Guidepost

FTC PROPOSES STRENGTHENING CHILDREN'S PRIVACY RULE

Important Context

On January 11, 2024, the Federal Trade Commission (FTC) published a Notice of Proposed Rulemaking that would fortify the Children's Online Privacy Protection Act (COPPA). This move underscores a significant shift in the regulatory landscape, aiming to address the use of children's data by companies and to enhance privacy protections for children. The proposed rule modifications would strengthen regulations pertaining to how businesses interact with children's data online. The act applies to websites and online applications directed at children under 13, but can also apply to general audience sites and apps if the website operator knows personal information is being collected from children under 13. Past enforcement actions have been directed at education technology providers, video game and entertainment products, e-commerce, online rewards, talent search sites, mobile advertising platforms, weight loss apps, online review sites, and social networking apps.

Key Provisions from the Proposed Updates

1. Expansion of COPPA's Scope: The proposal aims to extend protections to cover biometric data. However, the FTC declined to expand the scope to include data "inferred" about children.
2. Enhanced Consent Mechanisms: It creates separate parental consent mechanisms prior to disclosure of a child's personal information (with some exceptions).
3. Security Requirements: The current regulations under COPPA already mandate that operators adopt reasonable measures for safeguarding children's personal data. However, the FTC's proposed changes aim to enhance these requirements with greater specificity and structure. Operators would be tasked with creating and enforcing a comprehensive Children's Personal Information Security Program (CPISP). This program must be tailored to fit the sensitivity of the data collected, as well as the operator's size and the complexity of its operations. Key elements of a CPISP include appointing a coordinator, conducting yearly risk assessments, developing and upholding protective measures to mitigate identified risks, routinely evaluating the

effectiveness of these measures, and making necessary adjustments to the CPISP on an annual basis.

4. Data Retention: The FTC's proposed updates seek to refine the rules around data retention, emphasizing that personal information should be kept only as long as it serves the purpose for which it was initially gathered, without being repurposed. Furthermore, the FTC intends to obligate operators to formulate and disclose a clear data retention policy. This policy must outline the reasons for collecting children's personal information, justify the need for retaining this data, and establish a specific timeline for its deletion to avoid indefinite storage.

Preparing for Heightened COPPA Obligations

Businesses potentially affected by these updates should begin preparations to ensure compliance. This involves:

- Continuously identifying what children's data is collected, especially biometric data, how it is used, how long it is retained, and whether it is shared with third parties can help businesses understand their data practices and areas needing adjustment.
- Ensuring that consent mechanisms comply with the enhanced requirements of the proposed rule. This may involve developing more straightforward and transparent consent forms.
- Strengthening data security practices to protect children's information from unauthorized access or breaches is more important than ever. A well-documented risk-based program should be implemented by qualified professionals.
- Educating employees about COPPA requirements and the importance of protecting children's privacy can foster a culture of compliance.

Key Takeaways

The FTC has been increasingly vigilant in enforcing COPPA, with several high-profile cases highlighting the potential risks businesses face. Third-party consultants specializing in COPPA compliance bring deep expertise and experience in navigating the intricacies these regulatory changes, enforcement trends, and best practices, ensuring businesses receive accurate and current guidance. They can identify potential risks, recommend practical solutions, and help implement the most appropriate safeguards to ensure compliance with COPPA requirements. This is especially important where risks or safeguards have a technical as well as regulatory facets.

Penalties have ranged from hefty fines to mandates for changes in business practices. For example, Epic Games was recently fined $275 million for COPPA violations. These enforcement actions signal the FTC's commitment to children's privacy and serve as a cautionary tale for businesses to take their COPPA obligations seriously.

The FTC's proposed updates to COPPA represent a pivotal moment in the protection of children's online privacy. As the digital landscape evolves, so too must the frameworks that safeguard the youngest users. Businesses operating in this space must stay informed of these changes and proactively adjust their practices to ensure they not only comply with the law, but also contribute to a safer online environment for children. Here again consultants can provide excellent value, both in assessing the types of personal information collected from children, such as names, addresses, or

geolocation data, and evaluating the alignment of technical implementations and business operations against COPPA requirements. They also can recommend adjustments to data collection mechanisms to minimize the collection of sensitive information without parental consent, or alternatively they can recommend improvements to ensure that consent processes are robust, verifiable, and effectively obtain affirmative parental consent before children's personal information is collected.

The FTC's emphasis on stronger protections against the monetization of children's data is a clear message to companies: the privacy and security of young internet users are paramount. Businesses which disregard this message do so at their own peril.

MATTHEW CORWIN CISA, CISSP, CDPSE

Managing Director

Matthew A. Corwin has more than 20 years of experience specializing in privacy, regulatory compliance, and cybersecurity with specialized hands-on experience directing the implementation and integration of secure design principles and service engineering initiatives leveraging the latest technologies. He has a successful track record of facilitating technology-business alignment while balancing risk exposure and corporate growth. Mr. Corwin also has extensive expertise in analyzing technical architecture to attain and demonstrate best-in-class industry and regulatory standards compliance in global environments.