LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Privacy Lessons From FTC Settlement With Chinese Toymaker

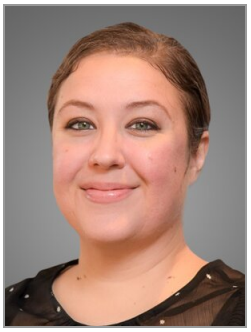
By **Liisa Thomas and Kathryn Smith** (November 3, 2025, 2:06 PM EST)

Companies have been closely watching how the Federal Trade Commission under President Donald Trump will approach consumer protection issues.

In September, the Apitor Technology Children's Online Privacy Protection Act **settlement** with the agency gave us some guidance.

In reviewing United States of America v. Apitor Technology Co. Ltd., in the U.S. District Court for the Northern District of California, it is helpful to keep in mind the current makeup of the agency.[1]

Liisa Thomas



Kathryn Smith

While the FTC is typically led by five commissioners from both sides of the aisle, there have been no Democratic commissioners since March. Instead, Republican commissioners fill three of the five seats, with two being vacant, and one of those three was not appointed by Trump.

The case before the commission was brought under COPPA, a law that dates to the early days of the internet.

For the reasons outlined below, the settlement suggests that, moving forward, the agency may focus on situations where children's information is sent offshore, companies use software development kits on kids' sites or apps, or companies passively collect personal information from children.

COPPA

COPPA applies to entities that collect personally identifiable information online from children under 13. The law was created and passed under a markedly different digital environment: Those who were children at the law's inception are now almost 40 years old.

COPPA does not contain a private right of action. Instead, the FTC and states can bring actions for violations, and the FTC is charged with developing regulations under the law. Those regulations have been updated many times in the last 27 years.

The most recent set of changes was made under the Biden administration, delayed after Trump took office, and then ultimately went into effect in June.

Under the law, companies must, among other things, get parental consent before collecting children's personal information. They must also outline — in a company's privacy policy and directly in a notice to parents — how children's personal information will be used.

The FTC's amended COPPA regulations have attempted to bring the parental notice requirement in line with other laws, adding a requirement to list specific categories of personal information collected, the identities or categories of third-party recipients, and the purposes of these disclosures.

Like other privacy laws, the rule differentiates between service providers, acting on behalf of the company, and independent third parties. For the privacy policy, the rule has added to the extensive existing content requirements an obligation to tell parents how they can contact the company, and

details regarding changes to the information practices.[2]

Over the years, the FTC has grappled with defining personal information under COPPA. Its amended regulation now includes persistent identifiers and photos. The amendment also set out more detailed data security obligations and has a separate opt-in obligation for targeted ads.

Finally, the revised regulation allows parents to withhold consent to the sharing of their child's personal information with third parties.

The Apitor Matter

With these obligations as a backdrop, the FTC brought this recent matter against Apitor, a toy manufacturer that released an app for children to use with their robot toys.

According to the FTC complaint, the app let children program their robots — but to do so, the children needed to enable location permissions. Once enabled, a third-party software development kit, JPush, developed by Chinese-based Jiguang, would send the child's physical location to that entity's Chinese-based servers.

In its complaint against Apitor, the FTC did not provide many details about the rationale for its conclusions.

However, it seems clear from the settlement reached that it presumed that children's location was personal information — not a new position for the FTC or others — and Jiguang was a third party. If true, this would trigger COPPA's obligations to give notice and get parental consent as noted above, unless a COPPA exception applied.

For support that the FTC may have viewed Jiguang as more than a service provider, we see in the FTC complaint a reference to the Jiguang privacy policy. Namely, that Jiguang will "use [personal information] as it sees fit, including for advertising and sharing data with third parties."[3]

As part of the settlement, the FTC pointed to several issues with Apitor's activities. These included failing to provide appropriate notice to parents, failing to ensure that parents received such notices, and failing to obtain verifiable parental consent before collecting personal information from children.

The FTC also alleged that Apitor did not delete children's personal information when parents requested it and kept it longer than necessary to fulfill the child's request.

To settle this matter, Apitor agreed, among other things, to delete geolocation information, modify its privacy policy, and obtain parental consent in the future.

In addition, the company agreed to delete children's information upon a parent's request or when it is no longer needed. While the FTC imposed a $500,000 civil penalty, it was suspended due to the inability to pay.

Lessons Learned

For companies looking to derive lessons from this case, there are many. And lessons can be gleaned even if your app doesn't cater to children.

Perhaps the biggest takeaway is how to evaluate and conduct diligence on your company's own practices. Here are several tips.

First, keep in mind that information collected passively can include personal information. Related to this is the very real possibility that your business team's working definition of "personal" is a lot narrower than the legal definition. Thus, when conducting diligence to understand what information the tracking tools on your site gather, ask business teams "what information is being tracked," and not "are we tracking personal information?"

Second, carefully consider how to conduct due diligence on the third parties that operate these tools. Will they be placing them on your company's site or within an app and using the information for their

own purposes? Or will they be using the information only to support your operations? What contractual promises are in place to support their representations? What do their privacy policies say? What about other documentation, like pitch decks, websites or email communications with your team?

Third, evaluate how you will audit and assess these tools generally. Who within the organization can help you understand the reasons the tools have been placed on your site or app? Is it one central team? Or do many different teams have the ability to place tools on your platforms?

Fourth, take extra care when information is sensitive in nature, like children's information, for example, and if it is being sent to entities in sensitive jurisdictions. Here, it may be helpful to get external validation or to do separate research. With the names of the third parties, looking up where they are located may be the best option.

Fifth, and finally, do not put your diligence on a set-it-and-forget-it path. Just as your company's own practices may change, so may the practices of the third parties with whom you do business. Similarly, the tools that are gathering limited information today may get upgraded to gather more tomorrow. Having a regular cadence of confirming practices can be a useful way to mitigate risk.

Liisa Thomas is a partner, and leader of the privacy and cybersecurity team, at Sheppard Mullin Richter & Hampton LLP.

Kathryn Smith is an associate at the firm.

[1] United States of America v. Apitor Technology Co., Ltd., No. 3:25-cv-07363, Stipulated Order for Permanent Injunction, N.D. Cal., Sept 25, 2025.

[2] 16 C.F.R. § 312.4(b)(2)(vi)-(vii).

[3] Paragraph 18 of the FTC complaint.
