

Assignment 6.1: HyperBeard COPPA Compliance Analysis

Joshua A. Wortz

University of San Diego

CSOL-540

Dr. Michelle Moore

08/01/2025

Introduction

As the digital gaming market continues to expand, so too do the regulatory responsibilities of developers, particularly those creating content for children. In 2020, the Federal Trade Commission (FTC) announced a settlement with HyperBeard Inc., a mobile gaming company that violated the Children's Online Privacy Protection Act (COPPA). The case stands as a critical warning to other companies in the space: failure to implement meaningful privacy protections, especially for child-directed content, can result in substantial regulatory and reputational damage. This paper presents a thorough analysis of the HyperBeard case, legal interpretation of the FTC's decision under COPPA, and strategic recommendations for implementing robust, child-focused privacy protections within our organization.

Case Summary: HyperBeard's COPPA Violation

HyperBeard is a mobile gaming company known for publishing visually charming, whimsical games such as *KleptoCats* and *Chichens*, which feature animated animals and simplistic, tap-based gameplay. These features, along with the art style, music, and user experience, led the FTC to conclude that the apps were directed toward children under 13, despite the company's attempt to disclaim this with language stating the games were "not intended for children."

Between 2017 and 2019, HyperBeard allowed third-party advertising networks to be embedded in its games. These networks collected persistent identifiers (such as device IDs and geolocation data) to deliver targeted advertising. According to the FTC, HyperBeard failed to (1) notify parents of data collection practices, (2) obtain verifiable parental consent, and (3) implement mechanisms to stop data collection when children were users. As a result, the FTC

filed a complaint and reached a settlement under which HyperBeard agreed to pay \$150,000 and delete all improperly collected data (Federal Trade Commission, 2020).

Notably, the FTC emphasized that the company could not shield itself from COPPA responsibilities simply by posting disclaimers. The actual content and audience appeal of the games, not intent, determines whether an app falls under COPPA's jurisdiction. HyperBeard neither disputed the charges nor admitted guilt, but the outcome made clear that passive compliance or disclaimers are not sufficient.

Legal Analysis: COPPA and the FTC's Enforcement

The Children's Online Privacy Protection Act of 1998 (15 U.S.C. §§ 6501–6506) mandates that websites and online services directed to children under 13 must obtain verifiable parental consent before collecting personal information from children. "Personal information" includes names, contact information, and persistent identifiers such as cookies or device IDs when used for behavioral tracking (COPPA Rule, 16 C.F.R. Part 312).

COPPA is content-neutral but audience-focused. The FTC evaluates factors such as the app's visuals, music, language, and promotional materials to determine whether it is "directed to children." This was a key point in the HyperBeard case: although the company attempted to sidestep compliance with disclaimers, the FTC applied a "totality of the circumstances" standard, similar to *Jacobellis v. Ohio*'s "I know it when I see it" test used in obscenity cases (Mireles & Hobaugh, 2024). This level of subjectivity challenges companies to interpret vague guidelines while avoiding liability.

Furthermore, HyperBeard's integration of third-party advertising SDKs meant that external parties were collecting data without consent, yet HyperBeard was still held accountable. This reinforces the FTC's stance that companies are liable for the actions of their embedded services. The Commission's message was clear: failing to audit or control data flows from third-party partners is not a defense under COPPA.

Strategic Recommendations for Compliance and Risk Mitigation

To safeguard our organization against similar regulatory action and potential civil litigation, I recommend a three-tiered compliance framework based on design, governance, and enforcement:

1. Design: Build Child Privacy into the Product

- Child-directed Content Review: Implement an internal review board to assess whether apps or game features may be perceived as child-directed under COPPA's criteria. If so, default to complete compliance requirements regardless of intent.
- Age Gate Reinforcement: Incorporate neutral, age-gating mechanisms (e.g., requiring manual input of birthdate without suggestive cues) on all apps with child-attractive features. This ensures age screening is documented and meets FTC expectations.

2. Governance: Strengthen Data Practices and Vendor Oversight

- Parental Consent Platform: Integrate a verifiable parental consent workflow using reputable identity verification tools for all data collection from users under 13.

- Third-party SDK Vetting: Require all advertising or analytics partners to sign data processing agreements (DPAs) affirming compliance with COPPA and undergo periodic audits to confirm that no unauthorized tracking is occurring.
- Privacy-by-Design Audits: Conduct recurring audits of data flow maps to identify any unintentional data capture, especially from embedded SDKs and APIs.

3. Enforcement: Monitor, Train, and Disclose

- Employee Training: Launch mandatory privacy training for development, marketing, and legal teams with a focus on COPPA and FTC enforcement trends.
- Transparent Privacy Policies: Disclose data practices in privacy notices tailored for parents, with simple, non-legalistic language. Maintain a direct contact point for parental inquiries or deletion requests.
- Litigation Readiness: Establish a privacy incident response protocol to rapidly detect, contain, and report data exposure involving minors. Ensure documentation practices can support regulatory inquiries or civil litigation defense.

Conclusion

The HyperBeard case is a cautionary tale for any company operating in the child-focused digital space. It illustrates that disclaimers are not enough, third-party tools are a liability without

oversight, and intent is irrelevant when the product's appeal speaks for itself. In a regulatory environment where FTC judgments may appear subjective, companies must proactively exceed the minimum legal requirements to protect both children and their business interests. By embedding privacy into product design, governance, and enforcement, our company can establish itself as a trustworthy steward of children's data, while avoiding fines, lawsuits, and brand damage.

References

Federal Trade Commission. (2020, June 4). *Mobile app developer HyperBeard settles FTC allegations it violated children's privacy law.*

<https://www.ftc.gov/news-events/news/press-releases/2020/06/mobile-app-developer-hyperbeard-settles-ftc-allegations-it-violated-childrens-privacy-law>

Mireles, M. S., & Hobaugh, J. L. (2024). *Principles of cybersecurity law* (2nd ed.). West Academic.

The National Law Review. (2023, September 20). *Tracking kids through your app? Think again.*

<https://www.natlawreview.com/article/tracking-kids-through-your-app-think-again>