Fortnite Skinned: Fined $520 Million by the FTC for Privacy Violations

On Dec. 19, 2022, Epic Games, the developer of popular video game Fortnite, agreed to pay more than $520 million to settle Federal Trade Commission (FTC) claims that alleged a violation of the Children's Online Privacy Protection Act (COPPA) and the deployment of "dark patterns" used to trick players into making in game purchase. The settlement amount is divided into two parts. Epic will pay a $275 million penalty to the FTC for privacy violations and $245 million in refunds to users tricked into making unwanted purchases.

Released in July 2017, the colorful survival shooter quickly became a household name and currently boasts 400 million active players. Children make up a substantial portion of the player base. A 2019 survey revealed that a staggering 53% of U.S. children aged 10-12 played Fortnite weekly, compared to 33% of teens aged 13-17 and 19% of young adults aged 18-24.

The game is as profitable as it is popular. Despite purporting to be "free to play," Fortnite reported more than $9 billion dollars in revenue in the game's first two years alone. Fortnite earns revenue through in-game microtransactions for cosmetic items such as character costumes. Players cannot purchase anything that would give them a competitive advantage or increase their odds of winning.

Privacy Violations

Under COPPA, it is "unlawful for any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information." In a federal court complaint, the FTC alleged that Epic violated COPPA by collecting personal information from players under the age of 13 without obtaining verifiable parental consent.

The FTC determined that there was overwhelming evidence to suggest that Fortnite targeted children. Through market research, Epic understood a majority of its player base was under the age of 13. The developer executed various marketing and licensing deals for children's toys and Halloween costumes and hosted live events featuring celebrities popular with children. The FTC also highlighted intercompany communications clearly revealing Epic's focus: "Agree with the idea that, generally, all theming should be relevant to [an 8 to 10 year old] as a litmus test."

Despite Epic's clear targeting of young consumers, the developer failed to establish a mechanism for obtaining parental consent for players under 13. While the FTC did acknowledge that Epic eventually started requiring parental consent, the developer still did not obtain consent for accounts created on Xbox and PlayStation consoles. Moreover, Epic made limited efforts to retroactively correct consent issues with existing accounts.

In addition, the FTC alleged that Fortnite's always-on text and voice chat harmed minors. Adult players had unfettered access to chatting with minors, with no way for parents to limit their child's exposure. The FTC found evidence that children were bullied, threatened, harassed and exposed to sensitive and adult content while playing Fortnite. Shortly after the game launched, Epic employees attempted to bring this issue to the company's attention, but these complaints were largely ignored. Epic did eventually add privacy controls to turn chat functions off, but the FTC found they were not easily accessible and buried in the settings menu.

Dark Patterns

In a separate administrative complaint, the FTC alleged that Epic tricked players into making unwanted purchases by employing dark patterns. Put simply, dark patterns are interfaces designed to trick the user into doing things the user does not intend. For example, the FTC alleged that Fortnite's counterintuitive menu layout and button configuration caused players to make accidental purchases with one click. Players could be charged while attempting to wake the game from sleep mode or while the game was loading. Additionally—and similar to claims brought against Amazon, Apple and Google—Fortnite allowed children to continually reauthorize their parents' credit cards without their parents' consent. These practices generated hundreds of millions of dollars in unauthorized charges.

Key Takeaways

Through this settlement, the FTC sent a strong signal that it will be closely monitoring commercial marketing activity targeting children. This is consistent with the FTC's recent activity in the privacy and commercial surveillance space. On Aug. 11, 2022, the FTC published an Advance Notice of Proposed Rulemaking to "ask the public to weigh in on whether new rules are needed to protect people's privacy and information in the commercial surveillance economy." The notice focuses on the need to bolster children's privacy online and the importance of obtaining informed consent, among other topics. Organizations looking to avoid regulatory attention should consider the following compliance tips:

- Evaluate your organization's customer base and determine whether your organization's website markets toward children. Does the website sell children's products or contain branding from popular children's franchises?
- Listen to your employees. Often, your employees have the most accurate understanding of your brand, website and products. Check in with them often and carefully consider any issues they bring to your attention.
- Disclaimers are not enough. Claiming that your organization complies with COPPA or that your website is not intended for children will not deter regulatory scrutiny. Here, the FTC conducted a detailed factual inquiry that considered Epic's practices and actions. A privacy statement that contains the right language is insufficient without actual compliance.
- Evaluate your website's interface. How many clicks does it take to make a purchase? Are key privacy controls difficult to locate? Does the website provide notice to consumers regarding the collection of payment information and an opportunity to consent? Does your website ask consumers to reauthorize payment information after each purchase? Are there adequate checks to prevent children from accessing stored credit and debit cards?

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters, including compliance with COPPA and other privacy authorities. If you have any questions about COPPA, or the FTC privacy enforcement, please contact Jessica Copeland, CIPP/US, Mario Ayoub or any attorney in Bond's cybersecurity and data privacy practice.

BOND SCHOENECK & KING ATTORNEYS