AN A.S. PRATT PUBLICATION
JANUARY 2026
VOL. 12 NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 1** **January 2026**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2026–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Flurry of Federal Trade Commission Activity Shows Enforcement Emphasis on Youth Protection

By Kathleen Benway, Alexander G. Brown, Maki DePalo, Jennifer C. Everett, Graham Gardner and Hyun Jai Oh*

The Federal Trade Commission (FTC) is intensifying its scrutiny and enforcement of youth protection issues, particularly around minors' privacy and content safety. This article explains the increased regulatory expectations for companies providing digital services to children and teens.

The Federal Trade Commission (FTC) recently announced a flurry of youth protection matters with broad implications for operators of online services, mobile apps, and user generated content platforms, showcasing continued engagement in an area of emphasis for the Trump-Vance FTC.

FTC YOUTH PROTECTION MATTERS

On September 3, 2025, the FTC announced[1] a settlement[2] with a Chinese toy robot manufacturer over allegations that the toymaker violated the Children's Online Privacy Protection Rule (COPPA Rule). The FTC claimed that the toymaker allowed a third-party company to collect sensitive geolocation data from children (defined by COPPA as individuals under 13) who used the toys without providing notice to parents and obtaining verifiable consent from parents. This settlement came one day after the FTC's announcement[3] of another COPPA Rule settlement with a prominent content publisher that the FTC alleged misclassified child-directed videos on a popular video-sharing platform, which enabled the collection and use of children's personal information without proper parental notice or consent.

In addition to these two COPPA Rule settlements, the FTC, together with the State of Utah, announced[4] on September 3, 2025, a settlement with operators of pornography-streaming websites. This settlement addressed allegations that the operators failed to

* The authors are attorneys at Alston & Bird LLP. They may be contacted at kathleen.benway@alston.com, alex.brown@alston.com, maki.depalo@alston.com, jennifer.everett@alston.com, graham.gardner@alston.com and hyunjai.oh@alston.com, respectively.

[1] https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-takes-action-against-robot-toy-maker-allowing-collection-childrens-data-without-parental-consent?utm_source=govdelivery.

[2] https://www.ftc.gov/system/files/ftc_gov/pdf/Apitor-JointMotion-StipOrder.pdf.

[3] https://www.ftc.gov/news-events/news/press-releases/2025/09/disney-pay-10-million-settle-ftc-allegations-company-enabled-unlawful-collection-childrens-personal.

[4] https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-takes-action-against-operators-pornhub-other-pornographic-sites-deceiving-users-about-efforts.

block and remove content featuring child sexual abuse material and nonconsensual material.

The FTC's focus on youth protection issues was further demonstrated by its announcement[5] on September 11, 2025, that the FTC was using its 6(b) authority to request information from seven artificial intelligence (AI) companies about the impact of AI chatbots on children's and teens' mental health. Under Section 6(b) of the FTC Act, the FTC is authorized to conduct broad-based studies about specific aspects of a company's business or an industry sector.

COPPA RULE ACTIONS

The COPPA Rule requires companies to disclose their practices for the collection and use of children's personal information and to obtain verifiable parental consent before collecting and disclosing personal information from children. The FTC's two most recent COPPA Rule settlements illustrate how the FTC exercises its enforcement authority in practice.

First, the FTC brought an action against a China-based manufacturer that sells toy robots to children in the United States. The toy robots were paired with a free mobile app that allowed users to program and control the toys. According to the FTC, the toymaker integrated a third-party software development kit (SDK) into the mobile app. When Android users interacted with the mobile app, the SDK allegedly accessed users' geolocation data, including data from children, without the toymaker providing notice to parents or obtaining verifiable parental consent.

The proposed settlement order requires the toymaker to take multiple corrective measures, including:

- Deleting any personal information collected in violation of the COPPA Rule.
- Providing notice to parents and obtaining verifiable parental consent before collecting and using personal information from children.
- Deleting children's personal information upon a parent's request.
- Retaining children's personal information only as long as reasonably necessary to fulfill the purpose it was collected for.

[5] https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-launches-inquiry-ai-chatbots-acting-companions?utm_source=govdelivery.

- Submitting a compliance report to the FTC one year after the settlement, under penalty of perjury, describing whether and how the Chinese toymaker is complying with the settlement order.
- Updating the compliance report within 14 days of any change in its designated point of contact or corporate structure that may affect compliance obligations, for 10 years.
- Creating and maintaining records related to revenues, personnel providing services to consumers, consumer complaints and refund requests involving privacy practices, and compliance with the settlement order for 10 years. Retain each record for five years.
- Otherwise complying with the COPPA Rule.

The settlement also imposes a civil penalty of $500,000, which is suspended based on the toymaker's inability to pay. Notably, the settlement does not require the toymaker to engage an independent third-party auditor to periodically assess its compliance with the settlement order, a measure the FTC often leveraged in prior enforcement settlements.

Second, the FTC alleged that a prominent video content publisher failed to properly designate its videos on a major video-sharing platform as "Made for Kids." Instead, the video content publisher allegedly posted child-directed videos on channels marked as "Not Made For Kids." This mislabeling allegedly resulted in the collection of children's personal information by both the video-sharing platform and the video content publisher without proper notice or verifiable parental consent. It also allegedly exposed children to age-inappropriate videos through the autoplay features of the video-sharing platform.

Like the proposed settlement order against the Chinese toymaker, the proposed settlement order against the video content publisher requires:

(1) Providing parental notice and obtaining verifiable parental consent before collecting and using personal information from children;

(2) Submitting a compliance report to the FTC and updating it for 10 years;

(3) Creating and maintaining compliance records for 10 years and retaining each record for five years; and

(4) Complying with the COPPA Rule.

The video content publisher must also take the following additional steps:

- Pay a $10 million civil penalty.
- Implement an age designation program to ensure videos are accurately designated as "Made for Kids" or "Not Made For Kids."

- Designate qualified employees to coordinate and be responsible for the age designation program.
- Train employees with roles and responsibilities in publishing videos on the video-sharing platform on the requirements of the age designation program upon hire and at least once every 12 months afterwards.
- Assess and document the effectiveness of the age designation program at least every 12 months.

Notably, the age designation program requirement will be removed if the video-sharing platform either (1) implements age-assurance technologies capable of determining the age, age range, or age category of all platform users, or (2) eliminates platform users' ability to label videos as "Made for Kids." The FTC explained that this forward-looking provision reflects the anticipated adoption of age-assurance technologies.

OTHER YOUTH PROTECTION INITIATIVES

In addition to the two COPPA Rule actions, the FTC took two further initiatives underscoring its focus on youth protection. These highlight the FTC's increasing focus on not only children under 13 but also all minors under 18.

First, in an enforcement action brought jointly with Utah's Division of Consumer Protection, the FTC alleged that operators of major adult content websites engaged in unfair and deceptive practices by failing to block and remove child sexual abuse material and nonconsensual content. The proposed settlement order imposes a $15 million penalty, with $10 million suspended, and requires the operators to implement procedures to prevent the dissemination of such material on their websites. In a statement[6] accompanying the settlement announcement, FTC Chair Andrew Ferguson emphasized that protection of minors remains a central priority of the FTC under President Trump.

Second, the FTC's focus was further demonstrated in its announcement that the FTC had launched an inquiry to study the impact of consumer-facing AI chatbots on minors' mental health and was requesting information from seven tech companies operating popular AI chatbots. The inquiries seek information about how these companies measure, test, and monitor potentially negative impacts on children and teens. This development followed on the heels of a recent meeting of the White House Task Force on AI Education hosted[7] by First Lady Melania Trump.

---

[6] https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-chairman-andrew-n-ferguson-joined-commissioner-melissa-holyoak-commissioner-mark-r-meador-re-ftc-utah-division-consumer-protection-v-aylo-group-ltd-et-al.

[7] https://www.whitehouse.gov/briefings-statements/2025/09/first-lady-melania-trump-hosts-a-meeting-of-the-white-house-task-force-on-artificial-intelligence-education/.

KEY TAKEAWAYS

As practitioners assess how the Trump-Vance FTC's consumer protection enforcement priorities may evolve under Ferguson, it is clear that youth protection issues, including those addressed by COPPA, will remain central.

Companies that offer minor-directed or minor-appealing products or services should anticipate increased scrutiny by the FTC. If companies collect and maintain minors' personal information or partner with another company that does, now is the time to confirm that required disclosures are provided, relevant consents are obtained, and appropriate security safeguards are implemented and maintained. Failure to take these steps can lead to lengthy and onerous investigations, significant penalties, and reputational harm.

Practical implications for companies include:

- Treat geolocation as highly sensitive information, especially for children, and disable the unnecessary collection of geolocations by default in child-directed content.
- Design notice provision and consent processes, including a consent withdrawal mechanism, into product workflows.
- Confirm there is no gap between a company's published privacy policy and its actual data-handling practice.
- Enable a standard operating procedure for prepublication content controls, content takedown, and regular content monitoring.
- Conduct adequate due diligence, including compliance assessments of the use of SDKs, analytics, and moderation vendors.
- Contractually require vendors to adhere to minors' privacy requirements.
- Implement and execute comprehensive privacy and security programs.
- Adopt repeatable operational mechanisms such as documented controls and auditable metrics.
- Regularly train personnel for compliance with evolving regulatory requirements.