 11, 2024) (to be codified at 16 C.F.R. pt. 312).

[3] Press Release, Fed. Trade Comm'n, FTC Seeks Comments on Children's Online Privacy Protection Act Rule (July 25, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-seeks-comments-childrens-online-privacy-protection-act-rule>.

[4] Children's Online Privacy Protection Rule, *supra* note 1, at 1.

[5] On January 20, 2025, President Trump issued an order imposing a regulatory freeze on all executive agencies. See White House, Regulatory Freeze Pending Review (Jan. 20, 2025), <https://www.whitehouse.gov/presidential-actions/2025/01/regulatory-freeze-pending-review/>. While the extent to which independent agencies like the FTC are subject to the order may be subject to litigation, the presidential memorandum signals skepticism regarding actions taken by such agencies in the final days of the Biden administration. The FTC may choose to take steps consistent with Section 2 of the memorandum, which would involve withdrawal of the final COPPA Rule for review by a Republican majority (which, if re-approved, would then be sent to the federal register for publication). Accordingly, the publication in the federal register and implementation of the COPPA Rule should be monitored, as it could be subject to other actions taken to delay or revoke it, such as through the Congressional Review Act. See 5 U.S.C. §§ 801 *et seq.*

[6] See Andrew N. Ferguson, Comm'r, Fed. Trade Comm'n, Concurring Statement of Commissioner Andrew N. Ferguson COPPA Rule Amendments Matter Number P195404 (Jan. 16, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/ferguson-coppa-concurrence-revised.pdf.

[7] See Adjustments to Civil Penalty Amounts, 90 Fed. Reg. 5580 (Jan. 17, 2025) (to be codified at 16 C.F.R. pt. 1). The FTC annually adjusts the civil penalty amount applicable to COPPA violations based on inflation, pursuant to the Federal Civil Penalties Inflation Adjustment Act

Improvements Act of 2015. See Press Release, Fed. Trade Comm'n, FTC Publishes Inflation-Adjusted Civil Penalty Amounts for 2024 (Jan. 11, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-publishes-inflation-adjusted-civil-penalty-amounts-2024?utm_source=govdelivery. Accordingly, civil penalty violation amounts will rise in future years.

[8] See, e.g., S.2073, Kids Online Safety and Privacy Act, 118th Cong. (as passed by Senate, July, 30, 2024).

[9] Fed. Trade Comm'n, Complying with COPPA: Frequently Asked Questions (Jan. 2024), <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>.

[10] *Id.*

[11] 16 C.F.R. §§ 312.4 - 312.5. All citations to the COPPA Rule are to the COPPA Rule as amended, unless otherwise stated.

[12] *Id.* at § 312.6.

[13] *Id.* at § 312.8.

[14] *Id.* at § 312.10.

[15] *Id.* at § 312.2.

[16] Children's Online Privacy Protection Rule, *supra* note 1, at 9-10.

[17] 16 C.F.R. § 312.2; Complying with COPPA: Frequently Asked Questions, *supra* note 10.

[18] Children's Online Privacy Protection Rule, *supra* note 1, at 8.

[19] *Id.* at 9.

[20] 16 C.F.R. § 312.2. Examples of biometric data include "fingerprints; handprints; retina patterns; iris patterns; genetic data, including a DNA sequence; voiceprints; gait patterns; facial templates; or faceprints."

[21] *Id.* at § 312.4(c)(1)(iii).

[22] *Id.* at § 312.4(c)(1)(iv).

[23] *Id.* at §§ 312.4(a) - (c)(1).

[24] *Id.* at § 312.4(d).

[25] *Id.* at § 312.4(d)(2).

[26] *Id.* at § 312.4(d)(3).

[27] *Id.* at § 312.4(d)(4).

[28] *Id.* at § 312.4(d)(2).

[29] *Id.* at § 312.5(a)(1).

[30] *Id.* at § 312.5(b)(2)(ii).

[31] *Id.* at § 312.5(b)(2)(vi)

[32] *Id.* at § 312.5(b)(2)(vii).

[33] *Id.* at § 312.5(b)(2)(ix). See also *id.* at § 312.2 (modifying the definition of “online contact information” to include a “mobile telephone number” in order to “give [companies] another way to initiate the process of seeking parental consent quickly and effectively.” Children’s Online Privacy Protection Rule, *supra* note 1, at 16).

[34] 16 C.F.R. § 312.5(c)(9).

[35] See, e.g., 106. Fed. Trade Comm’n, Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings (Oct. 20, 2017), https://www.ftc.gov/system/files/documents/public_statements/1266473/coppa_policy_statement_audiorecordings.pdf.

[36] 16 C.F.R. § 312.5(c)(9).

[37] *Id.* at § 312.5(a)(2); Children’s Online Privacy Protection Rule, *supra* note 1, at 106.

[38] 16 C.F.R. § 312.5(a)(2).

[39] *Id.* at § 312.10.

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.* at § 312.8(a).

[44] *Id.* at § 312.8(b).

[45] *Id.* at § 312.8(b)(1)-(3).

[46] *Id.* at § 312.8(c).

[47] Children’s Online Privacy Protection Rule, *supra* note 1, at 159. See generally 16 C.F.R. § 312.11.

[48] 16 C.F.R. § 312.11(g).

[49] *Id.* at § 312.5(c)(4).

[50] Children’s Online Privacy Protection Rule, *supra* note 1, at 116.

[51] *Id.* at 118-19. The American Civil Liberties Union argued the proposal was inconsistent with the COPPA statute given the statute states regulations “shall” permit operators to respond “more than once directly to a specific request from a child” when parents are provided notice and an opportunity to opt out. *Id.* at 117-18.

[52] *Id.* at 3-4. See also Complying with COPPA: Frequently Asked Questions, *supra* note 10, Section N.

[53] Children’s Online Privacy Protection Rule, *supra* note 1, at 4.

[54] *Id.*

[55] *Id.* at 56-61.

[56] *Id.* at 88-89.

[57] Lina M. Khan, Chair, Fed. Trade Comm’n, Statement of Chair Lina M. Khan Regarding the Final Rule Amending the Children’s Online Privacy Protection Rule Commission File No. P195404 (Jan. 16, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/statement-of-chair-lina-m-khan-re-coppa-amendments-1-16-2025.pdf.

[58] *Id.* at 1.

[59] *Id.* at 4.

[60] Andrew N. Ferguson, Comm’r, Fed. Trade Comm’n, Concurring Statement of Commissioner Andrew N. Ferguson COPPA Rule Amendments Matter Number P195404 (Jan. 16, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/ferguson-coppa-concurrence-revised.pdf.

[61] *Id.* at 1-3.

[62] *Id.* at 3.

[63] *Id.*

[64] Alvaro M. Bedoya, Comm'r, Fed. Trade Comm'n, Statement of Commissioner Alvaro M. Bedoya Joined by Commissioner Rebecca Kelly Slaughter Notice of Final Rulemaking to Update the Children's Online Privacy Protection Rule (COPPA Rule) (Jan. 16, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/bedoya-coppa-statement-2025-01-16.pdf.

[65] Press Release, Fed. Trade Comm'n, Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges (Dec. 19, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations>.

[66] Press Release, Fed. Trade Comm'n, Genshin Impact Game Developer Will be Banned from Selling Lootboxes to Teens Under 16 without Parental Consent, Pay a \$20 Million Fine to Settle FTC Charges (Jan. 17, 2025), <https://www.ftc.gov/news-events/news/press-releases/2025/01/genshin-impact-game-developer-will-be-banned-selling-lootboxes-teens-under-16-without-parental>.

[67] Andrew N. Ferguson, Comm'r, Fed. Trade Comm'n, Statement of Commissioner Andrew N. Ferguson Concurring in Part and Dissenting in Part In the Matter of Cognosphere, LLC, (Jan. 17, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/ferguson-cognosphere-concurrence.pdf.

[68] In September 2024, the House Energy and Commerce Committee passed COPPA 2.0 by a voice vote. In July 2024, the U.S. Senate passed the Kids Online Safety and Privacy Act, which included COPPA 2.0, by a 91-3 vote. In July 2023, the Senate Commerce, Science, and Transportation Committee unanimously passed COPPA 2.0. See Press Release, Ed Markey, Sen. of Mass., Senator Markey Celebrates FTC's Update to Children's Online Privacy Rule, (Jan. 16, 2025), <https://www.markey.senate.gov/news/press-releases/senator-markey-celebrates-ftcs-update-to-childrens-online-privacy-rule>.

[69] *Id.*

[70] See Securing Children Online through Parental Empowerment (SCOPE) Act, H.B. 18, 88th Leg., R.S. (2023).

[71] See Protecting Our Kids from Social Media Addiction Act, S.B. 976, 88th Leg. (2024).

[72] See Press Release, Ken Paxton, Att'y Gen. of Tex., Attorney General Ken Paxton Sues TikTok for Sharing Minors' Personal Data In Violation of Texas Parental Consent Law (Oct. 3, 2024), <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-tiktok-sharing-minors-personal-data-violation-texas-parental>.

[73] See Press Release, Ken Paxton, Att'y Gen. of Tex., Attorney General Ken Paxton Launches Investigations into Character.AI, Reddit, Instagram, Discord, and Other Companies over Children's Privacy and Safety Practices as Texas Leads the Nation in Data Privacy Enforcement (Dec. 12, 2024), <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-investigations-characterai-reddit-instagram-discord-and-other>.

[74] See Press Release, Eur. Comm'n, Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram (May 15, 2024), (IP/24/2664); see also Press Release, Eur. Comm'n, Commission opens formal proceedings against TikTok under the Digital Services Act (Feb. 18, 2024), (IP/24/926).

[75] Press Release, Austl. eSafety Comm'r, Social Media Age Restrictions (Dec. 20, 2024), <https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions>.

Please click on the link below to view the complete update and endnotes on Gibson Dunn's website:

Read More

The following Gibson Dunn lawyers prepared this update: [Ashley Rogers](#), [Ryan T. Bergsieker](#), [Natalie Hausknecht](#), [Vivek Mohan](#), [Lore Leitner](#), [Ashlie Beringer](#), [Svetlana Gans](#), [Alexus Leach](#), [Nick Carey](#), [Samantha Abrams-Widdicombe](#), [Amy Shao](#), and [Jayee Malwankar](#).

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any leader or member of the firm's [Privacy, Cybersecurity & Data Innovation](#) practice group:

United States:

[Ashlie Beringer](#) – Co-Chair, Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com)

[Ryan T. Bergsieker](#) – Denver (+1 303.298.5774, rbergsieker@gibsondunn.com)

[Gustav W. Eyer](#) – Washington, D.C. (+1 202.955.8610, geyer@gibsondunn.com)

[Cassandra L. Gaedt-Sheckter](#) – Palo Alto (+1 650.849.5203, cgaedt-sheckter@gibsondunn.com)

[Svetlana S. Gans](#) – Washington, D.C. (+1 202.955.8657, sgans@gibsondunn.com)

[Lauren R. Goldman](#) – New York (+1 212.351.2375, lgoldman@gibsondunn.com)

[Stephenie Gosnell Handler](#) – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com)

[Natalie J. Hausknecht](#) – Denver (+1 303.298.5783, nhausknecht@gibsondunn.com)

[Jane C. Horvath](#) – Co-Chair, Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com)

[Martie Kutscher Clark](#) – Palo Alto (+1 650.849.5348, mkutscherclark@gibsondunn.com)

[Kristin A. Linsley](#) – San Francisco (+1 415.393.8395, klinsley@gibsondunn.com)

[Timothy W. Loose](#) – Los Angeles (+1 213.229.7746, tloose@gibsondunn.com)

[Vivek Mohan](#) – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com)

Rosemarie T. Ring – Co-Chair, San Francisco (+1 415.393.8247, rking@gibsondunn.com)
Ashley Rogers – Dallas (+1 214.698.3316, arogers@gibsondunn.com)
Sophie C. Rohnke – Dallas (+1 214.698.3344, srohnke@gibsondunn.com)
Eric D. Vandeveld – Los Angeles (+1 213.229.7186, evandeveld@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650.849.5395, bwagner@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213.229.7472, dwongyang@gibsondunn.com)

Europe:

Ahmed Baladi – Co-Chair, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Joel Harrison – Co-Chair, London (+44 20 7071 4289, jharrison@gibsondunn.com)
Lore Leitner – London (+44 20 7071 4987, lleitner@gibsondunn.com)
Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com)
Lars Petersen – Frankfurt/Riyadh (+49 69 247 411 525, lpetersen@gibsondunn.com)
Robert Spano – London/Paris (+44 20 7071 4000, rspano@gibsondunn.com)

Asia:

Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

If you would prefer NOT to receive future emailings such as this from the firm, please reply to this email with "Unsubscribe" in the subject line.

If you would prefer to be removed from ALL of our email lists, please reply to this email with "Unsubscribe All" in the subject line. Thank you.

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit our [website](#).