Bloomberg Law

Professional Perspective

Consent Is Key to Avoiding Child Privacy Class Actions

Cynthia Larose and Natalie Prescott,
Mintz, Levin, Cohn, Ferris, Glovsky and Popeo

Consent Is Key to Avoiding Child Privacy Class Actions

Contributed by Cynthia Larose and Natalie Prescott, Mintz, Levin, Cohn, Ferris, Glovsky and Popeo

Privacy class actions involving children are on the rise. In light of the Covid-19 pandemic, stay-at-home orders, school closures, and children's increased use of technology for remote e-learning, courts and regulatory agencies are on high alert when it comes to protecting the minors online. Technology companies, businesses, and services that interact with children must be especially vigilant about safeguarding minors' privacy rights going forward.

This article analyzes the latest litigation trends that are emerging from the most recent privacy class actions involving children. While the focus is on the three latest high-profile cases against TikTok, Google, and Amazon, lessons learned from lawsuits filed against these companies can help businesses of all sizes.

The most important trend apparent from these cases is the importance of obtaining a verifiable, documented, and informed parental consent before any of child's personal information is collected online. Additionally, because different laws have a different age cutoffs for requiring parental consent, in these uncertain times it behooves companies to carefully analyze the age demographic of their target customers and the various state and federal laws that apply.

Biometric Privacy Class Action Against TikTok

On April 30, 2020, popular social media platform TikTok was hit with a biometric privacy class action for allegedly collecting children's facial geometry scans through its app platforms. See Complaint, *P.S. et. al v. TikTok, Inc.*, N.D. Cal., Case No. 20-cv-02992. The complaint was filed on behalf of all Illinois residents who are users of the musical.ly app or the TikTok app who used the apps' face filters, stickers, or tracker-lens features while residing in Illinois. While not expressly limited to minors, this lawsuit effectively encompasses a class of minors, since the named plaintiffs specifically, and a large percentage of the app users generally, are children.

The plaintiffs alleged that TikTok's apps use facial geometry primarily for two purposes—to determine the users' age and to allow them to superimpose animated filters. The plaintiffs further assert that TikTok does not disclose what it does to the data, who has access to it, whether this data is stored, and for how long it is stored—all in direct violation of the Illinois Biometric Information Privacy Act.

BIPA is a state law that protects privacy rights of Illinois residents and sets forth an elaborate list of requirements for companies using biometric technology. Most notably, BIPA prohibits companies from collecting, storing, or using biometric data without prior notice and written consent. The law allows private parties to sue and to seek penalties between $1,000 and $5,000 per every violation, as well as attorney's fees and costs. BIPA class actions are some of the costliest privacy class actions, and BIPA settlements often range in the millions or even tens of millions.

According to the complaint, TikTok collects, stores, and uses the facial scans of the minors without informed consent and without a required data-use and retention policy. In this case, the plaintiffs pleaded a single cause of action against TikTok for BIPA violations and relied on it to seek damages of at least $1,000 per each violation, as well as attorneys' fees and costs.

TikTok was already in hot water with regulators well before this litigation. In 2019, TikTok agreed to pay $5.7 million to settle with the Federal Trade Commission over allegations that it violated the Children's Online Privacy Protection Act when it illegally collected images, voice recordings, and geolocation of minors without parental consent. See FTC complaint, *United States v. Musical.Ly*, N.D. Cal., Case No. 19-cv-1439. At that time, this settlement was deemed to be the largest civil penalty ever collected in the U.S. in a child privacy case. In both of the above lawsuits, lack of proper consent was the main litigation trigger and the primary violation on which the case against TikTok was built by the plaintiffs' lawyers and by the FTC.

Biometric and COPPA Privacy Class Action Against Google

Google was sued in April 2020 by minor students for alleged violations of California's Unfair Competition Law (UCL), BIPA, and the Children's Online Privacy Protection Act (COPPA). See complaint, *H.K. et al. v. Google LLC*, N.D. Cal., Case No. 20-cv-02257. This lawsuit came just weeks after all U.S.-based schools were forced to turn to remote learning, with many

choosing to rely on Google's e-learning solutions and educational platforms. What many parents and educators may have seen as a blessing quickly turned into a privacy litigation phase for Google.

In this lawsuit, the plaintiffs claim that Google unlawfully collected, stored, and used their personal information and biometric data without their parents' informed consent. By providing access to its ChromeBooks and educational platforms, Google was allegedly able to create, collect, store, and use facial geometry scans and voiceprints of millions of children. Unlike many other child privacy class actions we have seen to date, this lawsuit expanded the scope of allegations, with a shift towards an interplay of multiple state and federal laws.

Nevertheless, the complaint still primarily emphasized Google's failure to obtain informed consent to collection and storage of children's personal and biometric information as its main theme throughout. In addition to BIPA claims, which protect only Illinois residents, this putative class action complaint asserted numerous violations of COPPA and UCL. This pleading strategy vastly expanded the scope of the proposed class to include not only Illinois but also California residents, in addition to a broader, nationwide class.

By a way of background, COPPA is a federal law that protects minors under 13. COPPA gives parents control over what data is collected about their children online. It requires operators of websites and apps aimed at children under 13 to obtain parental consent before collecting their data or information. To avoid triggering COPPA's penalties, most companies operating online in the U.S. expressly prohibit users under 13 from using their products or services in the terms and conditions. Unlike BIPA, COPPA expressly requires "verifiable parental consent" before collection of data.

"Incredibly, Google has managed to violate both … COPPA and BIPA … at the same time, by collecting, storing, and using the personally identifying biometric data of millions of school children throughout the country … without seeking, much less obtaining the requisite informed written consent from any of their parents or other legal guardians," the complaint alleged.

The plaintiffs also pointed out that the FTC had "recently released a 'Best Practices' guide for companies using facial recognition technology," which "underscores the importance of companies' obtaining affirmative consent from consumers before extracting and collecting their biometric identifiers and biometric information from digital photographs." The complaint alleges that Google failed to abide by all of these consent-related requirements.

A Wiretap Privacy Class Action Against Amazon

The consent theme re-emerged in a case against Amazon, where the court held that the minors' privacy voice-recording claims cannot be forced into arbitration without proper consent from their parents. On April 22, 2020, Amazon.com, Inc. filed an appeal, asking the Ninth Circuit to find that Amazon's broad arbitration and class-action waiver agreement with its adult users also also binds their minor children who used their parents' Alexa devices.

This appeal stemmed from a ruling by a District Court for the Western District of Washington, which declined to automatically enforce parental arbitration agreements against children who had never consented to them, thereby strengthening the minors' privacy class action claims in a federal court, instead of forcing them to arbitrate individual claims piecemeal. See order, *B.F. v. Amazon.com Inc.*, W.D. Wash., Case No. C19-910 RAJ-MLP.

In this case, the plaintiffs filed their putative class action complaint against Amazon.com, Inc. and a2z Development Center, Inc., d/b/a Amazon Lab126 back in in June 2019. The complaint alleged that Alexa illegally created and stored voiceprints of millions of children without their consent or their parents' consent. It was filed on behalf of a proposed class of residents "in Florida, Illinois, Maryland, Massachusetts, Michigan, New Hampshire, Pennsylvania, and Washington who used Alexa on a household Alexa Device while they were minors, but who have not downloaded and installed the Alexa App." It included but one cause of action–for violation of wiretap statutes of these various state laws. The plaintiffs immediately demanded a jury trial–the right which their parents had voluntarily given up by entering into their user agreements with Amazon.

Three months after this complaint was filed, Amazon finally filed a motion to compel arbitration, asking the district court to find that the "[p]arents and their children cannot, by clever pleading, evade the agreements to arbitrate all disputes with Amazon." See Motion at 1. Amazon pointed out that there was a valid and enforceable arbitration agreement and class-action-waiver provision between the parties. Amazon based this plea on the assumption that the account holders for the Alexa devices in question were the ones who expressly agreed to arbitrate disputes with Amazon, and that this agreement

effectively bound their respective households as well. Specifically, Amazon believed that minor plaintiffs were legally bound through their parents, who allowed the minors to use their Alexa devices. By exploiting the "benefits" of their parents' agreements with Amazon—argued the defendants—the families could not "avoid arbitrating their claims by suing in the names of th[e] children."

The district court strongly disagreed with Amazon's reasoning. On April 9, 2020, it adopted the Magistrate Judge's Report and Recommendation in favor of the putative class plaintiffs. Applying Washington law, which governed this dispute and the long-established arbitrability principles, the court found that Amazon did not meet its burden to prove that there was a valid agreement to arbitrate, which encompassed the dispute in question.

The court emphasized that, as a general rule, the parties that did not sign an agreement to arbitrate disputes are not bound by it. The court declined to recognize an exception to this rule proposed by Amazon—that the doctrine of equitable estoppel should compel minor plaintiffs to arbitrate. While Washington law does recognize such an exception in instances where a non-signatory party knowingly exploited the benefits of the contract or made misrepresentations to the defendant, this exception was not so broad as to encompass those who merely "directly benefit" from the contract. Moreover, even if the "direct benefit" exception did apply, the court found that the minor plaintiffs, at most, received only an indirect benefit from the contract.

Importantly, the district court pointed out that Amazon could have salvaged its binding-arbitration claim, had it expressly included in its agreement with the parents a clear requirement that the parents must consent to arbitration on behalf of their children as a condition to using Amazon's services. Absent this express agreement, siding with Amazon's contention would lead to "absurd results, where any nonregistered user who uses the devices in question could be bound by the arbitration agreement," ruled the court.

Conclusion

As more and more companies are increasing their online presence and reaching an audience in the wider age range, the following are some of the takeaways from the latest set of court filings:

- Express parental consent (and a means to track that consent) is an important element to protecting companies from regulatory and child privacy class actions.
- Companies that do not intentionally target children but are aware that their platforms may attract child users and collect personal information from those children should take steps either to prevent sign-ups by children or to obtain parental consent on their behalf.
- Companies that specifically target children online, provide services to children, or otherwise collect personal information from children should consult with experienced counsel to analyze and ensure compliance with every applicable state and federal law.
- Companies that specifically collect biometric data (whether that of children of otherwise) should account for the requirements of individual states where the company does business. Currently, Illinois, Texas, and Washington have the most stringent biometric laws, though many other state laws may mandate at least a minimal level of compliance.
- Review your terms and conditions and analyze whether a class action waiver, jury waiver, and arbitration agreement may be appropriate for your user terms, and if so, ensure that the terms are properly entered into by end users and well documented.