Published on *The National Law Review* https://natlawreview.com

Operational Takeaways from the Latest CCPA Enforcement Settlement (Hint: SDKs and Consent for Children's Data Don't Just Live in a Pineapple Under the Sea…)

Article By:

Darren Abernethy

The California Attorney General and Los Angeles City Attorney last week jointly settled an enforcement action against a mobile gaming company ("the Company") for alleged violations of the Children's Online Privacy Protection Act (COPPA), the California Consumer Privacy Act (CCPA), and the state's Unfair Competition Law. The city and state did so based on claims that the Company (1) collected, disclosed, sold and/or shared children's personal information without the proper corresponding forms of required consent, and (2) based on age-inappropriate personalized advertising to children in connection with the Company's free mobile app games. The matter has been settled in the form of $500,000 in civil penalties and injunctive relief.

What follows is a brief recitation of the underlying facts in the matter, the third public CCPA enforcement settlement, followed by a broader focus on action items for businesses that can be gleaned from the case based on the enforcers' points of emphasis in relation to the respective laws involved.

Overview of the Facts Alleged

According to the complaint, the Company is a video game developer and publisher that generates revenue through advertising and in-app purchases within free versions of its mobile apps—some of which are directed to children or targeted to mixed audiences (i.e., when underage children are part of the audience but not the primary target). Focusing on one mobile game in particular, the cooking simulation game, "SpongeBob: Krusty Cook-Off" (the "App"), the California Office of the Attorney General (OAG) and L.A. City Attorney (together, "enforcers") argued that the Company did not properly obtain parental consent under the federal COPPA for the online collection of personal information from children under 13 years of age, and also did not obtain affirmative opt-in consent before disclosing the personal information of consumers between the ages of 13 and 16 under the CCPA. Other relevant case facts include that:

- Although the Company's terms of service and privacy policy stated that consumers must be 13 or older to use the Company's services, the Company was aware that children under 13 were using the App and that it was directed to children;

- In September 2022, the Children's Advertising Review Unit (CARU) of the Better Business Bureau published findings that the Company had violated both CARU's children's advertising guidelines and COPPA through the App by failing to provide "a neutral and effective age screen…or to obtain verifiable parental consent" before collecting or disclosing children's personal information. CARU's investigation found that the Company's display ads also used "deceptive tactics," as further described below.
- Regardless of the age entered on the App's improperly configured age screens (discussed further below), and due to incorrectly implemented third-party software development kits (SDKs), the personal information of consumers who self-identified as under 13, or as at least 13 and less than 16, was sold or shared to third parties (including for advertising purposes) without the required parental or opt-in consent.

Operational Takeaways from the Settlement

As described in more detail in the complaint or proposed final judgment and permanent injunction before the federal District Court for the Central District of California, the following represent explicit or inferred action items that the OAG and L.A. City Attorney believe are relevant for compliance with the applicable laws:

- **Maintain a Robust "SDK Governance Framework" and Add Privacy Policy Details Regarding SDK Data Collection and Use Practices.** The enforcers placed responsibility on the Company for insufficiently reviewing or auditing the setup and use of third-party SDKs in the App, which it needed to do as part of its CCPA and COPPA compliance efforts. Similarly placed businesses should ensure that they do not sell or share the personal information of consumers—including through SDKs, advanced programming interfaces, or other third-party programming code—if they have actual knowledge that a consumer is less than 13 (unless proper parental notice and consent is obtained) or is between 13 and 16 (unless the consumer provides opt-in consent to doing so). This should be explained to consumers as part of a "*just-in-time notice*" at the time of collection of such personal information, explaining what information will be sold or shared, offering links to the relevant portion of the privacy policy, and disabling actual disclosure of the data to third parties until *after* the corresponding appropriate level of opt-in consent is obtained (whether for COPPA or the CCPA).

  To the extent the settlement agreement here can be read as putting others on notice as to what the regulators expect of *all* companies, the proposed consent decree requires that where personal information is sold or shared through SDKs, a *business's privacy policy* must provide "clear and conspicuous notice to consumers regarding its use of SDKs, including, without limitation, identification of the categories of SDKs, identification of the categories of personal information sold or shared through SDKs, and the business or commercial purpose for selling or sharing the personal information." This clarification is a relatively high bar for SDK specificity.

  Going further, the settlement also requires the Company in this case to implement and maintain a "*SDK governance framework*," including identification of each SDK in a children-directed app (name and third-party provider); the purpose for each SDK's use; evaluation of the configuration settings and controls for each SDK's collection, use or disclosure of personal information; evaluation of the contract governing any SDK that involves collection of children's personal information; and documentation of sell/share compliance. *Data minimization* in relation to SDKs is stressed by the enforcers as well, such that the Company must "at least annually conduct an assessment of its data minimization efforts and its SDK

governance framework," ensuring appropriate testing of data flows and conducting adequate training of relevant employees on configuration and use of the SDKs.

- **Be Aware of the General Characteristics of Kid-Directed Content—And Don't Willfully Disregard a Consumer's Age, or Else.** Although reference is made to the COPPA Rule's stated elements for determining whether an online service is directed to children for purposes of COPPA (16 C.F.R. section 312.2), the enforcers in this case summarized the child-focused nature of the App by noting that "the visual content, use of animated characters and fun background music, as well as the simplistic nature of gameplay, make the game simple and basic for consumers under the age of 13," notwithstanding the older teens and adults also targeted by the App. Companies whose online content, games or services would seem to align with such a description should take note and ensure a vigorous children's privacy and parental consent program. The enforcers further reminded readers in the complaint that "a business that *willfully disregards* the consumer's age is deemed to have actual knowledge of the consumer's age," reinforcing that turning a blind eye to a consumer's age will lead to negative inferences by regulators. It is also the case that an *age-limit set forth in an applicable terms of use is not enough* to overcome knowledge of underage children's use or an app being directed to kids.
- **Use Age Screens in a Neutral, Privacy-Proactive Default Manner—Especially in Mixed Audience Services.** In this case, when the App was first available in 2020, an initial screen asked users to select their birthday—starting with the year 1953 by default. This meant that users under the age of 13 needed to scroll through more than 50 years to find an accurate, underage birth. The enforcers found that "the non-neutral age gate likely biased consumers under age 13 to identify as adults" rather than be directed to a child-version of the game.

  The settlement also clarifies that when using an age screen in a *mixed audience app*, businesses should not collect personal information from *any* consumer prior to collecting age information. Such businesses should also *not default to an age-screening mechanism that defaults to a set age of 16* or above (thereby encouraging users to falsify age information) and not suggest that certain features will not be available for users who identify as younger than 16.
- **Steer Clear of Dark Pattern-Like Deceptive Ad Tactics.** The enforcers took issue with the App having advertisements with "unclear methods to exit the ads," blurred lines between advertising and gameplay (especially given the child-directed nature of the App), the forced downloading of unnecessary other mobile applications, and the display of some ads that they deemed were inappropriate for child audiences, such as for a gambling app and a marijuana-growing game.

  Businesses should consider working with their ad operations teams or agencies to ensure that ads are labelled as such; full-screen video ads have clear exit methods; display ads can be stopped or dismissed without a player having to engage with an ad or download unnecessary apps; manipulative designs are not used that cause children to "inadvertently or unknowingly engage with" ads or third-party apps; and age-inappropriate ads are not displayed in apps directed to kids or mixed audiences. The enforcers viewed these practices as violative and therefore have placed others on notice that it may do so again.
- **Don't Let Your Guard Down Once a Self-Regulatory Investigation Is Complete—It May Provide the Basis for Other Investigations or Further Claims of Deception If Promised Remediations Are Not Made.** This case serves as a reminder that the closing of an investigation does not necessarily end the matter entirely. On the contrary, here, *it was not until CARU completed its investigation that the OAG began inspecting* the Company's compliance with children's privacy laws. In particular, when a company that has been

investigated—whether by a self-regulatory body like the BBB's CARU arm, or by a state's attorney general—agrees to implement changes and then does not do so, as the enforcers claim here following the CARU investigation, it may strengthen other regulators' or prosecutors' resolve against the organization, or even provide further claims under the state's unfair and deceptive acts and practices (UDAP) statutes. The OAG mentions in this case that the Company did not identify or resolve its misconfiguration of SDKs, even after receiving CARU's report, a fact that the enforcers did not view favorably.

- **Clarify Privacy Policy Wording.** The enforcers dinged the Company for its privacy policy being "ambiguous and incomplete regarding the use of personal information for targeted and behavioral advertising," in particular in relation to children's data and via the use of SDKs. Here, the Company did not disclose in its privacy policy that it sells or shares personal in connection with targeted or behavioral advertising, and nor did it describe the CCPA's "opt-in" regime in relation to selling or sharing the personal information of consumers under the age of 16 (or parental consent when under 13).

  Note, as well, that the OAG clarified in the stipulated final judgment that "personal information" included not just "persistent identifiers" and the items listed in the COPPA Rule's definition but also terms from the CCPA, such as "unique identifier," or "unique personal identifier." Reference was also made in the settlement to complying with the separate "CalOPPA" privacy policy disclosures law. As such, this case saw the merging of multiple definitions across the applicable laws, further broadening the reach and scope of such investigations.

Conclusion

In light of the depth of the enforcers' investigation and the reach of their settlement—including a half-million dollar fine, required updated disclosures to children and parents, and the imposition of a compliance, monitoring and enforcement program (with annual assessments) for a period of three years—businesses potentially subject to COPPA or the CCPA should consider reviewing the above to look for potential areas of improvement within their own privacy programs. The case represents yet another example of children's privacy being a major focus of federal, state, and international privacy regulators, extending this explicitly to the mobile app and SDK context, where historically less attention has been paid in comparison to web-based advertising and data collection.

National Law Review, Volume XIV, Number 178