

UNITED STATES DISTRICT COURT
DISTRICT OF NEW MEXICO

STATE OF NEW MEXICO *EX REL.*
HECTOR BALDERAS, ATTORNEY
GENERAL,

The State,

v.

TINY LAB PRODUCTIONS; TWITTER
INC.; MOPUB, INC.; GOOGLE, INC.;
ADMOB, INC.; AERSERV LLC;
INMOBI PTE LTD.; APPLOVIN
CORPORATION; and
IRONSOURCE USA, INC.

Defendants.

Case No. _____

COMPLAINT

DEMAND FOR JURY TRIAL

COMES NOW, the State of New Mexico, by Attorney General Hector Balderas (“the State”), who brings this Complaint against Defendants Tiny Lab Productions (“Tiny Lab”), Twitter, Inc., MoPub, Inc., Google, Inc., AdMob, Inc., AerServ LLC, InMobi PTE Ltd., AppLovin Corporation, and ironSource USA (collectively “Defendants”), and alleges as follows:

I. INTRODUCTION

1. This action is brought to protect children in the State of New Mexico from Defendants’ surreptitious acquisition of their personal information for the purposes of profiling and targeting them for commercial exploitation.

2. Defendants design, develop, and/or market mobile gaming applications (“apps”) expressly for children. When children play Tiny Lab’s gaming apps on their mobile devices, their geolocation, demographic characteristics, online activity, and other personal data, are inescapably—and without verifiable parental consent—exfiltrated to third parties and their marketing networks in order to target the children with advertisements based on their own

personal information. This conduct endangers the children of New Mexico, undermines the ability of their parents to protect children and their privacy, and violates state and federal law.

3. Defendants are app developer Tiny Lab and advertising companies that Tiny Lab works with in its child-directed apps: Twitter, MoPub, Inc., Google, Inc., AdMob, Inc., AerServ LLC, InMobi Pte Ltd., AppLovin Corporation, and ironSource USA (together, “SDK Defendants”). The apps at issue here are—in substance, style, and marketing—clearly and indisputably designed for children. Their names alone reflect their appeal to children, including toddlers: Fun Kid Racing, Candy Land Racing, Baby Toilet Race: Cleanup Fun, and GummyBear and Friends Speed Racing.¹

4. Alarming, Tiny Lab’s CEO states that it is precisely *because* the company’s apps are directed at children that it engages in tracking and user profiling. In an interview, he laments the difficulty of monetizing children, stating “there is a low buying power of our players who are mainly under 13 years old. It’s hard to convince them to spend their money on additional game items or levels as most of them have to ask their parents for the purchase.”² Accordingly, the company relies on in-app advertising fueled by surreptitious data collection.

5. While children and their parents think that the Tiny Lab Gaming Apps games are innocent, online games—the digital equivalent of puzzles, blocks, or books—Defendants have embedded coding in the apps that allows them to exfiltrate children’s data as they play. These bits of coding are called software development kits (or “SDKs”). Tiny Lab and each SDK Defendant work together to place the SDKs in the Gaming Apps. Once embedded, the SDKs allow the app to communicate directly with the advertising companies (the SDK Defendants),

¹ This list is a subset of all of the Tiny Lab child apps at issue in this complaint. For a full list of all applicable apps, see Exhibit 1, attached hereto. Together, these games are referred to here as “Gaming Apps.”

² *Tiny Lab Productions: Subscription Model Sounds Promising*, Startup Lithuania (Oct. 18, 2016) (available at <https://www.startuplithuania.com/news/tiny-lab-productions-subscription-model-sounds-promising/>) (accessed on Sept. 4, 2018).

sending data and advertisements back and forth. The SDK sends the child's data back to the SDK Defendants, where it is analyzed, stored, and used to build increasingly-detailed profiles of child users. It is also shared with and sold to myriad third-parties so that each can continue to build their own profiles. All of this activity serves one primary purpose: to learn more about the child in order to send her highly-targeted advertisements.

6. Federal law prohibits this very conduct. Recognizing the potential harms that sophisticated advertising could inflict upon children, the United States Congress enacted the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501, *et seq.* ("COPPA"). COPPA empowers parents—through enforcement actions brought by a State Attorney General or the FTC—to protect their children in the online marketplace. COPPA prohibits websites or online services from collecting personal information from children under the age of 13 without first obtaining verifiable parental consent. Specifically, COPPA requires websites and online services (1) to provide complete disclosure of the information they collect from children and how they use that information, (2) to ensure that disclosure is provided *directly* to parents, and (3) to obtain verifiable consent from the parent *before* collecting, using, or disclosing any personal information from children. Without first complying with these requirements, the online tracking of children is illegal. Defendants have violated all these mandates of COPPA.

7. Despite the requirements of COPPA, Defendants exfiltrate the personal information of children who play their apps—the very audience for whom the apps are designed—and use that data for commercial gain, all the while neglecting to obtain verifiable parental consent for their activities. This conduct is condoned by Defendant Google, which fraudulently facilitates and furthers Tiny Lab's marketing of its apps as being safe and appropriate for children in Google's app marketplace (the Google Play Store). Meanwhile, Google knows that Tiny Lab's apps track children unlawfully. Google's bad acts are compounded because it represents to parents and guardians that Tiny Lab's apps are *compliant*

with COPPA—despite express knowledge that this is not true—and safe for children. Indeed, Google itself is one of the SDK Defendants whose embedded coding tracks and profiles children.

8. Forensic testing reveals that the SDK Defendants’ software embedded in Tiny Lab’s gaming apps collect highly-sensitive personal data, including a child’s *precise location within +/- 5 meters, constantly updated*. The Supreme Court recently warned just how revealing location data can be. *See Carpenter v. United States*, 138 S. Ct. 2206 (2018). As Chief Justice John Roberts stated, “a cell phone—almost a ‘feature of human anatomy[.]’—tracks nearly exactly the movements of its owner....A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales,” and when a third-party has access to the information stored on one’s cell phone, that entity “achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.” *Id.* at 2218 (internal citations omitted).

9. The risks associated with exfiltration of personal data, including but not limited to location data, apply with greatest force when the privacy of children is at stake. Children have a long- and widely-recognized vulnerability which can be—and here is—exploited through the immediacy and ease with which information can be collected from them, and the ability of the online medium—including apps on smartphones and tablets—to circumvent the traditional gatekeeping role of their parents and guardians. Children also have a more difficult time differentiating between advertisements and content, a risk exacerbated by the highly-targeted nature of behavioral advertising.

10. The above acts and practices violate COPPA; violate New Mexico’s Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-1, *et seq.*; and are acts of intrusion upon seclusion.

II. PARTIES

11. This action is brought for and on behalf of the sovereign State of New Mexico, by and through its duly elected Attorney General, Hector Balderas. The Attorney General, as chief

legal officer of the State, is statutorily authorized to initiate and prosecute any and all suits deemed necessary for the protection of the interests and rights of the State. Specifically, the Attorney General is authorized to initiate and prosecute suits to penalize conduct that constitutes an unfair or deceptive trade practice. The Attorney General is also charged with the duty of guardian of the public interest, which includes protecting the privacy interests of New Mexico's citizens and the welfare of New Mexico's children online. The State brings this action in its *parens patriae* and/or sovereign capacity.

The Developer Defendant

12. Defendant Tiny Lab Productions ("Tiny Lab") is a commercial mobile game development company headquartered at Studentu g. 67, Kaunas, Lithuania. Since at least 2012, with the release of its Fun Kid Racing app, Tiny Lab has engaged in the business of developing and publishing numerous gaming apps for children to download in the Google Play Store and the Apple App Store, and markets these apps, including by working with advertisers, contracting with ad networks (as defined *infra*), embedding advertisers' software into its apps, and integrating social media platforms into its apps.

The SDK Defendants

13. The "SDK Defendants"—identified in paragraphs 14 through 18 below—are entities which provided their own proprietary computer code to Developer Defendant Tiny Lab, known as SDKs, for installation and use in Tiny Lab's Gaming Apps.³ Tiny Lab embedded each of the SDK Defendants' SDKs into its Gaming Apps, causing the transmittal of children's Personal Data—including in the form of persistent identifiers—to the SDK Defendants to facilitate subsequent tracking, profiling, and targeting. As used herein, "Personal Data" is any

³ See Exhibit 1.

data that refers to, is related to, or is associated with an identified or identifiable individual. This includes, but is not limited to, all “Personal Information” as defined in 12 C.F.R. § 312.2.

14. SDK Defendant Twitter, Inc. (“Twitter”) is an American technology company headquartered at 1355 Market Street Suite 900, San Francisco, California 94103. SDK Defendant MoPub, Inc. (“MoPub”) is Twitter’s “mobile-focused advertising exchange, which combines ad serving, ad network mediation and a real-time bidding exchange into one comprehensive monetization platform”⁴ and is located at the same address. Twitter and MoPub are collectively referred to as “Twitter/MoPub” in this Complaint. Twitter/MoPub owns and operates the Twitter/MoPub SDK, which was embedded in the Fun Kid Racing app (as well as other Gaming Apps)⁵ at some point during or after 2012 and has remained embedded until at least version 3.1, which was published on August 29, 2017. On May 29, 2018, MoPub filed a Certificate of Surrender with the California Secretary of State.

15. Defendant Google, Inc. (“Google”) is an American technology company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. Google operates the Google Play app store, through which Tiny Lab’s Gaming Apps are or have been marketed to consumers. Additionally, SDK Defendant AdMob, Inc. (d/b/a AdMob by Google)⁶ (“AdMob”) is Google’s mobile advertising unit, which owns and operates the AdMob SDK, which was embedded in the Fun Kid Racing app (as well as other Gaming Apps) at some point

⁴ Twitter, Inc. Form 10-K Annual Report, filed December 31, 2017, at p. 7 (*available at* https://www.sec.gov/Archives/edgar/data/1418091/000156459018003046/twtr-10k_20171231.htm) (accessed on Sept. 4, 2018).

⁵ The Complaint uses Tiny Lab’s Fun Kid Racing app as its exemplar, since this is Tiny Lab’s flagship app and is the most ubiquitous of the Gaming Apps. However, investigation demonstrates that the Gaming Apps are designed similarly to (and function similarly to) Fun Kid Racing, and include SDKs embedded therein, for the same purposes.

⁶ *AdMob by Google*, Google (*available at* <https://www.google.com/admob/>) (accessed on Sept. 4, 2018).

during or after 2012 and has remained embedded until at least version 3.46, which was published on June 27, 2018.

16. SDK Defendant AerServ LLC (“AerServ”) is a technology company headquartered at 15420 Laguna Canyon Rd., Irvine, CA 92618. AerServ was acquired by SDK Defendant InMobi Pte Ltd. (“InMobi”), a technology company with offices throughout the world and headquarters located at 30 Cecil Street # 19-08, Prudential Tower, Singapore 049712. AerServ and InMobi jointly administer the AerServ SDK, which was embedded in the Fun Kid Racing app (as well as other Gaming Apps) at some point during or after 2012 and has remained embedded until at least version 3.46, which was published on June 27, 2018. AerServ and InMobi jointly operate what they characterize as the online advertising industry’s “first mediation platform with a unified programmatic auction for mobile in-app publishers.”⁷ In so doing, and through technology including the AerServ SDK, AerServ and InMobi jointly endeavor to “enhance monetization for publishers globally and further enhance the InMobi Exchange, a premium mobile programmatic platform.”⁸

17. SDK Defendant AppLovin Corporation is an American technology company with offices throughout the world, engaged in the business of facilitating targeted advertising, including through the AppLovin SDK described herein, which was embedded in the Fun Kid Racing app (as well as other Gaming Apps) at some point during or after 2012 and has remained embedded until at least version 3.46, which was published on June 27, 2018. AppLovin’s headquarters are located at 640 2nd Street, San Francisco, CA 94107.

⁷ *InMobi Acquires Los Angeles Based AerServ for \$90 Million to Create World’s Largest Programmatic Video Platform for Mobile Publishers*, InMobi (Jan. 10, 2018) (available at <https://www.inmobi.com/company/press/inmobi-acquires-los-angeles-based-AerServ-for-90-million>) (accessed on Sept. 4, 2018).

⁸ *Id.*

18. SDK Defendant ironSource USA, Inc. (“ironSource”) is an American technology company headquartered at 17 Bluxome Street, San Francisco, CA 94107. SDK Defendant ironSource owns and operates the Supersonic SDK, which was embedded in the Fun Kid Racing app (as well as other Gaming Apps) at some point during or after 2012 and has remained embedded until at least version 3.46, which was published on June 27, 2018.

III. JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1367.

20. This Court has personal jurisdiction over each Defendant pursuant to N.M. Stat. Ann. § 38-1-16 because each Defendant engages in consumer transactions within the State of New Mexico, purposefully directs and/or directed its actions toward the State of New Mexico, tracks children by siphoning geolocation, persistent identifiers, and/or other Personal Data as they play Tiny Lab’s gaming apps in, and move about, New Mexico, and/or has the requisite minimum contacts within the State of New Mexico needed to permit this Court to exercise jurisdiction.

21. In accordance with 28 U.S.C. § 1391, venue is proper in this district because a substantial part of the conduct giving rise to the State’s claims occurred in this District, and because Defendants transact business in this District.

IV. ALLEGATIONS APPLICABLE TO ALL COUNTS

A. COPPA Outlaws the Collection of Personal Information of Children Under Age 13 Without Verifiable Parental Consent.

22. Children are especially vulnerable to online tracking and the resulting behavioral advertising and user profiling. As children’s cognitive abilities are still developing, they have limited understanding and awareness of sophisticated advertising and are therefore less likely than adults to distinguish between the actual content of online gaming apps and the advertising

content that is targeted to them alongside it. Thus, children may engage with advertising content without realizing they are doing so.⁹

23. Recognizing the vulnerability of children in the Internet age, Congress enacted COPPA, the express goal of which is to protect children's privacy while they are connected to the Internet.¹⁰ Under COPPA, developers of child-focused apps, and any third-parties working with these app developers, cannot lawfully obtain the Personal Information of children under 13 years of age without first obtaining verifiable consent from their parents. As discussed in further detail below, such consent must be informed and meaningful—COPPA requires more than checking a box in a “clickwrap” agreement¹¹ or posting an inconspicuous hyperlink to a privacy policy that a user may or may not peruse. Instead, there must be a strong, objective record of a parent's consent to her child being tracked.

24. COPPA applies to any operator of a commercial website or online service (including an app) that is directed to children and that: (a) collects, uses, and/or discloses Personal Information from children under 13, or (b) on whose behalf such information is collected or maintained. Under COPPA, Personal Information is “collected or maintained on behalf of an operator when . . . [t]he operator benefits by allowing another person to collect personal information directly from users of” an online service. 16C.F.R. § 312.2. In

⁹ Comments of The Center for Digital Democracy, et al., FTC, *In the Matter of Children's Online Privacy Protection Rule* at 13-14 (Dec. 23, 2011).

¹⁰ *New Rule Will Protect Privacy of Children Online*, Federal Trade Commission (Oct. 20, 1999) (available at <https://www.ftc.gov/news-events/press-releases/1999/10/new-rule-will-protect-privacy-children-online>) (accessed on Sept. 4, 2018).

¹¹ Clickwrap agreements require a user to affirmatively click a box on a website acknowledging agreement to the terms of service before the user is allowed to proceed. *See, From the Chair: 'Click Here to Accept the Terms of Service,'* American Bar Association Communications Lawyer Newsletter, Vol. 31 No. 1 (January 2015) (available at https://www.americanbar.org/publications/communications_lawyer/2015/january/click_here.html) (accessed on Sept. 4, 2018).

addition, COPPA applies to any operator of a commercial website or online service that has actual knowledge that it collects, uses, and/or discloses Personal Information from children under 13.

25. Under COPPA, “Personal Information” includes more traditional, pre-Internet information like names, physical addresses, telephone numbers, and social security numbers, but it also includes “persistent identifier[s] that can be used to recognize a user over time and across different Web sites or online services.” 16 C.F.R. § 312.2. COPPA’s broad definition of “Personal Information” is as follows:

“individually identifiable information about an individual collected online,” which includes (1) a first and last name; (2) a physical address including street name and name of a city or town; (3) online contact information (separately defined as “an email address or any other substantially similar identifier that permits direct contact with a person online”); (4) a screen name or user name; (5) telephone number; (6) social security number; (7) a media file containing a child’s image or voice; (8) geolocation information sufficient to identify street name and name of a city or town; (9) a “persistent identifier that can be used to recognize a user over time and across different Web sites or online services” (including but not limited to “a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier”); and (10) any information concerning the child or the child’s parents that the operator collects then combines with an identifier.

Id. Persistent identifiers and geolocation are the “Personal Information” of greatest value and utility for the purpose of tracking, profiling, targeting, and monetizing children and others generally on the Internet.

26. The FTC regards “persistent identifiers” as “personally identifiable” information that can be reasonably linked to a particular child. The FTC amended COPPA’s definition of “Personal Information” to clarify the inclusion of persistent identifiers.¹²

27. In order to lawfully collect, use, or disclose Personal Information (including geolocation and persistent identifiers), COPPA requires that an operator meet specific requirements, including *each* of the following:

- i. Posting a privacy policy on its website or online service providing clear, understandable, and complete notice of its information practices, including what information the website operator collects from children online, how it uses such information, its disclosure practices for such information, and other specific disclosures as set forth in the Rule;
- ii. Providing clear, understandable, and complete notice of its information practices, including specific disclosures, directly to parents; and
- iii. Obtaining verifiable parental consent prior to collecting, using, and/or disclosing Personal Information from children.

28. Under COPPA, “[o]btaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child. . . [r]eceives notice of the operator’s personal information collection, use, and disclosure practices; and [a]uthorizes any collection, use, and/or disclosure of the personal information.” 16 C.F.R. § 312.2.

29. The FTC recently clarified acceptable methods for obtaining verifiable parental consent, which include: (i) providing a consent form for parents to sign and return; (ii) requiring

¹² *Keeping Up With the Online Advertising Industry*, Federal Trade Commission (Apr. 21, 2016) (available at <https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry>) (accessed on Sept. 4, 2018).

the use of a credit card/online payment that provides notification of each transaction; (iii) connecting to trained personnel via video conference; (iv) calling a staffed toll-free number; (v) emailing the parent soliciting a response email plus requesting follow-up information from the parent; (vi) asking knowledge-based questions; or (vii) verifying a photo ID from the parent compared to a second photo using facial recognition technology.¹³

B. Defendants Surreptitiously Exfiltrate Children's Personal Data While They Play Tiny Lab's Gaming Apps.

1. Tiny Lab

30. Tiny Lab styles and promotes its Gaming Apps as fun, free, kid-focused games. The Gaming Apps are available for download in online stores, including Google's "Play Store." To date, Tiny Lab has marketed at least 91 such Gaming Apps. A complete list is attached as Exhibit 1.

31. Tiny Lab markets its Gaming Apps to parents as games that are expressly to be played by their children, and Google presents these apps with an "Everyone" rating in its Google Play Store. Google Play ratings "are intended to help consumers, especially parents, identify potentially objectionable content that exists within an app" and are based on the app developer's responses to questionnaires provided by Google—*i.e.* the ratings reflect the developer's representations about the appropriate audience for the app.¹⁴ An "Everyone" rating means the app's content is "generally suitable for all ages" and "[m]ay contain minimal cartoon, fantasy or mild violence and/or infrequent use of mild language."¹⁵

¹³ *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, Federal Trade Commission (available at <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>) (accessed on Sept. 4, 2018).

¹⁴ *Play Console Help*, Google (available at <https://support.google.com/googleplay/android-developer/answer/188189?hl=en>) (accessed on Sept. 4, 2018).

¹⁵ *Id.*

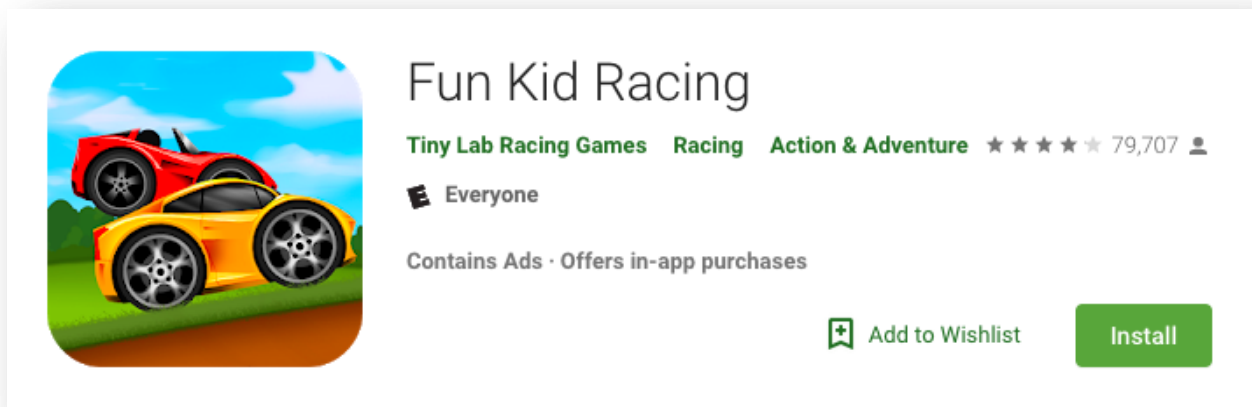


Figure 1¹⁶

As just one example, Fun Kid Racing players guide an assortment of cartoonish cars along a variety of race courses. A product description on Amazon, provided by Tiny Lab, describes the app as [*sic* throughout]:

One of the best simple and fun racing games for kids! This free game is made for 2 - 10 years children. Choose your ride and guide it to the finish line! . . . Other racing games become boring for your kid because of hard levels or controls? This is what you were looking for! . . . Even a toddler can play this game without any problems! . . . The tracks are designed so that kids would do many stunts on the run, the car will spin doing frontflip, backflip or even both - but watch out not to land on the roof! The comic cars reminds the toys and child-friendly soundtrack makes the mood ready for the awesome ride!¹⁷

2. Twitter/MoPub

32. MoPub is Twitter’s “mobile-focused advertising exchange, which combines ad serving, ad network mediation and a real-time bidding exchange into one comprehensive monetization platform.”¹⁸ MoPub “provides monetization solutions for mobile app publishers

¹⁶ Figure 1 is a picture of the Fun Kid Racing app as advertised in the Google Play Store, as of August 8, 2018.

¹⁷ *Fun Kid Racing*, Amazon.com (available at <https://www.amazon.com/Tiny-Lab-Productions-Fun-Racing/dp/B014T39TKA>) (accessed on Sept. 4, 2018).

¹⁸ Twitter, Inc. Form 10-K Annual Report, filed December 31, 2017, at p. 7 (available at

and developers around the globe.”¹⁹ MoPub enables app developers to profit from targeted advertising, including through its use of its programmatic (or real time bidding “RTB” platform), the MoPub Marketplace.²⁰ An RTB platform enables the automated buying and selling of mobile ads “in an auction environment,”²¹ using sophisticated algorithms that allow instantaneous buying and selling. MoPub functions like a matchmaker, where it uses data to “target the right inventory [mobile ads] with the right mobile ad network partner.”²² In turn, the ads served on mobile apps are “based on rich data signals to increase yield on every impression [advertisement]” and maximize an app developer’s advertising revenue.²³

33. Twitter/MoPub is able to serve its matchmaking function due to the ubiquity of its SDK. MoPub states that it works with more than 50,000 mobile apps on more than 1.5 billion mobile devices²⁴ and services 450 billion monthly app advertisement requests.²⁵ By relying on its wealth of personal data, including data obtained from third-parties, MoPub gives advertisers “access to rich and unique data, enhancing their targeting abilities.”²⁶

https://www.sec.gov/Archives/edgar/data/1418091/000156459018003046/twtr-10k_20171231.htm) (accessed on Sept. 4, 2018).

¹⁹ MoPub website homepage (available at <https://www.MoPub.com/>) (accessed on Sept. 4, 2018).

²⁰ *MoPub Marketplace*, MoPub (available at <https://www.MoPub.com/marketers/marketplace/>) (accessed on Sept. 4, 2018).

²¹ *Id.*

²² *MoPub’s Platform Maximizes Your Revenue*, MoPub (available at <https://www.MoPub.com/publishers/platform/>) (accessed on Sept. 4, 2018).

²³ *Id.*

²⁴ *MoPub Marketplace*, *supra* at n.20.

²⁵ *Our History*, MoPub (available at <https://www.MoPub.com/company/history/>) (accessed on Sept. 4, 2018).

²⁶ *Confidently Reach Your Audience in Mobile Apps*, MoPub (available at <https://www.MoPub.com/dsp/platform/>) (accessed on Sept. 4, 2018).

3. Google/AdMob

34. The AdMob SDK is incorporated into over one million apps, facilitating 200 billion ad requests per month, and paying developers over \$3.5 billion since July 2012.²⁷ The AdMob SDK is “[p]owered by Google’s ad technology”²⁸ and enables developers “to segment...users, then view reports to understand which ones are earning [the developers] the most revenue.”²⁹ AdMob’s website promises developers that “[w]hen you monetize with AdMob you get instant access to all of Google’s demand sources. This includes a million Google advertisers as well as real-time bidding (RTB) buyers via the DoubleClick Ad Exchange.”³⁰ As discussed in paragraph 32 above, RTB is synonymous with targeted advertising, and relies on user profiling.

4. InMobi/AerServ

35. InMobi is a mobile advertising company. On its website, InMobi claims that its advertising platform helps brands “engage mobile users across different stages of their lifecycle” by “turn[ing] every mobile moment into an opportunity to drive user engagement and uplift [return on advertising spending] and monetization.”³¹ InMobi offers businesses the ability to target those users who are most likely to respond to a particular commercial ad through targeted advertising.

36. According to its website, InMobi “combine[s] first, second, and third party data to create a holistic user graph, laying the foundation for the advanced targeting capabilities we

²⁷ *AdMob by Google*, Google (available at <https://www.google.com/admob/>) (accessed on Sept. 4, 2018).

²⁸ *Why AdMob? – Platform Benefits*, Google (available at <https://www.google.com/admob/platform.html>) (accessed on Sept. 4, 2018).

²⁹ *Id.*

³⁰ *Why AdMob? – Monetize*, Google (available at https://www.google.com/admob/monetize.html#?monetize-tabset_activeEl=overview) (accessed on Sept. 4, 2018).

³¹ *AerServ + InMobi*, InMobi (available at <https://www.inmobi.com/>) (accessed on Sept. 4, 2018).

offer.”³² InMobi’s targeted advertising capabilities include promoting an app to users “based on their app interests” and “target[ing] users based on demographics, location, context, behavior & interest” to reach the most relevant users.³³ InMobi can also collect location data, with which it claims it can “target their [brands’] audiences beyond just latitude or longitude. With 100% control on 1st party location data collected through our in-app SDK, we leverage verified location signals to deliver the best geo-targeted campaigns.”³⁴ InMobi “translate[s] [latitude/longitude] data into known places of interest: airport, supermarkets, banks & more.”³⁵ However, InMobi faced a regulatory enforcement action as a result of these location-tracking practices.³⁶

37. InMobi and AerServ work jointly through technologies that include the AerServ SDK in order to serve ads (and track and profile children) in mobile apps. InMobi’s ad-serving scale increased through its 2018 purchase of AerServ, according to a press release announcing the event.³⁷ This increase in scale is due to the fact that “AerServ runs more than 90 billion ad

³² *Acquire Quality Users Efficiently and Drive App Installs at Scale*, InMobi (available at <https://www.inmobi.com/advertisers/user-acquisition/>) (accessed on Sept. 4, 2018).

³³ *Id.*

³⁴ *Precision Targeting for Higher User Quality*, InMobi available at <https://www.inmobi.com/products/targeting>) (accessed on June 4, 2018).

³⁵ *Id.*

³⁶ InMobi entered into a consent decree in June 2016 with the Federal Trade Commission, to settle claims for violation of the Federal Trade Commission Act and COPPA, as a result of its tracking technology. The FTC alleged that InMobi tracked the locations of hundreds of millions of consumers, including children, without consent. The consent decree required InMobi to, *inter alia*, obtain affirmative express consent before collecting consumer’s location information. In relation to the consent decree, the Director of the FTC’s Bureau of Consumer Protection stated, “This settlement ensures that InMobi will honor consumers’ privacy choices in the future, and will be held accountable for keeping their privacy promises.” *Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers’ Locations Without Permission*, Federal Trade Commission (June 22, 2016) (available at <https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked>) (accessed on Sept. 4, 2018).

³⁷ *InMobi Acquires Los Angeles Based AerServ for \$90 Million to Create World’s Largest Programmatic Video Platform for Mobile Publishers*, InMobi (Jan. 10, 2018) (available at <https://www.inmobi.com/company/press/inmobi-acquires-los-angeles-based-AerServ-for-90->

opportunities each month and provides access to brand programmatic demand to over 2,000 mobile apps.”³⁸ The announcement further explains that the “acquisition fits in perfectly with [InMobi’s] global strategy to bring best-in-class technology for premium publishers and driving mobile programmatic video revenues to them.”³⁹ The “combined entities will double [their respective] headcount in the U.S. while establishing a product and tech hub for InMobi in Los Angeles, a hotspot of innovation for media and video content.”⁴⁰ Per Abhay Singhal, co-founder and Chief Revenue Officer at InMobi. “We are two profitable companies combining forces in North America and this will further cement our leadership position in video advertising[.]”⁴¹

5. AppLovin

38. AppLovin is a mobile advertising company that owns and operates its own SDK. Per the company’s website, “[w]hen you integrate our SDK, you immediately have the ability to use our self-serve platform. Reach your ideal users and continuously optimize for greater ROI – all in one place.”⁴² AppLovin concerns itself with “[d]esigning, building, and operating the fabric that connects game developers of all sizes with their ideal consumers around the globe,”⁴³ and its “platform gives game developers of all sizes the ability to monetize, grow, and even finance their businesses.”⁴⁴ AppLovin touts its ability to track and profile users, telling prospective developer customers “[t]he better information you have, the closer you get to the prize.”⁴⁵

[million](#)) (accessed on Sept. 4, 2018)

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Monetize With Us*, AppLovin (available at <https://www.applovin.com/monetize/>) (accessed 4).

⁴³ *About*, AppLovin (available at <https://www.applovin.com/about/>) (accessed on Sept. 4, 2018)

⁴⁴ *Id.*

⁴⁵ *Game on: three steps to successful retargeting*, AppLovin (Apr 18, 2014) (available at <https://blog.applovin.com/game-on-three-steps-to-successful-retargeting/>) (accessed on Sept. 4,

6. ironSource

39. ironSource is a mobile advertising company that helps developers “turn their digital content into viable businesses without having to charge for them.”⁴⁶ In other words, it helps developers who want to offer free apps make money through advertising revenue. ironSource does this by using data to target potential app customers (it calls this “multi-touchpoint data targeting”)⁴⁷ and by providing ads for placement inside the app, telling developers it can provide “[o]ne of the industry’s largest in-app ad networks leveraging all available ad units to drive revenue and user engagement.”⁴⁸

40. ironSource selects and places ads based on specific user data; ironSource states that “users are unique, and each will respond to a different mix of ad units.”⁴⁹ ironSource is able to obtain this data through its large digital footprint. Indeed, ironSource claims that it serves three billion ads every month to nearly 1 billion users.⁵⁰

41. ironSource aggregates the information it collects through its SDK with information provided by publishers or developers, that said publishers and developers “may [have] separately collected” about the user, and further acknowledges sharing *this* bundled information with advertisers, developers, and publishers.⁵¹

2018).

⁴⁶ *We’re all-in Players*, ironSource, (available at <https://www.ironsrc.com/about/>) (accessed on June 4, 2018).

⁴⁷ *Networks – ironSource*, Annecy (available at <https://www.annecy.media/networks/ironsource>) (accessed on June 4, 2018).

⁴⁸ *Powering the App Economy*, ironSource (available at <https://company.ironsrc.com/developer-solutions/>) (accessed on Sept. 4, 2018).

⁴⁹ *Monetization Never Looked So Good*, ironSource, available at <https://www.ironsrc.com/for-developers/ad-units/> (accessed on June 4, 2018).

⁵⁰ *Welcome to the New Primetime*, ironSource, (available at <https://www.ironsrc.com/for-advertisers/brand-awareness/>) (accessed on June 4, 2018).

⁵¹ *ironSource Mobile Privacy Policy*, ironSource (available at <https://web.archive.org/web/20170927162013/https://developers.ironsrc.com/ironsource-mobile/android/ironsource-mobile-privacy-policy/>) (accessed on Sept. 4, 2018).

42. ironSource also helps apps make money off of their current users by using player data and providing “user-level insight and ad engagement intelligence to fully understand how [app] users are being monetized.”⁵² ironSource’s SDK allows developers to target individual users—based on demographics derived from their data—in specific locations for specific results, as shown in Figure 2 below. This figure demonstrates how advertisers can select a particular demographic—*e.g.*, a female between ages 25 and 30—and select a specific action they would like her to take—*e.g.*, make an in-game purchase, install an app, or get to a certain level on an app—and a geographic location. The ironSource SDK can use all of the data it has collected to find users that its algorithms determine best fit that description, live in that area, and are likely to be influenced to take that action, and serve an ad to those users through the ironSource SDK.

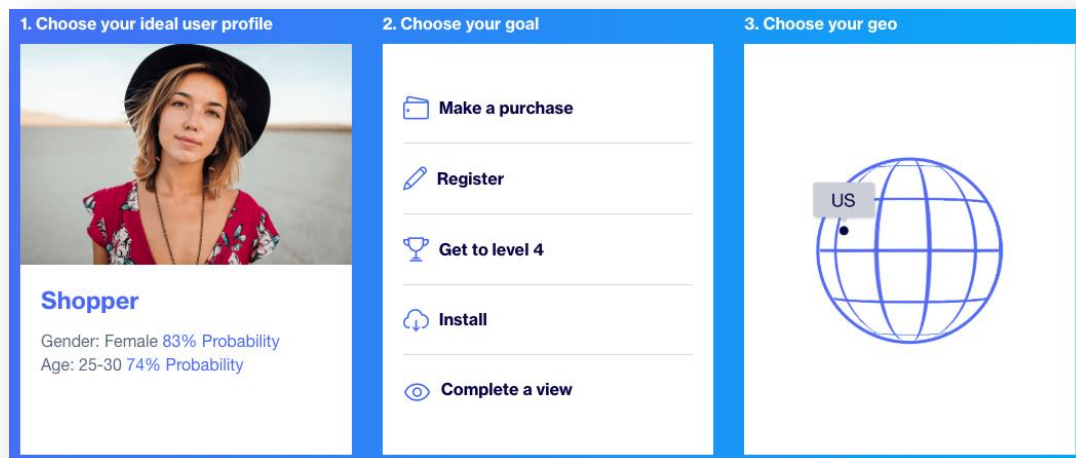


Figure 2⁵³

⁵² *Drive maximum revenue with minimum effort*, ironSource, available at <https://www.ironsrc.com/for-developers/mediation/> (accessed on June 4, 2018).

⁵³ Figure available at <https://www.ironsrc.com/for-advertisers/user-acquisition/> (accessed on June 4, 2018).

7. Defendants' Collective Role in the Unlawful Exfiltration of Children's Personal Data.

43. Unbeknownst to parents and their children, Tiny Lab, in partnership with the SDK Defendants, collects and exfiltrates Personal Data (including but not limited to geolocation and persistent identifiers) as children play Tiny Lab's Gaming Apps.

44. However, this exfiltration of children's Personal Data—done, for among other purposes, to track and profile the children—is undertaken without first obtaining verifiable parental consent. In point of fact, no effort is made to alert parents that their children's Personal Data is being harvested, much less an effort to obtain verifiable parental consent in a manner required by COPPA (such as the methods outlined in paragraph 29, *supra*).

45. Defendants fail to reasonably and meaningfully inform parents that, as children play the Gaming Apps, Defendants are surreptitiously collecting their Personal Data and tracking online behavior to profile children for targeted advertising. Certainly, parents are not asked to consent to these practices. This is all the more egregious given that COPPA does not just require *notice* in its compliance regime (which Defendants fail to provide in a reasonable and meaningful manner). COPPA also requires the separate, equally-critical component of verifiable parental consent. Defendants' obfuscation is all the more violative, accordingly.

46. As children play the Gaming Apps, the SDK Defendants' advertising software collects their Personal Data and, without the parent's knowledge or consent, exfiltrates the Personal Data to sophisticated advertising companies where it is used to track and profile children for targeted advertising.

47. Targeted advertising is driven by individuals' Personal Data and employs sophisticated algorithms that interpret the Personal Data to determine the most effective advertising for those individuals.⁵⁴ Once exfiltrated to SDK Defendants' servers, the Personal

⁵⁴ For a detailed discussion of targeted advertising, see Section IV.G.1, *infra*.

Data harvested from children playing the Gaming Apps can be combined with other data associated with those same children via persistent identifiers or by virtue of other data (*e.g.*, online activity or demographics) which can track and identify the children, individually. This is often accomplished via an ad network where additional data may be associated with the children in a similar fashion.

48. The ad network is also where the buying and selling of advertising space takes place. It is a virtual marketplace where app developers and advertisers buy and sell advertising space and the ads to fill it. These networks connect advertisers looking to sell data-driven, targeted ads to mobile apps that want to host advertisements. A key function of an ad network is aggregating available ad space from developers and matching it with advertisers' demands.

49. Using advanced, custom analytics and network analysis tools, the State has been able to: (1) determine that the SDK Defendants have their software embedded into Tiny Lab's Gaming Apps; (2) record network traffic as it leaves the device, including encrypted data; (3) detect the Personal Data that Defendants access in real time and exfiltrate from children's devices; and (4) identify the SDK Defendants that received Personal Data.

8. The Role of Persistent Identifiers

50. The most common data Defendants take from children's devices and use for tracking, profiling, and targeting are called persistent identifiers. These identifiers are a set of unique data points (typically numbers and letters), akin to a social security number, and can link one specific individual to all of the apps on her device and her activity on those apps, allowing her to be tracked over time and across devices (*e.g.*, smart phones, tablets, laptops, desktops and smart TVs).

51. The common persistent identifiers in Google's Android operating system are the Android Advertising ID ("AAID") and the Android ID. Both the AAID and Android ID are

unique, alphanumeric strings assigned to an individual device—and the individual who uses that device—in order to track and profile the user, and to serve her with targeted advertising.⁵⁵

52. A device’s International Mobile Equipment Identity (“IMEI”) is also a persistent identifier. An IMEI is a fixed, unique 15-digit serial number that is used to route calls to one’s phone and reflects information about the origin, model, and serial number of the device. A device has one fixed IMEI.

53. Additionally, each device can be identified by its “Device Fingerprint” data, which is another form of persistent identifier. Device Fingerprint data include myriad individual pieces of data about a specific device, including details about its hardware—such as the device’s brand (*e.g.*, Apple or Android), the type of device (*e.g.*, iPhone, Galaxy, iPad)—and details about its software, such as its operating system (*e.g.*, iOS or Android). This data can also include more detailed information, such as the network carrier (*e.g.*, Sprint, T-Mobile, AT&T), whether the device is connected to Wi-Fi, and the “name” of the device. The name of the device is often particularly personal, as the default device name is frequently configured to include children’s first and/or last names (*e.g.*, “Jane Minor’s iPhone”). In combination, the pieces of data comprising the Device Fingerprint provide a level of detail about the given device that allows that device and its user to be identified individually, uniquely, and persistently—as the appellation “Fingerprint” implies.

54. Defendants exfiltrate and analyze persistent identifiers—including, but not limited to, a child’s AAID, IMEI, Android ID, and/or Device Fingerprint data⁵⁶—in order to learn more

⁵⁵ The common persistent identifiers for Apple are the ID for Advertisers (“IDFA”) and ID for Vendors (“IDFV”). Both the IDFA and the IDFV are unique, alphanumeric strings that are used to identify an individual device—and the individual who uses that device—in order to track and profile the user, and to serve her with targeted advertising. However, the focus of this action is Defendants’ behavior in the Android/Google marketplace, not in the Apple/iTunes marketplace. All of the Gaming Apps at issue in this Complaint are offered for Android devices but not Apple devices.

⁵⁶ There are multiple, additional items of data that are universally recognized as persistent

about children, including their behaviors, demographics, and preferences, and, thereafter, to serve them with tailored and targeted advertising. Defendants also use persistent identifiers to track the effectiveness of those advertisements after the child sees them (to determine, for example, whether the child downloaded the app or bought the product advertised).

9. The Moment Children Launch A Gaming App, the SDK Software Sends Children's Persistent Identifiers to the SDK Defendants.

55. As soon as a New Mexico child opens up a Gaming App on her device and it connects to the Internet, the app will connect to servers, including those belonging to the SDK Defendants, and begin sending those servers data. This activity is invisible to the child (and her parent), who simply sees the given app's game interface. However, forensic analysis of the Internet communication between the device and server can capture the data exchanged between the two.

56. As the child plays the Gaming App, the embedded SDK Defendants' software continues to communicate with the SDK Defendants' respective servers, sending requests for an ad—or “calls”—to the servers. With each request from an SDK Defendant's SDK, the SDK also sends the child's Personal Data, including in the form of persistent identifiers and (often) geolocation. The SDK Defendant then stores and analyzes the Personal Data to enable continued tracking of the child, such as what ads she has already seen, what actions she took in response to those ads, other online behavior, and additional demographic data. This way, each SDK Defendant (and other affiliated entities) can generally monitor, profile, and track her over time, across devices, and across the Internet.

identifiers. For example, a device's Wi-Fi MAC address is a fixed serial number that is used to identify one's phone when transmitting and receiving data using Wi-Fi. The State's forensic analysis has principally focused on the exfiltration and use of AAID, IMEI and Device Fingerprint data persistent identifiers.

57. The exfiltration of this Personal Data, the purposes for which it is used, and the lack of restrictions placed on its exfiltration, retention, and use are demonstrated through forensic testing and the business relationship between the SDK Defendants and Tiny Lab.

58. At no point, and in no context, is sufficient disclosure provided or verifiable parental consent obtained for any of the data exfiltration described herein as required by COPPA.

C. The SDK Defendants Exfiltrate Children’s Personal Data While They Play Tiny Lab’s Gaming Apps

1. Twitter/MoPub

a. Forensic Analysis of Twitter/MoPub’s Activity in Tiny Lab’s Gaming Apps.

59. To show ads to children via a Gaming App, the Twitter/MoPub SDK embedded in the Gaming App communicates with or “makes a call” to Twitter/MoPub servers (as evidenced by, for example, data being sent to servers affiliated with the address `ads.MoPub.com` and `analytics.MoPub.com`), and requests that an ad be shown to a particular child while he or she is playing the game.

60. Through this, Twitter/MoPub can receive the user’s Personal Data, in the form of persistent identifiers including, among others, the child’s AAID and Android ID.

61. Additionally, Twitter/MoPub can receive the GPS location of the child’s device, with an accuracy of +/-5 meters (*i.e.*, granular location to the street level). Additionally, forensic testing indicates that Twitter/MoPub updates its receipt of the child’s location continuously, in real time (testing indicates that these updates can occur at very short intervals—even at the millisecond level). This continual updating of the child’s geolocation allows Twitter/MoPub to persistently and pervasively track a child as she moves about her day.

62. Twitter/MoPub can also receive the IP address of the child’s device, which enables the identification of the child’s location, the identification of the child’s device, and

cross-device tracking. An IP address is a unique number that identifies a given device, allowing it to communicate with other computers on the Internet (which have their own IP addresses).

63. Twitter/MoPub's call to its servers can also disclose other valuable Personal Data in the form of Device Fingerprint data that can be used to identify, profile, and target specific children. This information can include, *inter alia*:

- a. the child's language;
- b. the child's country;
- c. the child's time zone;
- d. the child's cellular carrier;
- e. the manufacturer, make, and model of the child's device;
- f. the child's device operating system and version;
- g. the screen dimensions of the child's device; and
- h. the name and developer of the app the child is operating.

Data Point	Exemplar Data Field ⁵⁷	Personal Information Derived from Data
AAID	A42c89c4-1dc7-5b79-92cd-01fa2cd5cab2	Jane Minor's device's unique AAID
Android ID	28507917b736aa3	Jane Minor's device's unique Android ID
Child's device's IP address	206.3.128.12	Jane Minor's device can be identified and located on the Internet, her location can be identified, and she can be tracked across devices via this number
Child's language	Accept-Language: en	Jane Minor's Fun Kid Racing app is in American English
Child's country	iso: us	Jane Minor's device is located in the U.S.

⁵⁷ The figures in this table are exemplars and do not disclose any individual's personally identifying information. Except where indicated otherwise, data points are derived from forensic analysis of the gaming app Fun Kid Racing on an Android device.

Child's time zone	z: +0000	Jane Minor is playing Fun Kid Racing on a device with a clock set to GMT
Child's mobile network	cn: T-Mobile	Jane Minor's service provider is T-Mobile
Manufacturer, make, and model of the child's device	dn: LGE, AOSP on BullHead, aosp_bullhead	Jane Minor is playing Fun Kid Racing on her LG Nexus 5X running the open source branch of the Android OS ⁵⁸
Child's device operating system and version	User-Agent: Android 6.0.1	Jane Minor's phone is running the Android operating system, version 6.0.1
Screen dimensions of the child's device	h: 1080 w: 1920	Jane Minor's device screen is 1080 by 1920
Application name and developer	bundle: com.tinylab productions.FunKidRacing	Jane Minor is a Tiny Lab Fun Kid Racing user

b. Forensic Analysis Demonstrates That the Twitter/MoPub SDK Behaves Similarly Across All of the Gaming Apps In Which it is Embedded.

64. Forensic testing reveals that the Twitter/MoPub SDK behaves similarly in each of the Gaming Apps in which it is embedded—surreptitiously exfiltrating children's Personal Data (including but not limited to persistent identifiers and geolocation), without verifiable parental consent.

c. Twitter/MoPub is in the Business of Collecting Personal Data to Track and Profile Children.

65. As alleged herein, Twitter/MoPub is in the business of collecting Personal Data to track and profile children and sharing such Personal Data with publishers, advertisers, service providers, and Twitter/MoPub's affiliates.

⁵⁸ In the example, "LGE" refers to the LG phone hardware, "AOSP" is "Android Open Source Project" (the open-source branch of Android), and "Bullhead" is the codename for the Nexus 5X hardware. Thus, the example is reporting that this was run on an LG Nexus 5X running the open source branch of the Android OS.

66. Tiny Lab's and Twitter/MoPub's concerted efforts to exfiltrate children's Personal Data—for purposes of tracking and profiling children—are undertaken without (1) reasonable and meaningful notice to parents, or (2) verifiable parental consent.

2. Google/AdMob

a. Forensic Analysis of Google/AdMob's Activity in Tiny Lab's Gaming Apps.

67. To show ads to children via a Gaming App, the AdMob SDK embedded in the Gaming App communicates with or “makes a call” to Google/AdMob's servers (as evidenced by, for example, data being sent to servers affiliated with the address `googleads.g.doubleclick.net`), and requests that an ad be shown to a particular child while he or she is playing the game.

68. Through this, Google/AdMob can receive the child's Personal Data, in the form of persistent identifiers including, among others, the child's AAID and IMEI .

69. Additionally, Google/AdMob can receive the GPS location of the child's device, with a street-level granular accuracy.

70. Google/AdMob can also receive the IP address of the child's device, which enables the identification of the child's location, the identification of the child's device, and cross-device tracking.

71. Google/AdMob's call to its servers can also disclose other valuable Personal Data in the form of Device Fingerprint data that can be used to identify, profile, and target specific children. This information can include, *inter alia*:

- a. the manufacturer, make, and model of the child's device;
- b. the operating system of the child's device; and
- c. the name and developer of the app the child is operating.

Data Point	Exemplar Data Field ⁵⁹	Personal Information Derived from Data
AAID	A42c89c4-1dc7-5b79-92cd-01fa2cd5cab2	Jane Minor's device's unique AAID
IMEI	721781239167920	Jane Minor's device's unique IMEI
Child's device's IP address	206.3.128.12	Jane Minor's device can be identified and located on the Internet, her location can be identified, and she can be tracked across devices via this number
Manufacturer, make, and model of the child's device	AOSP on BullHead Build	Jane Minor is playing Fun Kid Racing on her LG Nexus 5X running the open source branch of the Android OS ⁶⁰
Child's device operating system and version	User-Agent: Android 6.0.1	Jane Minor's phone is running the Android operating system, version 6.0.1
Application name and developer	app: com.TinyLab Productions.FunKidRacing	Jane Minor is a Tiny Lab Fun Kid Racing user

b. Forensic Analysis Demonstrates That the Google/AdMob SDK Behaves Similarly Across All of the Gaming Apps In Which it is Embedded.

72. Forensic testing reveals that the AdMob SDK behaves similarly in each of the Gaming Apps in which it is embedded—surreptitiously exfiltrating children's Personal Data (including but not limited to persistent identifiers and geolocation), without verifiable parental consent.

⁵⁹ The figures in this table are exemplars and do not disclose any individual's personally identifying information. Except where indicated otherwise, data points are derived from forensic analysis of the gaming app Fun Kid Racing on an Android device.

⁶⁰ In the example, "AOSP" is "Android Open Source Project" (the open-source branch of Android), and "Bullhead" is the codename for the LG Nexus 5X hardware. Thus, the example is reporting that this was run on an LG Nexus 5X running the open source branch of the Android OS.

c. **Google/AdMob is in the Business of Collecting Personal Data to Track and Profile Children.**

73. As alleged herein, Google/AdMob is in the business of collecting Personal Data to track and profile children and sharing such Personal Data with publishers, advertisers, service providers, and Google/AdMob affiliates.

74. Tiny Lab's and Google/AdMob's concerted efforts to exfiltrate children's Personal Data—for purposes of tracking and profiling children—are undertaken without (1) reasonable and meaningful notice to parents, or (2) verifiable parental consent.

3. **AerServ**

a. **Forensic Analysis of AerServ's Activity in Tiny Lab's Gaming Apps.**

75. To show ads to children via a Gaming App, the AerServ SDK embedded in the Gaming App communicates with or "makes a call" to AerServ's servers (as evidenced by, for example, data being sent to servers affiliated with the address `ads.AerServ.com`), and requests that an ad be shown to a particular child while he or she is playing the game.

76. Through this, AerServ can receive the child's Personal Data, in the form of persistent identifiers including, among others, the child's AAID and IMEI.

77. Additionally, AerServ can receive the GPS location of the child's device, with a street-level granular accuracy.

78. AerServ can also receive the IP address of the child's device, which enables the identification of the child's location, the identification of the child's device, and cross-device tracking.

79. AerServ's call to its servers can also disclose other valuable Personal Data in the form of Device Fingerprint data that can be used to identify, profile, and target specific children. This information can include, *inter alia*:

- a. the child's language;
- b. the child's network connection;

- c. the manufacturer, make, and model of the child's device;
- d. the operating system of the child's device;
- e. the screen dimensions of the child's device; and
- f. the name and developer of the app the child is operating.

Data Point	Exemplar Data Field ⁶¹	Personal Information Derived from Data
AAID	A42c89c4-1dc7-5b79-92cd-01fa2cd5cab2	Jane Minor's device's unique AAID
IMEI	721781239167920	Jane Minor's device's unique IMEI
Child's device's IP address	206.3.128.12	Jane Minor's device can be identified and located on the Internet, her location can be identified, and she can be tracked across devices via this number
Child's language	lang=en	Jane Minor's Fun Kid Racing app is in American English
Child's network connection	network=wifi	Jane Minor's device is connected to wifi
Manufacturer, make, and model of the child's device	Make=LGE AOSP on BullHead Build	Jane Minor is playing Fun Kid Racing on her LG Nexus 5X running the open source branch of the Android OS ⁶²
Child's device operating system and version	User-Agent: Android 6.0.1	Jane Minor's phone is running the Android operating system, version 6.0.1
Screen dimensions of the child's device	h: 411 w: 683	Jane Minor's device screen is 411 by 683
Application name and developer	bundleid = com.tinylab productions.FunKidRacing	Jane Minor is a Tiny Lab Fun Kid Racing user

⁶¹ The figures in this table are exemplars and do not disclose any individual's personally identifying information. Except where indicated otherwise, data points are derived from forensic analysis of the gaming app Fun Kid Racing on an Android device.

⁶² In the example, Jane Minor is playing on an "LGE" phone, "AOSP" is "Android Open Source Project" (the open-source branch of Android), and "Bullhead" is the codename for the Nexus 5X hardware. Thus, the example is reporting that this was run on an LG Nexus 5X running the open source branch of the Android OS.

b. **Forensic Analysis Demonstrates That the AerServ SDK Behaves Similarly Across All of the Gaming Apps In Which it is Embedded.**

80. Forensic testing reveals that the AerServ SDK behaves similarly in each of the Gaming Apps in which it is embedded—surreptitiously exfiltrating children’s Personal Data (including but not limited to persistent identifiers and geolocation), without verifiable parental consent.

c. **AerServ is in the Business of Collecting Personal Data to Track and Profile Children**

81. As alleged herein, AerServ is in the business of collecting Personal Data to track and profile children and sharing such Personal Data with publishers, advertisers, service providers, and AerServ’s affiliates.

82. Tiny Lab’s and AerServ’s concerted efforts to exfiltrate children’s Personal Data—for purposes of tracking and profiling children—are undertaken without (1) reasonable and meaningful notice to parents, or (2) verifiable parental consent.

4. AppLovin

a. **Forensic Analysis of AppLovin’s Activity in Tiny Lab’s Gaming Apps.**

83. To show ads to children via a Gaming App, the AppLovin SDK embedded in the Gaming App communicates with or “makes a call” to AppLovin servers (as evidenced by, for example, data being sent to servers affiliated with the address `rt.applovin.com` and `a.applovin.com`), and requests that an ad be shown to a particular child while he or she is playing the game.

84. Through this, AppLovin can receive the child’s Personal Data, in the form of persistent identifiers including, among others, the child’s AAID and IMEI.

85. AppLovin can also receive the IP address of the child’s device, which enables the identification of the child’s location, the identification of the child’s device, and cross-device tracking.

86. AppLovin's call to its servers can also disclose other valuable Personal Data in the form of Device Fingerprint data that can be used to identify, profile, and target specific children. This information can include, *inter alia*:

- a. the child's country;
- b. the child's time zone;
- c. the child's mobile carrier;
- d. the precise moment in time that the child installed the app;
- e. whether the child had previously installed the app on her phone;
- f. the manufacturer, make, and model of the child's device;
- g. the child's operating system version; and
- h. the name and developer of the app the child is operating.

Data Point	Exemplar Data Field ⁶³	Personal Information Derived from Data
AAID	A42c89c4-1dc7-5b79-92cd-01fa2cd5cab2	Jane Minor's device's unique AAID
IMEI	721781239167920	Jane Minor's device's unique IMEI
Child's device's IP address	206.3.128.12	Jane Minor's device can be identified and located on the Internet, her location can be identified, and she can be tracked across

⁶³ The figures in this table are exemplars and do not disclose any individual's personally identifying information. Except where indicated otherwise, data points are derived from forensic analysis of the gaming app Fun Kid Racing on an Android device.

		devices via this number
Child's country	country_code=us	Jane Minor's device is located in the U.S.
Child's time zone	tz_offset: +0000	Jane Minor is playing Fun Kid Racing on a device with a clock set to GMT
Child's mobile carrier	cn: T-Mobile	Jane Minor's service provider is T-Mobile
The precise moment in time that the child installed the app	"installed_at"=1527608937	The Fun Kid Racing app on Jane Minor's device was installed on May 29, 2018 at 15:48:57 ⁶⁴ UTC. ⁶⁵
Whether the child had previously installed the app on her phone	"first_install": "true"	Jane Minor has not previously installed Fun Kid Racing on her phone
Manufacturer, make, and model of the child's device	brand=LGE hardware=bullhead model=AOSP+on+BullHead	Jane Minor is playing Fun Kid Racing on her LG Nexus 5X running the open source branch of the Android OS ⁶⁶
Child's device operating system and version	platform=Android os=6.0.1	Jane Minor's phone is running the Android operating system, version 6.0.1
Application name and developer	"package_name": com.tinylab productions.FunKidRacing	Jane Minor is a Tiny Lab Fun Kid Racing user

⁶⁴ This data point is known as a "timestamp," and identifies the time at which an event is recorded (here, app installation). In the ad tech world, this data point plays a useful role. The data point tracks time from a pre-established start date. The timestamp tells online companies exactly when an event occurs after the start date—measured to the second or millisecond—and thus permits a company to build a profile of when a user is active on her phone regardless of the time zone in which she resides. The timestamp is formatted to track the number of seconds since Jan. 1, 1970. By using a decoder, such as <http://coderstoolbox.net/unixtimestamp>, the timestamp can be converted to an exact date and time (accessed on Sept. 4, 2018).

⁶⁵ Coordinated Universal Time.

⁶⁶ In the example, "LGE" refers to the LG phone hardware, "AOSP" is "Android Open Source Project" (the open-source branch of Android), and "Bullhead" is the codename for the Nexus 5X hardware. Thus, the example is reporting that this was run on an LG Nexus 5X running the open source branch of the Android OS.

b. **Forensic Analysis Demonstrates That the AppLovin SDK Behaves Similarly Across All of the Gaming Apps In Which it is Embedded.**

87. Forensic testing reveals that the AppLovin SDK behaves similarly in each of the Gaming Apps in which it is embedded—surreptitiously exfiltrating children’s Personal Data (including but not limited to persistent identifiers), without verifiable parental consent.

c. **AppLovin is in the Business of Collecting Personal Data to Track and Profile Children.**

88. As alleged herein, AppLovin is in the business of collecting Personal Data to track and profile children and sharing such Personal Data with publishers, advertisers, service providers, and AppLovin’s affiliates.

89. Tiny Lab’s and AppLovin’s concerted efforts to exfiltrate children’s Personal Data—for purposes of tracking and profiling children—are undertaken without (1) notice to parents, or (2) reasonable and meaningful verifiable parental consent.

5. **ironSource**

a. **Forensic Analysis of ironSource’s Activity in Tiny Lab’s Gaming Apps.**

90. To show ads to children via a Gaming App, the ironSource SDK embedded in the Gaming App communicates with or “makes a call” to ironSource servers (as evidenced by, for example, data being sent to servers affiliated with the address `outcome.supersonicads.com` and `rv-gateway.supersonicads.com`), and requests that an ad be shown to a particular child while he or she is playing the game.

91. Through this, ironSource can receive the child’s Personal Data, in the form of persistent identifiers including, among others, the child’s AAID and IMEI.

92. ironSource can also receive the IP address of the child’s device, which enables the identification of the child’s location, the identification of the child’s device, and cross-device tracking.

93. ironSource's call to its servers can also disclose other valuable Personal Data in the form of Device Fingerprint data that can be used to identify, profile, and target specific children. This information can include, *inter alia*:

- a. the child's language;
- b. the child's network connection;
- c. the child's time zone;
- d. the precise time at which the child was served with an ad;
- e. the manufacturer, make, and model of the child's device;
- f. the child's operating system version; and
- g. the name and developer of the app the child is operating.

Data Point	Exemplar Data Field ⁶⁷	Personal Information Derived from Data
AAID	A42c89c4-1dc7-5b79-92cd-01fa2cd5cab2	Jane Minor's device's unique AAID
IMEI	721781239167920	Jane Minor's device's unique IMEI
Child's device's IP address	206.3.128.12	Jane Minor's device can be identified and located on the Internet, her location can be identified, and she can be tracked across devices via this number
Child's language	"language": "en"	Jane Minor's Fun Kid

⁶⁷ The figures in this table are exemplars and do not disclose any individual's personally identifying information. Except where indicated otherwise, data points are derived from forensic analysis of the gaming app Fun Kid Racing on an Android device.

		Racing app is in American English
Child's network connection	"connectionType": "wifi"	Jane Minor's device is connected to the Internet via WiFi.
Child's time zone	"gmtMinutesOffset": 0	Jane Minor is playing Fun Kid Racing on a device with a clock set to GMT
The precise time at which the child was served with an ad	"timestamp"=1527608937	The ironSource SDK served an ad on Jane Minor's on May 29, 2018 at 15:48:57 ⁶⁸ UTC. ⁶⁹
Manufacturer, make, and model of the child's device	"deviceOEM": "LGE" "deviceModel": "AOSP on Bullhead"	Jane Minor is playing Fun Kid Racing on her LG Nexus 5X running the open source branch of the Android OS ⁷⁰
Child's device operating system and version	"devicesOS": Android "osVersion": "23(6.0.1)"	Jane Minor's phone is running the Android operating system, version 6.0.1
Application name and developer	"bundleID": "com.tinylab productions.FunKidRacing"	Jane Minor is a Tiny Lab Fun Kid Racing user

⁶⁸ This data point is known as a "timestamp," and identifies the time at which an event is recorded (here, app installation). In the ad tech world, this data point plays a useful role. The data point tracks time from a pre-established start date. The timestamp tells online companies exactly when an event occurs after the start date—measured to the second or millisecond—and thus permits a company to build a profile of when a user is active on her phone regardless of the time zone in which she resides. The timestamp is formatted to track the number of seconds since Jan. 1, 1970. By using a decoder, such as <http://coderstoolbox.net/unixtimestamp>, the timestamp can be converted to an exact date and time (accessed on Sept. 4, 2018).

⁶⁹ Coordinated Universal Time.

⁷⁰ In the example, "LGE" refers to the LG phone hardware, "AOSP" is "Android Open Source Project" (the open-source branch of Android), and "Bullhead" is the codename for the Nexus 5X hardware. Thus, the example is reporting that this was run on an LG Nexus 5X running the open source branch of the Android OS.

b. Forensic Analysis Demonstrates That the ironSource SDK Behaves Similarly Across All of the Gaming Apps In Which it is Embedded

94. Forensic testing reveals that the ironSource SDK behaves similarly in each of the Gaming Apps in which it is embedded—surreptitiously exfiltrating children’s Personal Data (including but not limited to persistent identifiers), without verifiable parental consent.

c. ironSource is in the Business of Collecting Personal Data to Track and Profile Children

95. As alleged herein, ironSource is in the business of collecting Personal Data to track and profile children and sharing such Personal Data with publishers, advertisers, service providers, and ironSource’s affiliates.

96. Tiny Lab’s and ironSource’s concerted efforts to exfiltrate children’s Personal Data—for purposes of tracking and profiling children—are undertaken without (1) reasonable and meaningful notice to parents, or (2) verifiable parental consent.

D. Tiny Lab’s “Age Gate” Is Unlawful Under COPPA, as the Gaming Apps Are Directed to Children.

97. Tiny Lab belatedly added an age screening function to its Fun Kid Racing and other Gaming Apps on or about January 30, 2017, purportedly for purposes of limiting the tracking of children. However, this belated and facile implementation of age verification, known as “age gating,” to identify child users of the Gaming Apps is prohibited in this context by COPPA. Moreover, it is illusory and does not protect children’s privacy.

98. At the outset, the FTC’s guidelines prohibit companies like Tiny Lab—that develop child-directed apps—from using age screening to segment their users into multiple groups to receive different COPPA treatment. The FTC specifies that:

Because of its very nature, in most instances, a website or online service (such as an app) directed to children must treat all visitors as children and provide COPPA’s protections to every such visitor.

This means that for the most part, a website or online service directed to children may not screen users for age.⁷¹

99. The FTC created a narrow exception to this prohibition, allowing an app to use an age gate *if and only if* that app is for a general audience, and not directed towards children. If, however, the app is directed towards children (such as each of the Gaming Apps), a developer may not rely on an age gate to screen children, and instead must treat all users in a COPPA-compliant, privacy-protective manner.

100. Tiny Lab’s Gaming Apps are indisputably designed for children, as is evident from their cartoonish design and subject matter, as well as Tiny Lab’s specific representations regarding the Gaming Apps.⁷² For example, Tiny Lab has at least two websites, which both advertise their games as being directed at “kids.” For instance, at <https://www.tinylabkids.com/>, the website boldly proclaims, “keep your kids entertained for months” (*see* Figure 3, *infra*). On their other website (<http://tinylabproductions.com/>), Tiny Lab features Fun Kid Racing and describes it as a “racing game for kids” (*see* Figure 4, *infra*). This advertisement goes on to say that “children love it” and that the “levels are designed specifically for children.” This makes plain that Tiny Lab’s games are directed at—and designed specifically for—children, which means that Tiny Lab cannot employ age gates to offer COPPA-compliant treatment to only a subset of its users. Indeed, Tiny Lab may not lawfully use age gates, full stop.

⁷¹ *Complying with COPPA: Frequently Asked Questions*, Federal Trade Commission (available at <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>) (accessed on Sept. 4, 2018).

⁷² As stated in paragraphs 195-196, *infra*, Tiny Lab’s CEO acknowledged in an interview that the Gaming Apps are kid-friendly games designed for toddlers.



Figure 3⁷³

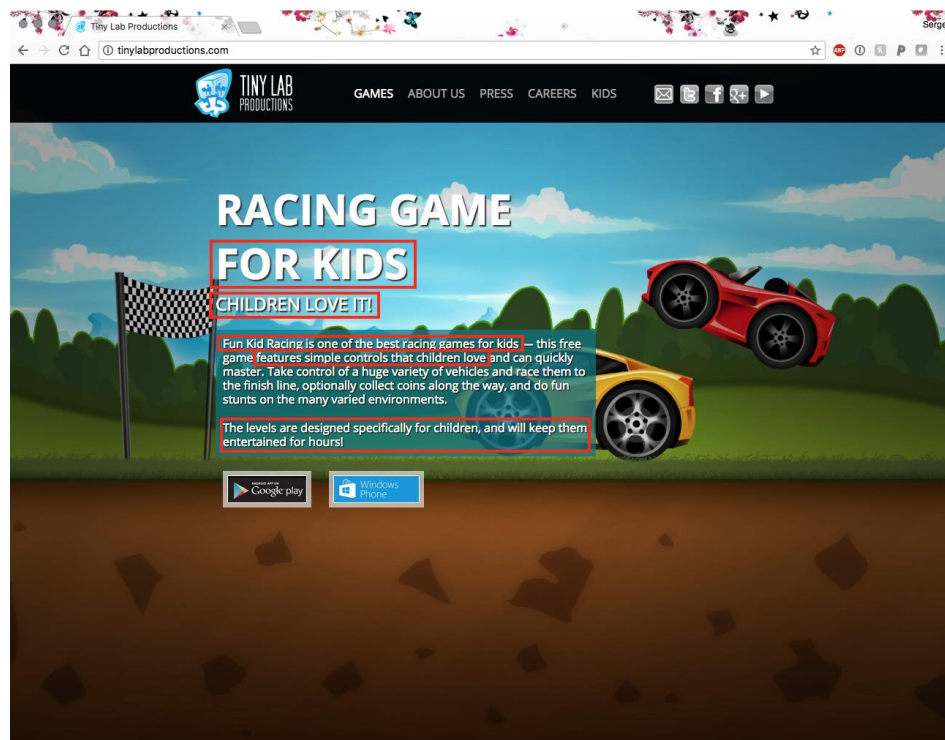


Figure 4⁷⁴

⁷³ Tiny Lab Kids (available at <https://tinylabkids.com/>) (accessed on Sept. 4, 2018).

⁷⁴ Tiny Lab Productions (available at <http://tinylabproductions.com/>) (accessed on Sept. 4,

101. Moreover, even if an age gate were permissible in the Gaming Apps—it is not—such an age gate would have to be “neutral,” and may not be designed to encourage children to enter an age over 13 (and thus enable online tracking and profiling).⁷⁵ Tiny Lab’s age gate flunks this test.

102. Rather than simply requiring children to enter their numerical age, Tiny Lab’s age gate requires children to enter their birth year (*see* Figure 5, *infra*), and currently defaults to a birth year between 2000 and 2001. Children can tap the left and right arrows to increase or decrease the year. Thus, simply clicking an arrow once will yield an age of 17 (2001) or 18 (2000), whereas it takes a minimum of six taps (plus the “OK” button) to specify an age under 13. Even more taps are required to enter an accurate age for younger children—the toddlers for whom the Gaming Apps are designed and to whom they are directed. This means that if a young child is uncomprehendingly, mistakenly, randomly and/or impatiently clicking, she will almost always enter an age older than 13.

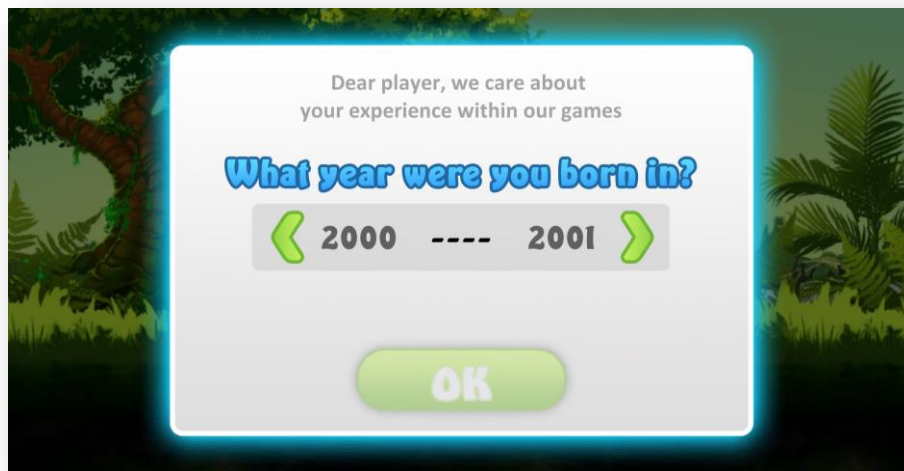


Figure 5

2018).

⁷⁵ *Complying with COPPA: Frequently Asked Questions*, Federal Trade Commission (available at <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>) (accessed on Sept. 4, 2018).

103. The presence of Tiny Lab’s age gate heightens the invasiveness of the Gaming Apps and increases the potential for the exfiltration of children’s Personal Data, because the mere presence of the age gate implies that Tiny Lab will abide by social norms that require parental consent before conducting business with a minor.

104. Further, the very presence of the age gate confirms that the SDK Defendants engage in targeted advertising (as opposed to contextual advertising, which is permitted under COPPA). The only purpose of the age gate is to segregate users for advertising purposes – targeting users on one side of the age gate threshold and serving contextual ads for all other users. Of course, for the reasons stated above, Tiny Lab may not use an age gate at all, given the child-directed nature of the Gaming Apps at issue. However, the age gate’s presence is an admission, by Tiny Lab, that targeted advertising—facilitated by the SDK Defendants—is taking place within the Gaming Apps. In a press release, Tiny Lab confirms that anyone entering an age over 13 *will* have her personal information (as that term is defined by COPPA) collected by the SDK Defendants.⁷⁶ Tiny Lab impermissibly uses an age gate (which allows for tracking of users), and further rigs that age gate to make it more likely than not that an unsuspecting user will be tracked. This results in the unlawful collection of Personal Data for targeted advertising, by the SDK Defendants in conjunction with Tiny Lab.

E. The SDK Defendants Have Actual Knowledge That Their Exfiltration of Personal Data Takes Place in the Child-Directed Gaming Apps

105. Each SDK Defendant, as a for-profit commercial entity that has agreed and continues to agree with Tiny Lab for its SDK to be used, deployed and/or integrated in Gaming Apps, had and has actual knowledge that Personal Data (including “personal information” as defined by COPPA) is collected directly from users of Tiny Lab’s child-directed Gaming Apps. The parties – SDK Defendants and Tiny Lab – are sophisticated entities in the business of

⁷⁶ See <https://www.tinylabkids.com/press>

commercializing users' Personal Data extracted from child-directed Gaming Apps. As such, they are aware of, and benefit or profit from the conduct at issue described herein. Indeed, this forms a core component of their business models.

106. Moreover, the SDK Defendants' actual knowledge is evidenced by, *inter alia*, (1) communications between Tiny Lab and each SDK Defendant, and (2) SDK Defendants' own actions recognizing the child-directed nature of the Gaming Apps' content.

107. The communications to and from Tiny Lab evidencing each SDK Defendant's actual knowledge of the child-directed nature of Gaming Apps occur from the initial interactions between them, as the SDK is first deployed within the Gaming Apps, and throughout their transactional relationship, as the SDK functions within the Gaming Apps. Indeed, these communications recur every time a Gaming App communicates with an SDK Defendant and/or to its technology, including but not limited to its servers. As demonstrated in the respective charts in paragraphs 63, 71, 79, 86, and 93, *supra*, among the items of Personal Data that are communicated by Tiny Lab to the SDK Defendants is the bundle ID ("com.tinylabproductions.FunKidRacing"), which contains both the name of the developer ("Tiny Lab") and the child-directed app title at issue (in this example, "Fun Kid Racing"). Each call invariably and manifestly indicates the child-directed nature of the Gaming App and its content.

108. Each SDK Defendant's *own* actions recognizing the child-directed nature of the Gaming Apps' content occur, *at minimum*, each time an SDK Defendant acquires a child's Personal Data from a Gaming App (including "personal information" as defined by COPPA) for purposes of profiling the child and serving her age-based behavioral advertising targeted to children. As discussed, *infra*, the SDK Defendants use the Personal Data at their (or their partners') command to profile and target children with specific ads, through their SDK, and those ads are child-oriented. Ads served through the Gaming Apps are intentionally child-directed—

for instance, testing reveals, *inter alia*, service to users of ads for cartoonish games very similar in content and cartoonish presentation to the Tiny Lab Gaming Apps. The SDK Defendants can and do seek and acquire age-identifying information about each child and can and do use this information to profile and target that child. The SDK Defendants, acting as intermediary, partner or broker between Tiny Lab and putative advertisers, are the entities that match ads with a given Gaming App. As a result of the Personal Data acquired (and attendant user profiling), SDK Defendants can and do serve child-directed advertisements on Tiny Lab's child-directed Gaming Apps via the communications engendered by their embedded SDKs. Here, the delivery of these ads, and the varied and broad use of this Personal Data, create a distinct segment of their business that is child-directed. By embedding their SDKs, communicating with Tiny Labs and serving age-based behavioral advertising targeted to children, each SDK Defendant adopts the child-directed content as its own.

109. In addition, as described, *infra*, the majority of Tiny Lab's Gaming Apps were submitted to Google as family friendly, child-directed and appropriate for inclusion in Google's Designed For Family section on Google Play. Upon receiving that information, at the time of initial marketing each Gaming App, Google had actual knowledge that the each such Gaming App was child-directed. Moreover, for Defendant Google, it had actual knowledge of the child-directed nature of the Gaming Apps given its communications with security researchers detailed in paragraphs 110-121, *infra*. While Google chose and continues to choose to disregard the information the researchers provided, the fact remains that Google claims to have reviewed thoroughly the subject matter and presentation of myriad Tiny Lab Gaming Apps, into which its AdMob SDK is embedded, and from which its SDK can, does and continues to collect Personal Data for targeted advertising. Accordingly, Google has actual knowledge of the child-directed nature of Tiny Lab's Gaming Apps.

F. Defendant Google Was Alerted to the COPPA-Violative Behavior Endemic to Tiny Lab's Apps, But Ignored It and Continues to Market the Apps as Child-Appropriate and Safe in Its Online Store

110. In Spring 2018, Google was notified by security researchers at the University of California, Berkeley, that they had identified Defendants' privacy-invasive technology and practices in Tiny Lab's Gaming Apps, as identified above.

111. In particular, the researchers called Google's attention to the fact that the COPPA-violative Gaming Apps were marketed by Google as part of the "Family" category of its Google Play Store.

112. As discussed in further detail in paragraphs 195-196, *infra*, in order to be featured in the Family section of Google Play, Google requires that the app be a part of the "Designed for Families" program,⁷⁷ which comes with specific requirements. Particularly, in order to be included in the program,⁷⁸ Tiny Lab had to expressly warrant, *inter alia*, that their apps met specific criteria related to privacy guidelines set by Google. These express guidelines include the following:

Eligibility

All apps participating in the Designed for Families program must be relevant for children under the age of 13 and comply with the eligibility criteria below. App content must be appropriate for children. Google Play reserves the right to reject or remove any app determined to be inappropriate for the Designed for Families program.

...

⁷⁷ *Designed for Families*, Google Play (available at <https://developer.android.com/google-play/guides/families/>) (accessed September 7, 2018). Per Google, "Only apps and games that are part of the Designed for Families program will show up in searches initiated from the Family section in Apps Home."

⁷⁸ As noted in Exhibit 1, each of the Gaming Apps is or has been a participant in Google's Designed for Families program, with five exceptions: Chhota Bheem Speed Racing; Christmas Snow Racing; Fun Kid Bubble Pop; Fun Kid Racing - Stickman Mode; and Windy Way.

2. If your Designed for Families app displays ads, you confirm that:

2.1 You comply with applicable legal obligations relating to advertising to children.

2.2 Ads displayed to child audiences do not involve interest-based advertising or remarketing.

2.3 Ads displayed to child audiences present content that is appropriate for children.

2.4 Ads displayed to child audiences follow the Designed for Families ad format requirements.

...

7. You represent that apps submitted to Designed for Families are compliant with COPPA (Children's Online Privacy Protection Rule) and other relevant statutes, including any APIs [a synonym for SDKs] that your app uses to provide the service.

113. Thus, in marketing these apps and seeking the commercial advantage of the improved visibility to parents afforded by its family-oriented positioning in Google Play, Tiny Lab warranted that the Designed for Families (or DFF, as defined *infra*) Gaming Apps are child-friendly, that they (and Tiny Lab, generally) act in accordance with all applicable privacy laws and regulations (including COPPA, specifically), and that any third-party software contained within the apps will comply with all applicable privacy laws and regulations.

114. Accordingly, upon uncovering the surreptitious tracking rampant within the Gaming Apps, the security researchers wrote to Google that

We have identified that 2,667 apps are potentially incorrectly listed as directed to "mixed audiences," and "not primarily directed to children," corresponding to ~51% of Designed for Families (DFF) apps from our original sample which are still listed on DFF. Developers seem to have an incentive to miscategorize their apps as "not primarily directed to children" so they will be able to engage in defective "age gating," thereby very likely causing children under 13 to enter ages over 13, allowing COPPA-

prohibited behavioral advertising.

Using 84 of Tiny Lab Productions' ("Tiny Lab") apps, with a total of 75,000,000 downloads, as a case study: we illustrate how the listing of an app under the "mixed audience" category, could be misleading to consumers and in potential violation of COPPA, despite the representations app developers are making to Google as part of their participation in the DFF program. We further explain how Tiny Lab (and potentially others) employ defective "age gates" in potential violation of COPPA. Moreover, since according to the FTC, "in most instances, a website or online service (such as an app) directed to children must treat all visitors as children and provide COPPA's protections to every such visitor," and given the "child-friendly" nature of DFF, we find it puzzling that more than 50% of our corpus, amounting to thousands of apps, are categorized as so-called "not primarily directed to children."

More generally, we explain how Google's DFF terms are contributing to this problem and might be incentivizing developers to potentially abuse DFF and deceive consumers by potentially misrepresenting their apps' true nature and stating they are not primarily directed to children (mixed-audience), when they clearly are. We suggest potential methods to mitigate this potential abuse more generally.

115. In response, Google offered two primary rebuttals: (1) there was no mechanism to detect and prevent the issue "at scale"; and (2) more information was required on appropriate "heuristics" to support the conclusion that the Tiny Lab apps at issue were child directed.

116. With respect to the first assertion by Google, the researchers responded that

[T]his is precisely what we did. . . . this was a case study using the app analysis infrastructure that we built. The point is, Google could replicate our infrastructure to do the exact same type of testing at scale. More importantly, in this specific report, we *do* recommend multiple mechanisms that Google can use:

1) requiring all mixed-audience DFF apps to periodically report age information based on the age gates that they use. If, as a result of the age gating, a developer knows that 70% of its users are under 13, it's obvious that the app is "primarily child directed."

2) without doing #1, require all apps that are categorized by

developers as being mixed audience to undergo manual verification. When the app is initially submitted, it would be trivial for a human to quickly check to see whether the app's marketing materials imply that the primary audience consists of children.

117. Regarding the second concern about appropriate heuristics, the researchers suggested that Google simply ascertain (1) whether the app's name, description, or developer include the words "children," "kids," "baby," etc.; and (2) whether the description or information on a given developer's website addresses parents. Tiny Lab's website provides an object lesson in the value of this exercise. *See* Figures 3-4, *supra*.

118. Google, faced with simple solutions to their purported concerns, ended the dialogue by simply stating that Tiny Lab apps are not directed to children, and accordingly there are no COPPA concerns. Specifically, Google responded,

We really appreciate the research that your organization has been looking in to, to make the internet a more safe space for everyone.

I also have some feedback from our policy team regarding the research that you conducted on DFF apps. Unfortunately, after a thorough investigation of each of the apps that you highlighted in your research paper, *our policy teams did not come to the same conclusion that any of these 84 Tiny Lab Productions apps were violating COPPA in anyway and we do not considered [sic] these apps to be designed primarily for children, but for families in general.*

The Tiny Lap [sic] Production apps that contacted malicious/suspicious domains is very troublesome and we are looking into how to better detect this behavior within our apps review process.

Overall, we do agree that bad developers may still potentially abuse our DFF system by misrepresenting their apps' true nature, but our DFF review team will be enforcing against this type of abuse, when we are aware of its occurrence in our Apps store.

119. This conclusion cannot rationally be said to be grounded in fact. As demonstrated by the above screen shot of Tiny Lab’s website—as well as the allegations contained throughout this Complaint—it is beyond dispute that Tiny Lab’s Gaming Apps are designed for children and directed to children. Tiny Lab’s own CEO makes clear that the apps are directed to not just children, but toddlers.⁷⁹

120. Nor can it reasonably be disputed that Google is aware of the COPPA-violative behavior referenced above. Google, itself, has embedded its AdMob SDK in the Gaming Apps and collects children’s Personal Data therefrom.

121. However, Google affirmatively elected to do nothing to ameliorate the misconduct. Ignoring these facts is particularly egregious in light of the fact that they set and enforce the DFF requirements, and one of the core requirements is COPPA compliance. Specifically, on the portion of Google’s website addressing DFF, Google states “Families and COPPA – Google Play offers a rich platform for developers to showcase trusted, high-quality and age appropriate content for the whole family. Before submitting an app to the Designed for Families program, ensure your app is appropriate for children and compliant with COPPA and other relevant laws.”⁸⁰

G. The Privacy-Invasive and Manipulative Commercial Purposes Behind Defendants’ Data Exfiltration, and its Effect on Children

1. The Role of Personal Data in User Profiling and Targeted Advertising

122. The SDK Defendants and Tiny Lab, in coordination, collect and use the Personal Data described above to track, profile, and target children with targeted advertising.

123. When children are tracked over time and across the Internet, various activities are linked to a unique and persistent identifier to construct a profile of the child of a given mobile

⁷⁹ See ¶¶ 195-196, *infra*.

⁸⁰ *Families and COPPA*, Google (available at <https://play.google.com/about/families/coppa-compliance/integrate/>) (accessed on Sept. 4, 2018).

device. Viewed in isolation, a persistent identifier is merely a string of numbers uniquely identifying a child, but when linked to other data points about the same child, such as app usage, geographic location (including likely domicile), and Internet navigation, it discloses a personal profile that can be exploited in a commercial context.

124. Defendants aggregate this data, and also buy it from and sell it to other third-parties, all the while amassing more data points on children to build ever-expanding profiles for enhanced targeting. Across the burgeoning online advertising ecosystem—often referred to as the “mobile digital marketplace”—multiple ad networks or other third-parties can buy and sell data, exchanging databases amongst themselves, creating an increasingly sophisticated profile of how, when, and why a child uses her mobile device, along with all of the demographic and psychographic inferences that can be drawn therefrom.

125. Similarly, a critical (and thus, fiercely desired) component of user profiles is an individual’s geolocation, which the FTC describes as a “key data point” for advertisers.⁸¹

126. The FTC provides an illustration of these precise data points being used to amass a data profile, via an SDK embedded within an app. In its 2012 report entitled “Mobile Apps for Kids: Disclosures Still Not Making the Grade,” (the “FTC Mobile Apps for Kids Report”) addressing privacy dangers for children in the app space, the FTC cited forensic analysis in which:

[O]ne ad network received information from 31 different apps. Two of these apps transmitted geolocation to the ad network along with a device identifier, and the other 29 apps *transmitted other data (such as app name, device configuration details, and the time and duration of use) in conjunction with a device ID. The ad network could thus link the geolocation information obtained through the two apps to all the other data collected through the*

⁸¹ *Track or Treat? InMobi’s location tracking ignored consumers’ privacy settings*, Federal Trade Commission, (June 22, 2016) (available at <https://www.ftc.gov/news-events/blogs/business-blog/2016/06/track-or-treat-inmobis-location-tracking-ignored-consumers>) (accessed on Sept. 4, 2018).

*other 29 apps by matching the unique, persistent device ID.*⁸²

127. The FTC expressed particular “[c]oncerns about creations of detailed profiles based on device IDs [such as those created and facilitated by Defendants]...where...companies (like ad networks and analytics providers) collect IDs and other user information through a vast network of mobile apps. This practice can allow information gleaned about a user through one app to be linked to information gleaned about the same user through other apps.”

128. Defendants traffic in the same data identified by the FTC (persistent identifiers such as AAID and Device Fingerprint data, in concert with geolocation) causing the same harm identified by the FTC: allowing ad networks to combine data points about children from a multitude of apps.

129. The FTC Mobile Apps for Kids Report cautions that it is standard practice—and long has been standard practice—for ad networks, mobile advertisers, and ad middlemen (including, for example, Defendants and their partners and agents) to link the persistent identifiers and geolocation data they acquire with *additional* Personal Data—such as name, address, and email address—allowing those entities and their partners to identify individual users whom they profile with indisputably individual specificity.⁸³

⁸² *Mobile Apps for Kids: Disclosures Still Not Making the Grade*, Federal Trade Commission, FTC Staff Report (Dec. 2012), at 10 n. 25 (emphasis added) (citing David Norris, Cracking the Cookie Conundrum with Device ID, AdMonsters (Feb. 14, 2012) (*available at* <https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf> (accessed on Sept. 4, 2018) (“Device ID technology is the ideal solution to the problem of remembering what a user has seen and what actions he or she has taken: over time, between devices and across domains. . . . *Device ID can also help businesses understand visitor behavior across devices belonging to the same person or the same residence.*”) (emphasis added).

⁸³ *Id.* at 10 n. 25 (citing Jennifer Valentino-DeVries, *Privacy Risk Found on Cellphone Games*, *Digits Blog*, Wall St. J. (Sept. 19, 2011), *available at* <http://blogs.wsj.com/digits/2011/09/19/privacy-risk-found-on-cellphone-games/> (noting how app developers and mobile ad networks often use device IDs to keep track of user accounts and store them along with more sensitive information like name, location, e-mail address or social-networking data) (accessed on Sept. 4, 2018)).

130. Indeed, key digital privacy and consumer groups have described why and how a persistent identifier alone facilitates targeted advertising and challenges—effectively rendering meaningless—any claims of “anonymized” identifiers:

With the increasing use of new tracking and targeting techniques, any meaningful distinctions between personal and so-called non-personal information have disappeared. This is particularly the case with the proliferation of personal digital devices such as smart phones and Internet-enabled game consoles, which are increasingly associated with individual users, rather than families. This means that marketers do not need to know the name, address, or email of a user in order to identify, target and contact that particular user.⁸⁴

131. A 2014 report by the Senate Committee on Homeland Security and Governmental Affairs entitled “Online Advertising and Hidden Hazards to Consumer Security and Data Privacy” amplifies this concern in light of the growth of third-party trackers that operate behind the scenes in routine online traffic:

Although consumers are becoming increasingly vigilant about safeguarding the information they share on the Internet, many are less informed about the plethora of information created about them by online companies as they travel the Internet. *A consumer may be aware, for example, that a search engine provider may use the search terms the consumer enters in order to select an advertisement targeted to his interests. Consumers are less aware, however, of the true scale of the data being collected about their online activity. A visit to an online news site may trigger interactions with hundreds of other parties that may be collecting information on the consumer as he travels the web. The Subcommittee found, for example, a trip to a popular tabloid news website triggered a user interaction with some 352 other web servers as well....The sheer volume of such activity makes it difficult for even the most vigilant consumer to control the data being collected or protect against its malicious use.*⁸⁵

⁸⁴ Comments of The Center for Digital Democracy, et al., FTC, *In the Matter of Children’s Online Privacy Protection Rule* at 13-14 (Dec. 23, 2011).

⁸⁵ Staff Report, *Online Advertising and Hidden Hazards to Consumer Security and Data Privacy*, Permanent Subcommittee on Investigations of the U.S. Senate Homeland Security and Governmental Affairs Committee (May 15, 2014), at 1 (emphasis added).

132. A 2012 chart of the mobile digital marketplace,⁸⁶ attached hereto as Exhibit 2, indicates that hundreds of intermediaries from location trackers to data aggregators to ad networks “touch” the data that is used to track and profile an individual in a given online transaction.

133. By 2017, the number of unique companies in this space swelled to almost 5,000, as shown in Exhibit 3, attached hereto.⁸⁷

134. In the course of disclosing Personal Data to select and serve an advertisement (or to conduct any third-party analytics or otherwise monetize user data), the developer and its partner SDKs pass identifying user data to an ever-increasing host of third-parties, who, in turn, may pass along that same data to *their* affiliates. Each entity may use that data to track users over time and across the Internet, on a multitude of increasingly complex online pathways, with the shared goal of targeting users with advertisements.

135. The ability to serve targeted advertisements to (or to otherwise profile) a specific user no longer turns upon obtaining the kinds of data with which most consumers are familiar (name, email addresses, etc.), but instead on the surreptitious collection of persistent identifiers or geolocation, which are used in conjunction with other data points to build robust online profiles. These data points are better tracking tools than traditional identifiers because they are unique to each individual, making them more akin to a social security number. Once such uniquely identifiable data are sent “into the marketplace,” they are exposed to—and thereafter may be collected and used by—an almost innumerable set of third-parties.

⁸⁶ Laura Stampler, *This RIDICULOUS Graphic Shows How Messy Mobile Marketing Is Right Now*, Business Insider (May 23, 2012) (available at <http://www.businessinsider.com/this-ridiculous-graphic-shows-how-the-insanely-complicated-world-of-mobile-marketing-works-2012-5>) (accessed on Sept. 4, 2018).

⁸⁷ Scott Brinker, *Marketing Technology Landscape Supergraphic*, Chief Marketing Technology Blog (May 10, 2017) (available at <https://chiefmartec.com/2017/05/marketing-technology-landscape-supergraphic-2017/>) (accessed on Sept. 4, 2018).

136. Permitting technology companies to obtain children's Personal Data exposes those children to targeted advertising. The ad networks, informed by the surreptitious collection of Personal Data from children, will assist in the sale of advertising placed within the gaming apps and targeted specifically to children.

137. As established above, Defendants exfiltrate children's Personal Data or other information about their online behavior, which is then sold to third-parties who track multiple data points associated with those children, analyzed with the sophisticated algorithms of Big Data to create a user profile, and then used to serve targeted advertising to children whose profiles fit a set of demographic and behavioral traits.

2. Defendants Use Children's Personal Data to Target Them, Despite Children's Heightened Vulnerability to Advertising.

138. Defendants use children's Personal Data to serve them targeted advertising. Defendants engage in this behavior despite the known risks associated with and ethical norms surrounding advertising to children.⁸⁸

139. Advertisers regard children to be valuable advertising targets.⁸⁹ Children influence the buying patterns of their families—an influence that amounts to billions of dollars each year—and have lucrative spending power themselves.⁹⁰ Children and teens are thus prime targets for advertisers.

⁸⁸ Kristien Daems, Patrick De Pelsmacker & Ingrid Moons, *Advertisers' perceptions regarding the ethical appropriateness of new advertising formats aimed at minors*, J. of Marketing Communications (2017) at 13 (“In general, all advertising professionals acknowledge that children are a vulnerable advertising target group.”).

⁸⁹ Lara Spiteri Cornish, “Mum, can I play on the Internet?” *Parents' understanding, perception, and responses to online advertising designed for children*, 33 Int'l J. Advertising 437, 438 (2014) (“Indeed, in recent years, marketers targeting children have developed a strong online presence . . .”); Issie Lapowsky, “Why Teens are the Most Elusive and Valuable Customers in Tech,” Inc., available at <https://www.inc.com/issie-lapowsky/inside-massive-tech-land-grab-teenagers.html> (accessed on Sept. 4, 2018).

⁹⁰ Sandra L. Calvert, *Children as Consumers: Advertising and Marketing*, 18 Future Child 205,

140. Tiny Lab intentionally profits from embedding advertising SDKs, to collect and exploit children's Personal Data, into its "free-to-play" Gaming Apps.

141. Defendants target advertising efforts at children despite widespread awareness that children are more vulnerable to deception by advertisers because they are easily influenced by its content, lack the cognitive skills to understand the intention of advertisers, and can struggle to distinguish between advertisements and other content.⁹¹ This is particularly problematic when targeted advertising is used which, by design, more effectively sways target audiences.⁹² Research supports that online advertisements pose heightened risks to children.⁹³

142. Exposure to advertising can also lead to negative outcomes for children, including increasing conflict with their parents, cynicism, health issues, and increased materialism.⁹⁴

143. Children often lack the skills and knowledge necessary to assess and appreciate the risks associated with online data exfiltration and tracking.⁹⁵ Even attempts to disclose privacy-violative behavior are not easily understood. Research has found that policies explaining the exfiltration and use of children's data are difficult even for adults to understand, and marketers make no effort to explain their targeted marketing practices to child and teen audiences in developmentally appropriate and easy-to-understand ways.⁹⁶ This practice "could

207 (2008).

⁹¹ *Online Advertising on Popular Children's Websites: Structural Features and Privacy Issues*, *infra* at 143, at 1510 (collecting studies); *Children as Consumers: Advertising and Marketing*, *supra* at n.90; *Advertisers' perceptions regarding the ethical appropriateness of new advertising formats aimed at minors*, *infra* at 169, at 2 (collecting studies); 'Mum, can I play on the internet?', *supra* at n.89, at 438-39 (collecting studies).

⁹² Olesya Venger, *Internet Research in Online Environments for Children: Readability of Privacy and Terms of Use Policies; The Uses of (Non)Personal Data by Online Environments and Third-Party Advertisers*, 10 *Journal of Virtual Worlds Research* 1, 8 (2017).

⁹³ *Mum, can I play on the Internet?*, *supra* at n.89, at 440-42 (collecting studies).

⁹⁴ *Children as Consumers: Advertising and Marketing*, *supra* at n.90, at 118-119.

⁹⁵ Ilene R. Berson & Michael J. Berson, *Children and their Digital Dossiers: Lessons in Privacy Rights in the Digital Age*, 21 *Int'l J. of Social Education* 135 (2006).

⁹⁶ *Internet Research in Online Environments for Children*, *supra* at n.92, at 9.

mislead these vulnerable emerging consumers into thinking that they are only playing games and their data are not collected for any purpose.”⁹⁷

3. Defendants Exfiltrate and Analyze Children’s Personal Data to Track the Effect of Their Ads on Children’s Behavior.

144. Defendants exfiltrate and analyze children’s Personal Data before and after serving advertisements. On the front end, the data helps them know what ads to serve (based on children’s demographics and behaviors). On the back end, the data helps them determine whether the ad is successful in affecting children’s behavior. This is called ad attribution.

145. Defendants track the impact and value of the ads served by tracking children’s activities across the Internet after they interact with those ads.

146. Defendants want to reward advertisers whose ads influenced children’s behavior. But such attribution requires surveillance. For example, if 10-year-old Sally is served an ad for a pony game based on her age, implied income, and online activities, and later goes and downloads that pony game, the advertiser responsible for the pony game ad wants that download attributed to them, so that they can get paid for that action. But the only way for the advertising companies to connect the Sally that saw the ad with the Sally that downloaded the app is to track Sally’s online activities after she was shown the ad through the app—such as by tracking her persistent identifier.

147. The SDK Defendants market their ability to offer ad attribution services through their SDKs (as well as the attendant value of those services). For example, in a 2016 white paper titled “Why [Mobile] [In-app] Programmatic? A Marketer's Guide” (alterations original) Twitter/MoPub states:

Although there aren’t cookies in mobile in-app, marketers are able to measure the effects of their mobile web and app campaigns with

⁹⁷ *Internet Research in Online Environments for Children*, *supra* at n.92, at 10.

growing sophistication and precision, including the use of Device ID. Mobile attribution partners [such as MoPub] help collect advanced user data that can then be coupled with other data sources to inform future campaigns and develop lookalike strategies.⁹⁸

148. Similarly, ironSource recognizes that “the success of mobile advertising rests on knowing whether the user made the download after they saw the ad” and mobile advertising companies have “developed clever ways of figuring out if the user who clicked on the ad is indeed the same user who downloaded and opened the app.”⁹⁹ ironSource markets its ability to attribute action back to users, whether or not they click on an ad encouraging that action.¹⁰⁰ InMobi markets its ability to do the same by partnering with other ad networks.¹⁰¹ AppLovin describes attribution as “the only way mobile marketers can inform decisions in order to optimize their marketing spend.”¹⁰²

149. Defendants exfiltrate children’s Personal Data from their devices in order to target them for advertising based on their behavior, demographics, and location. Defendants continue to track children via their Personal Data after ads are shown in order to monitor their behavior into the future, and analyze whether and how it was influenced by those same targeted ads. This

⁹⁸ *Why [Mobile] [In-app] Programmatic? A Marketer's Guide*, MoPub, (2016) (available at <https://www.slideshare.net/MoPubInsights/why-mobile-inapp-programmatic-a-marketers-guide>) (accessed on June 4, 2018).

⁹⁹ Daniel Rosenberg, *What the Hell is Mobile Attribution*, ironSource Blog (Jan. 14, 2016) (available at <https://www.ironsrc.com/news/what-is-mobile-attribution-and-how-will-it-change-in-2016/>) (accessed on June 4, 2018).

¹⁰⁰ *View-Through Attribution*, ironSource Glossary (Mar. 12, 2018) (available at <https://www.ironsrc.com/glossary/view-through-attribution/>) (accessed on Sept. 4, 2018).

¹⁰¹ Rajesh Pantina, *View-Through Attribution: Shifting Gears in Performance Marketing*, InMobi Blog (Aug. 24, 2016) (available at <https://www.inmobi.com/blog/2016/08/24/view-through-attribution-shifting-gears-in-performance-marketing>) (accessed on Sept. 4, 2018).

¹⁰² Katy Jensen, *Ad Tech Deconstructed: What is mobile attribution?*, AppLovin Blog, (July 31, 2018) (available at <https://blog.applovin.com/ad-tech-deconstructed-what-is-mobile-attribution/>) (accessed on Sept. 4, 2018).

ongoing exfiltration, tracking, and analysis violate child consumers' privacy and exploit their vulnerabilities as children.

4. Defendants Use Personal Data to Encourage Children to Continue Using the App, Increasing the Risks Associated with Heightened Mobile Device Usage.

150. Defendants, and third-party advertisers, benefit from increased mobile device usage among children. The longer and more often a child plays Defendants' games, the more Personal Data about that child the Defendants can exfiltrate and commercialize. As the app is free, this increased opportunity to exfiltrate and monetize children's Personal Data and expose them to advertising is critically important to Defendants.¹⁰³

151. The mobile advertising ecosystem does not simply benefit from increases in app use and mobile device addiction, it actively feeds it. Defendants and their advertising partners use Personal Data to program their apps to "hook" children, and to keep them playing the app.¹⁰⁴

152. A key service marketed by SDK Defendants is the ability to use marketing to retain app users, *i.e.*, to keep children playing an app. The SDK Defendants market their ability to help app developers such as Tiny Lab increase user retention, and thereby their profits. Children are specifically targeted as part of this goal.

153. These retention services are fueled by children's Personal Data. To enhance retention, the SDK Defendants use children's Personal Data to analyze their demographics and behavior, and trigger events—both within the app and across the Internet—that will encourage them to play the app more often and for longer periods.

¹⁰³ *Your phone is trying to control your life*, PBS News Hour (available at <https://www.youtube.com/watch?v=MacJ4p0vITM>) (accessed on Sept. 4, 2018).

¹⁰⁴ *Brain Hacking*, 60 Minutes (Apr. 9, 2017) (available at <https://www.youtube.com/watch?v=awAMTQZmvPE>) (accessed on Sept. 4, 2018); Nicholas Kardaras, *Glow Kids: How Screen Addiction Is Hijacking Our Kids - and How to Break the Trance* (2015), at XVIII-XIX, 22, 32.

154. Defendants exfiltrate children's Personal Data from their devices and use it for tracking and targeting to entice the children to play the app longer and more often. Defendants use sophisticated algorithms to determine whether and when to target children with specific in-app cues or out-of-app ads. This behavior increases Defendants' revenue, all the while violating children's privacy and exposing them to the negative outcomes associated with increased mobile device usage by children.

155. Defendants' "retention" efforts take place in a context where mobile device usage among children is widespread and growing. As of 2017, 95% of families with children younger than 8-years-old had a smartphone, and 78% had a tablet.¹⁰⁵ The proportion of homes with a tablet has nearly doubled over the past four years.¹⁰⁶ Often, children have their own devices; as of 2017, 45% of children younger than 8-years-old had their own mobile device, up from only 3% in 2011 and 12% in 2013.¹⁰⁷

156. Children spend increasingly more time on mobile devices. On average, a child younger than 8-years-old spends 48 minutes every day on a mobile device, more than four times the average time spent in 2013,¹⁰⁸ while children between the ages of eight and twelve spend 141 minutes on mobile devices and teens spend 252 minutes.¹⁰⁹ Mobile games are popular among children, second only to watching TV or videos.¹¹⁰ Children younger than 8-years-old spend an

¹⁰⁵ Victoria Rideout, *The Common Sense Census: Media Use By Kids Age Zero To Eight*, Common Sense Media (2017) at 3 (available at <https://www.common sense media.org/research/the-common-sense-census-media-use-by-kids-age-zero-to-eight-2017>) (accessed on Sept. 4, 2018).

¹⁰⁶ *Id.*; *Media Use By Kids Age Zero To Eight*, *supra* at n.105, at 23

¹⁰⁷ *Id.*

¹⁰⁸ *Id.* at 3

¹⁰⁹ Victoria Rideout, *The Common Sense Census: Media Use by Tweens and Teens*, Common Sense Media (2015) at 21 (available at <https://www.common sense media.org/research/the-common-sense-census-media-use-by-tweens-and-teens>) (accessed on Sept. 4, 2018).

¹¹⁰ *Media Use By Kids Age Zero To Eight*, *supra* at n.105, at 23

average of 16 minutes every day gaming, more than doubling since 2013.¹¹¹ 27% of children ages 8 to 18 report playing mobile games every day,¹¹² and those who play games average about 70 minutes *every day* doing so.¹¹³

157. As the use of mobile devices rises, so too do awareness of and concern about the effects of this use on children.¹¹⁴ The consequences of mobile device overuse, particularly among children, is well-known in the tech industry,¹¹⁵ with many industry leaders refusing to allow their own children to own or use devices,¹¹⁶ or attend schools where such devices are prevalent.

158. In a recent study, 40% of parents of 5- to 8-year-olds reported difficulty getting their children to turn off mobile devices.¹¹⁷ 53% of teens and 72% of kids age 8-12 report conversations with their parents about how much time they spend on mobile devices.¹¹⁸ Parents

¹¹¹ *Id.* at 31

¹¹² *Media Use by Tweens and Teens*, *supra* at n.109, at 15

¹¹³ *Id.* at 24

¹¹⁴ See, e.g., Xiaomei Cai and Xiaoquan Zhao, *Online Advertising on Popular Children's Websites: Structural Features and Privacy Issues*, 29 *Computers in Human Behavior* 1510-1518 (2013); Barry Rosenstein and Anne Sheehan, *Open letter from JANA Partners and CALSTRS to Apple Inc.*, Jan. 4, 2018 (available at <https://thinkdifferentlyaboutkids.com/index.php?acc=1>) (accessed 4) (letter to Apple citing "growing body of evidence" that increasing mobile device use leads to "unintentional negative consequences" for young users).

¹¹⁵ See, e.g., Farhad Majoo, *It's Time for Apple to Build a Less Addictive iPhone*, *New York Times* (Jan. 17, 2018) (available at <https://www.nytimes.com/2018/01/17/technology/apple-addiction-iphone.html>) (accessed on Sept. 4, 2018) ("Tech 'addiction' is a topic of rising national concern."); Thuy Ong, *Sean Parker on Facebook: 'God only knows what it's doing to our children's brains'*, *The Verge*, Nov. 9, 2017 (available at <https://www.theverge.com/2017/11/9/16627724/sean-parker-facebook-childrens-brains-feedback-loop>) (accessed on Sept. 4, 2018) (former tech industry leader recognizing that app creators intentionally "exploit[] human vulnerabilities" to increase app engagement).

¹¹⁶ Nick Bilton, *Steve Jobs Was a Low-Tech Parent*, *New York Times* (September 10, 2014) (available at <https://www.nytimes.com/2014/09/11/fashion/steve-jobs-apple-was-a-low-tech-parent.html>) (accessed on Sept. 4, 2018); Claudia Dreifus, *Why We Can't Look Away From Our Screens*, *New York Times* (March 6, 2017) (available at <https://www.nytimes.com/2017/03/06/science/technology-addiction-irresistible-by-adam-alter.html>) (accessed on Sept. 4, 2018).

¹¹⁷ *Media Use By Kids Age Zero To Eight*, *supra* at 105, at 41

¹¹⁸ *Media Use by Tweens and Teens*, *supra* at n.109, at 71

are increasingly concerned about their children's mobile device usage, and for good reason: research has associated increasing usage with negative consequences for children,¹¹⁹ such as increasing rates of ADHD,¹²⁰ depression,¹²¹ anxiety,¹²² and reduced focus in the classroom.¹²³ One recent study showed that children between the ages of 12 and 18 who spent more time playing games had lower than average social-emotional well-being.¹²⁴

159. Most parents believe that children are better off spending less time on their mobile devices.¹²⁵ Three out of four parents are worried about their children's use of screen devices.¹²⁶ A recent study showed that 67% of parents of children under age 8 worry about companies collecting data about their children through media, while 69% are concerned about too much advertising.¹²⁷

160. Such fear is well-founded. The World Health Organization ("WHO") recently added "gaming disorder" to its globally-recognized compendium of medical conditions and diagnoses. In the 11th International Classification of Diseases, the WHO describes the condition as "impaired control over gaming, increasing priority given to gaming over other activities to the extent that gaming takes precedence over other interests and daily activities, and continuation or escalation of gaming despite the occurrence of negative consequences."¹²⁸

¹¹⁹ Ryan M. Atwood et al., *Adolescent Problematic Digital Behaviors Associated with Mobile Devices*, 19 North American J. Psychology 659-60 (2017) (collecting studies); *Id.* at 672-73 (finding that more than 82.5% of teens were classified as over-users of the Internet, and finding that mobile device usage increased Internet usage).

¹²⁰ *Glow Kids*, *supra* at n.104, at 123-124

¹²¹ *Id.* at 127

¹²² *Id.*; *Brain Hacking*, *supra* at n.104

¹²³ *Glow Kids*, *supra* at n.104, at 123

¹²⁴ *Media Use by Tweens and Teens*, *supra* at n.109, at 79

¹²⁵ *Media Use By Kids Age Zero To Eight*, *supra* at n.105, at 39

¹²⁶ *Id.* at 42

¹²⁷ *Id.*

¹²⁸ *Gaming Disorder*, World Health Organization, (available at <http://www.who.int/features/qa/gaming-disorder/en/>) (accessed 4); *see also* Haley Tsukayama,

H. State Privacy Laws Protect Children and Their Parents from Privacy-Invasive Tracking, Profiling, and Targeting of Children Online.

161. Invasion of privacy has been recognized as a common law tort for over a century. *Matera v. Google Inc.*, 15-CV-0402, 2016 WL 5339806, at *10 (N.D. Cal, Sept. 23, 2016) (citing Restatement (Second) of Torts §§ 652A-I for the proposition “that the right to privacy was first accepted by an American court in 1905, and ‘a right to privacy is now recognized in the great majority of the American jurisdictions that have considered the question’”). *Id.* As Justice Brandeis explained in his seminal article, *The Right to Privacy*, “[t]he common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.” Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890). The Second Restatement of Torts recognizes the same privacy rights through its tort of intrusion upon seclusion, explaining that “[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy.” Restatement (Second) of Torts § 652B (1977). The Supreme Court has similarly recognized the primacy of privacy rights, explaining that the Constitution operates in the shadow of a “right to privacy older than the Bill of Rights.” *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965).

162. Most recently, the Supreme Court explicitly recognized the reasonable expectation of privacy an individual has in her cell phone, and the Personal Data generated therefrom, in its opinion in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). There, the Court held that continued access to an individual’s cell phone location data constituted a search under the Fourth Amendment, and that the third-party doctrine (which obviates Fourth Amendment

Video Game Addiction is a Real Condition, WHO Says. Here’s What That Means, Washington Post (Jun. 18, 2018) (available at https://www.washingtonpost.com/news/the-switch/wp/2018/06/18/video-game-addiction-is-a-real-condition-who-says-heres-what-that-means/?utm_term=.9f718977d0e5) (accessed on Sept. 4, 2018).

protections when a party knowingly provides information that is the subject of the search to third-parties) did not apply to such data. Critical to the Court’s analysis was the fact that

a cell phone—almost a “feature of human anatomy[.]”—tracks nearly exactly the movements of its owner....A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales....Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.

Id. at 2218 (internal citations omitted).

163. It is precisely because of devices’ capacity for “near perfect surveillance” that courts have consistently held that time-honored legal principles recognizing a right to privacy in one’s affairs naturally apply to online monitoring.

1. Defendants’ Surreptitious and Deceptive Collection of Personal Data Violates Children’s Reasonable Expectations of Privacy and is Highly Offensive.

164. A reasonable person believes the conduct described above violates children’s expectations of privacy.

165. A survey conducted by the Center for Digital Democracy (“CDD”) and Common Sense Media of more than 2,000 adults found overwhelming support for the basic principles of privacy embedded in state common law, as well as federal law.¹²⁹ The parents who were polled responded as follows when asked whether they agreed or disagreed with the following statements:

¹²⁹ “Survey on Children and Online Privacy, Summary of Methods and Findings,” Center for Digital Democracy, (available at <http://www.centerfordigitaldemocracy.org/sites/default/files/COPPA%20Executive%20Summary%20and%20Findings.pdf>) (accessed on Sept. 4, 2018).

a. “It is okay for advertisers to track and keep a record of a child’s behavior online if they give the child free content.”

- 5% strongly agree
- 3% somewhat agree
- 15% somewhat disagree
- **75% strongly disagree**
- 3% do not know or refused to answer

b. “As long as advertisers don’t know a child’s name and address, it is okay for them to collect and use information about the child’s activity online.”

- 3% strongly agree
- 17% somewhat agree
- 10% somewhat disagree
- **69% strongly disagree**
- 1% do not know or refused to answer

c. “It is okay for advertisers to collect information about a child’s location from that child’s mobile phone.”

- 6% strongly agree
- 3% somewhat agree
- 7% somewhat disagree
- **84% strongly disagree**
- less than 1% do not know or refused to answer

d. “Before advertisers put tracking software on a child’s computer, advertisers should receive the parent’s permission.”

- **89% strongly agree**
- 5% somewhat agree
- 2% somewhat disagree
- 4% strongly disagree
- less than 1% do not know or refused to answer

e. When asked, “There is a federal law that says that online sites and companies need to ask parents’ permission before they collect personal information from children under age 13. Do you think the law is a good idea or a bad idea?” 93% said it was a good idea, 6% said it was a bad idea, and 1% did not know or refused to answer.

f. Non-parent adults tended to answer in the same way, although parents were more protective of their children's privacy.

166. In a 2013 primer designed for parents and kids to understand their privacy rights online, the CDD noted similar findings:¹³⁰

a. 91% of both parents and adults believe it is not okay for advertisers to collect information about a child's location from that child's mobile phone.

b. 96% of parents and 94% of adults expressed disapproval when asked if it is "okay OK [sic] for a website to ask children for personal information about their friends."

c. 94% of parents, as well as 91% of adults, believe that advertisers should receive the parent's permission before putting tracking software on a child's computer.

167. In a Pew Research Center study, nearly 800 Internet and smartphone users were asked the question, "how much do you care that only you and those you authorize should have access to information about where you are located when you use the Internet?" 54% of adult Internet users responded "very important," 16% responded "somewhat important," and 26% responded "not too important."¹³¹

168. According to the same study, "86% of Internet users have tried to be anonymous online and taken at least one step to try to mask their behavior or avoid being tracked." For example, 64% of adults claim to clear their cookies and browser histories in an attempt to be less visible online.

169. Smartphone owners are especially active when it comes to these behaviors. Some 50% of smartphone owners have cleared their phone's browsing or search history, while 30%

¹³⁰ See "The New Children's Online Privacy Rules: What Parents Need to Know," Center for Digital Democracy, 6 (June 2013) (available at <https://www.democraticmedia.org/sites/default/files/CDDCOPPAparentguideJune2013.pdf>) (accessed on Sept. 4, 2018).

¹³¹ Lee Rainie, et al., *Anonymity, Privacy, and Security Online*, Pew Research Center 7 (Sept. 5, 2013) (available at <http://pewinternet.org/Reports/2013/Anonymity-online.aspx>) (accessed 4).

have turned off the location tracking feature on their phone due to concerns over who might access that information.¹³² Such behaviors exemplify people's expectation that their personal information—including their location—not be tracked by others online.

170. In another study by the Pew Research Center done as part of its "Internet & American Life" project, respondents were asked, "Which of the following statements comes closest to exactly how you, personally, feel about targeted advertising being used online—even if neither is exactly right?" 68% said, "I'm not okay with it because I don't like having my online behavior tracked and analyzed." 28% said, "I'm okay with it because it means I see ads and get information about things I'm really interested in."¹³³ Thus, more often than not, attitudes toward data collection for use in targeted advertising are negative.

171. A survey of 802 parents and their age 12 to 17 year-old teenage children showed that "81% of parents of online teens say they are concerned about how much information advertisers can learn about their child's online behavior, with some 46% being 'very' concerned."¹³⁴

172. A study comparing the opinions of young adults between the ages of 18 to 23 with other typical age categories (25-34, 35-44, 45-54, 55-64, and 65+) found that a large percentage is in harmony with older Americans regarding concerns about online privacy, norms, and policy suggestions.¹³⁵ For example, 88% of young adults surveyed responded that "there

¹³² Jan Lauren Boyles, et al., *Privacy and Data Management on Mobile Devices*, Pew Research Center, Sept. 5, 2012 (available at http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf) (accessed 4).

¹³³ Kristen Purcell, et al., *Search Engine Use*, Pew Research Center 2012 (available at http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_Search_Engine_Use_2012.pdf) (accessed 4).

¹³⁴ Mary Madden, et al., *Parents, Teens, and Online Privacy*, Pew Research Center 2012 (available at http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_ParentsTeensAndPrivacy.pdf) (accessed 4).

¹³⁵ Chris Hoofnagle, et al., *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?* (2010) (available at

should be a law that requires websites and advertising companies to delete all stored information about an individual”; for individuals in the 45-54 age range, 94% approved of such a law.

173. The same study noted that “[o]ne way to judge a person’s concern about privacy laws is to ask about the penalties that companies or individuals should pay for breaching them.” A majority of the 18-24 year olds polled selected the highest dollar amount of punishment (“more than \$2,500”) in response to how a company should be fined if it purchases or uses someone’s personal information illegally; across all age groups, 69% of individuals opted for the highest fine. Finally, beyond a fine, around half of the sample (across all age groups) chose the harshest penalties for companies using a person’s information illegally—putting them out of business and jail time.

174. Another study’s “findings suggest that if Americans could vote on behavioral targeting today, they would shut it down.” The study found that 66% of 1000 polled individuals over the age of 18 did not want online advertisements tailored for them, and that when the same individuals were told that tailored advertising was “based on following them on other websites they have visited,” the percentage of respondents rejecting targeted advertising shot up to 84%.¹³⁶

175. Even when consumers are told that online companies will follow them “anonymously,” Americans are still averse to this tracking: 68% definitely would not allow it, and 19% would probably not allow it.

176. The study found that 55% of 18-24 year old Americans rejected tailored advertising when they were not informed about the mechanics of targeted advertising. As with the general sample, the percentage of rejections shot up to 67% when those 18-24 year olds were

<http://ssrn.com/abstract=1589864>) (accessed 4).

¹³⁶ Joseph Turow, et al., *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* (2009) (available at <http://ssrn.com/abstract=1478214>) (accessed 4).

informed that tailored advertising was based on their activities on the website they are visiting, and then 86% when informed that tailored ads were based on tracking on “other websites” they had visited. Despite the overwhelming aversion to targeted advertising, these findings suggest that public concern about privacy-intrusive targeted advertising is *understated* based on the fact that the public may not fully understand how a targeted advertisement is delivered to it. When properly understood by consumers, targeted advertising, and the tracking and profiling in the background, is decried across all age groups.

177. A survey on consumer expectations in the digital world, conducted by Deloitte’s Technology, Media & Telecommunications practice¹³⁷ and based on polling conducted in 2017 of 2,088 individuals (from the following age groups: ages 14-20 (born 1997-2003); ages 21-34 (born 1983-1996); ages 35-51 (born 1966-1982); ages 52-70 (born 1947-1965); ages 71+ (born 1946 or earlier) found:

- a. 73% of all U.S. consumers indicated they were concerned about sharing their personal data online and the potential for identity theft.
- b. In 2017, there was a 10-point drop in willingness to share personal data in exchange for personalized advertising (from 37% to 27%).
- c. The reason for the sudden change in U.S. consumers’ attitudes is they overwhelmingly lack confidence in companies’ ability to protect their data: 69% of respondents across generations believe that companies are not doing everything they can to protect consumers’ personal data.

¹³⁷ Kevin Westcott, et al., *Digital Media Trends Survey: A New World of Choice for Digital Consumers*, Center for Technology, Media & Telecommunications, 12th ed. (available at https://www2.deloitte.com/content/dam/insights/us/articles/4479_Digital-media-trends/4479_Digital_media%20trends_Exec%20Sum_vFINAL.pdf) (accessed 4).

d. 73% of all consumers across all generations said they would be more comfortable sharing their data if they had some visibility and control. In addition, 93% of U.S. consumers believe they should be able to delete their online data at their discretion.

178. In the same vein, one news organization recently summarized a *Journal of Consumer Research* article, capturing society's discomfort with and feelings of revulsion toward the practice of targeted advertising and the data exfiltration required: "There's something unnatural about the kind of targeting that's become routine in the ad world, this paper suggests, something taboo, a violation of norms we consider inviolable — it's just harder to tell they're being violated online than off. But the revulsion we feel when we learn how we've been algorithmically targeted, the research suggests, is much the same as what we feel when our trust is betrayed in the analog world."¹³⁸

179. By collecting and sharing children's Personal Data in order to profile and track them across multiple online platforms, and failing first to obtain verifiable parental consent, Defendants have breached children's and parents' expectations of privacy.

180. Various other sources provide manifestations of society's deep revulsion toward companies' collecting or accessing personal information for tracking and profiling purposes:

a. Legislative enactments reflect society's growing concern for digital privacy and security. For example, N.M. Stat. Ann. § 50-4-34 (2013) provides that employers may not force an applicant to provide access to her online social media accounts as a condition of employment. N.M. Stat. Ann. § 21-1-46 (2013) provides the same protections to applicant students in the post-secondary education context. Similarly, New Mexico's data breach notification law—N.M. Stat. Ann. § 57-12C-1, *et seq.* (2017)—imposes a duty of care on

¹³⁸ Sam Biddle, *You Can't Handle the Truth about Facebook Ads, New Harvard Study Shows* The Intercept, May 9, 2018 (available at https://theintercept.com/2018/05/09/facebook-ads-tracking-algorithm/?utm_source=digg&utm_medium=email) (accessed on Sept. 4, 2018).

businesses who collect and maintain citizens' personal data, recognizing the dangers inherent in unknown and unauthorized parties accessing such data.

b. Scholarly literature about the evolution of privacy norms recognizes society's expectation of determining for oneself when, how, and the extent to which information about one is shared with others.

c. Self-regulation agencies in the online advertising industry note the American consumer's reasonable concern with online privacy (92% of Americans worry about their online data privacy) and the top causes of that concern include Defendants' conduct at issue here: companies collecting and sharing personal information with other companies.¹³⁹

2. Defendants' Breach of Privacy Norms Is Compounded by Defendants' Targeting, Tracking, and Profiling of Children.

181. Defendants' unlawful intrusion into children's privacy is made even more egregious and offensive by the fact that the SDK Defendants and Tiny Lab have targeted and collected *children's* information, without obtaining verifiable parental consent.

182. Parents' interest in the care, custody, and control of their children is perhaps the oldest of the fundamental liberty interests recognized by society. The history of Western civilization reflects a strong tradition of parental concern for the nurture and upbringing of children in light of children's vulnerable predispositions. Our society recognizes that parents should maintain control over who interacts with their children and how in order to ensure the safe and fair treatment of their children.

183. Because children are more susceptible to deception and exploitation than adults, society has recognized the importance of providing added legal protections for children, often in the form of parental consent requirements.

¹³⁹ *Data Privacy is a Major Concern for Consumers*, TrustArc Blog, (Jan. 28, 2015) (available at <https://www.trustarc.com/blog/2015/01/28/data-privacy-concern-consumers/>) (accessed on Sept. 4, 2018).

184. By way of example, American society has expressed heightened concern for the exploitation of children in numerous ways:

a. At common law, children under the age of eighteen do not have full capacity to enter into binding contracts with others. The law shields minors from their lack of judgment, cognitive development, and experience.

b. At the federal level, COPPA protects, *inter alia*, children's Personal Information from being collected and used for targeted advertising purposes without parental consent, and reflects a clear nationwide norm about parents' expectations to be involved in how companies profile and track their children online.

c. Under the federal Family Educational Rights and Privacy Act of 1974 ("FERPA"), students have a right of privacy regarding their school records, but the law grants parents a right to access and disclose such records. 20 U.S.C. § 1232g(a)(4).

d. Under state law, New Mexico has expressly adopted and codified the privacy and consent protections for student data also afforded by FERPA in its own state analog: N.M. Code R. § 6.29.1.9.

185. Legislative commentary about the need for federal law to provide protections for children provides another expression of society's expectation that companies should not track *children* online without obtaining parental consent. For example, when discussing the need for federal legislation to protect children's privacy—which eventually led to Congress passing COPPA—Senator Richard Bryan (the primary author of the COPPA bill) stated: "Parents do not always have the knowledge, the ability, or the opportunity to monitor their children's online activities, and that is why Web site operators should get parental consent prior to soliciting personal information. The legislation that Senator McCain and I have introduced will *give*

*parents the reassurance that when our children are on the Internet they will not be asked to give out personal information to commercial Web site operators without parental consent.”*¹⁴⁰

186. The advertising industry’s own privacy standards, and the self-regulatory agencies which serve it, also support enhanced protections for children online, including obtaining parental consent.

187. For example, a survey of professionals in the advertising industry found that a “substantial majority of [advertising professionals] (79%) agrees that the collection of personal information of children should be prohibited,” and over “[h]alf of the advertisers (56.8%) agree with this statement if teenagers are concerned.”¹⁴¹

188. Further, “[t]he majority of advertisers agree with the statement that parents should give their permission for the data collection of their children (89.5%) and teenagers (78.9%).”

189. In the same vein, the Children’s Advertising Review Unit, an arm of the advertising industry’s self-regulation branch, recommends that companies take the following steps, *inter alia*, to meet consumers’ reasonable expectations of privacy and avoid violating the law.¹⁴²

a. Advertisers have special responsibilities when advertising to children or collecting data from children online. They should take into account the limited knowledge, experience, sophistication, and maturity of the audience to which the message is directed. They should recognize that younger children have a limited capacity to evaluate the credibility of

¹⁴⁰ S. 2326: *Children’s Online Privacy Protection Act of 1998*, Hearing before Senate Subcommittee on Communications, S. Hrg. 105-1069, at 4 (Sept. 23, 1998) (Statement of Sen. Bryan) (emphasis added).

¹⁴¹ Kristien Daems, Patrick De Pelsmacker & Ingrid Moons, *Advertisers’ perceptions regarding the ethical appropriateness of new advertising formats aimed at minors*, J. Marketing Comms. 8 (2017).

¹⁴² Children’s Advertising Review Unit, *Self-Regulatory Program for Children’s Advertising* (2014) (available at <http://www.asrcreviews.org/wp-content/uploads/2012/04/Self-Regulatory-Program-for-Childrens-Advertising-Revised-2014-.pdf>) (accessed on Sept. 74, 2018).

information, may not understand the persuasive intent of advertising, and may not even understand that they are being subjected to advertising.

b. Operators should disclose passive means of collecting information from children (*e.g.*, navigational tracking tools, browser files, persistent identifiers, etc.) and what information is being collected.

c. Operators must obtain “verifiable parental consent” before they collect, use or disclose personal information to third-parties, except those who provide support for the internal operation of the website or online service and who do not use or disclose such information for any other purpose.

d. To respect the privacy of parents, operators should not maintain in retrievable form information collected and used for the sole purpose of obtaining verifiable parental consent or providing notice to parents, if consent is not obtained after a reasonable time.

e. Operators should ask screening questions in a neutral manner so as to discourage inaccurate answers from children trying to avoid parental permission requirements.

f. Age-screening mechanisms should be used in conjunction with technology, *e.g.*, a session cookie, to help prevent underage children from going back and changing their age to circumvent age-screening.

190. By failing to (1) obtain verifiable parental consent, (2) disclose to parents the nature of their data collection practices, and (3) take other steps to preclude children from accessing apps that surreptitiously capture their Personal Information, Defendants have breached parents’ and their children’s reasonable expectations of privacy, in contravention not only of COPPA, but also of privacy norms that are reflected in consumer surveys, centuries of common law, state and federal statutes, legislative commentaries, industry standards and guidelines, and scholarly literature.

I. Tiny Lab's Omissions and Misrepresentations Create the False Impression That the Gaming Apps are Compliant with Privacy Laws and Social Norms.

191. Tiny Lab markets the Gaming Apps as suitable for children, both explicitly (through public-facing representations) and implicitly (through the game's content, design, and distribution channels).

192. However, despite doing so—and despite having indisputable knowledge that children play on the app—Tiny Lab omits any meaningful mention of the privacy-invasive collection of Personal Data by the SDKs embedded within the Gaming Apps; and indeed makes affirmative misrepresentations regarding the collection of children's Personal Data.

193. Tiny Lab creates the false impression that the Gaming Apps conform to established norms regarding children's privacy, and that Defendants' behavior respect those norms.

1. Tiny Lab Markets the Gaming Apps as Suitable for Children and in Compliance With All Applicable Privacy Laws and Norms.

194. Tiny Lab expressly designed all the Gaming Apps¹⁴³ to be played by minor children.¹⁴⁴

195. Indeed, in an interview with Tiny Lab's CEO and Founder Jonas Abromaitis, Mr. Abromaitis explains that the company's business model is premised exclusively on "free-to-play mobile games for kids and toddlers."¹⁴⁵ Providing more backstory into the company's history, Mr. Abromaitis explained that he created the company's flagship game, Fun Kid Racing, after he had

¹⁴³ Tiny Lab makes substantially similar representations and omissions with regard to all the Gaming Apps identified herein. Similarly, Tiny Lab markets all the Gaming Apps in an identical manner in all material respects.

¹⁴⁴ See also, Section IV.D, *supra*.

¹⁴⁵ *Tiny Lab Productions: Subscription Model Sounds Promising*, Startup Lithuania (Oct. 18, 2016) (available at <https://www.startuplithuania.com/news/tiny-lab-productions-subscription-model-sounds-promising/>) (accessed on Sept. 4, 2018).

visited his 2 years [sic] old nephew and wanted to download a simple racing game for a boy this young. Unfortunately he encountered a problem – there were plenty of racing games for teens and grown ups, with complicated controls, inappropriate ads and game content, and no easy and kid-friendly games for toddlers which wouldn't make them cry. The next day Jonas shared this idea with his colleagues and they decided to create a simple racing game for toddlers.¹⁴⁶

196. Abromaitis further lamented the difficulty of monetizing children, stating “there is a low buying power of our players who are mainly under 13 years old. It’s hard to convince them to spend their money on additional game items or levels as most of them have to ask their parents for the purchase.”¹⁴⁷

197. Fun Kid Racing, like the other Gaming Apps, is an app whose subject matter, design, and distribution mechanisms all suggest that the app is appropriate for children. The app is marketed for children of all ages in the Google Play Store. *See* Figure 1, *infra*.

198. In the Google Play Store, Tiny Lab’s Gaming Apps are rated as being appropriate for children.¹⁴⁸ In marketing the Gaming Apps as being suitable for children, Tiny Lab implicitly and explicitly purports to acknowledge and adhere to privacy-protective norms.

199. For example, Fun Kid Racing is featured in the “Family” section of the Google Play Store, which gives developers improved visibility to parents. As Google explains, being included in the Family section of the Google Play Store:

¹⁴⁶ *Fun Kid Racing – Accidentally Born Successful Game*, GameSauce (Oct. 6, 2016) (available at <http://www.gamesauce.biz/2016/10/06/fun-kid-racing-accidentally-born-successful-game/>) (accessed on Sept. 4, 2018).

¹⁴⁷ *Tiny Lab Productions: Subscription Model Sounds Promising*, Startup Lithuania (Oct. 18, 2016) (available at <https://www.startuplithuania.com/news/tiny-lab-productions-subscription-model-sounds-promising/>) (accessed on Sept. 4, 2018).

¹⁴⁸ As noted in Exhibit 1, each of the Gaming Apps is or has been a participant in Google’s Designed for Families program, and accordingly listed in the “Family” category of the Google Play app store, with five exceptions: Chhota Bheem Speed Racing; Christmas Snow Racing; Fun Kid Bubble Pop; Fun Kid Racing - Stickman Mode; and Windy Way.

[E]xpands the visibility of your family content on Google Play, helping parents easily find your family-friendly apps and games throughout the store. Other features create a trusted environment that empowers parents to make informed decisions and engage with your content.¹⁴⁹

200. As described above, it is critical that apps in the Family section are, in fact, “family-friendly” and contribute to a “trusted environment.” Thus, in order to be featured in the Family section of Google Play, Google requires that the app be a part of the “Designed for Families” program,¹⁵⁰ which comes with specific requirements.

201. In order for any of the Gaming Apps to have been included in the Family section of Google Play (and therefore for Tiny Lab to have enrolled in the Designed for Families program), Tiny Lab had to expressly warrant, *inter alia*, that the Gaming Apps met specific criteria related to privacy laws (set by Google):

Eligibility

All apps participating in the Designed for Families program must be relevant for children under the age of 13 and comply with the eligibility criteria below. App content must be appropriate for children. Google Play reserves the right to reject or remove any app determined to be inappropriate for the Designed for Families program.

...

2. If your Designed for Families app displays ads, you confirm that:

2.1 You comply with applicable legal obligations relating to advertising to children.

2.2 Ads displayed to child audiences do not involve interest-based advertising or remarketing.

2.3 Ads displayed to child audiences present content that is appropriate for children.

¹⁴⁹ *Designed for Families*, Google Play (available at <https://developer.android.com/google-play/guides/families/>) (accessed 4).

¹⁵⁰ *Id.* (“Only apps and games that are part of the Designed for Families program will show up in searches initiated from the Family section in Apps Home.”).

2.4 Ads displayed to child audiences follow the Designed for Families ad format requirements.

...

7. You represent that apps submitted to Designed for Families are compliant with COPPA (Children's Online Privacy Protection Rule) and other relevant statutes, including any APIs [(a synonym for SDKs)] that your app uses to provide the service.¹⁵¹

202. Thus, in marketing the DFF Gaming Apps and seeking the commercial advantage of the improved visibility to parents afforded by its family-oriented positioning in Google Play, Tiny Lab warrants that the DFF Gaming Apps are family-friendly, that the apps (and Tiny Lab, generally) act in accordance with all applicable privacy laws and regulations, and that any SDKs contained within the DFF Gaming Apps will comply with all applicable privacy laws and regulations.

203. Indeed, Tiny Lab specifically holds the DFF Gaming Apps out to its audience as being family-friendly, knowing that its audience reasonably expects such apps *not* to engage in privacy-violative behavior.

204. Tiny Lab has deceived the public as to the data exfiltration functionality of the DFF Gaming Apps. In so doing, it has created the false impression that the DFF Gaming Apps adhere to child privacy norms.

2. Similarly, Google Represents That Tiny Lab's DFF Gaming Apps Are Suitable for Children and Adhere to Privacy Laws and Norms, Despite Having Notice That This Is Not True.

205. As discussed *supra*, Google has been made aware of the depth and breadth of Tiny Lab's unlawful and privacy-invasive behavior. However, rather than taking any form of action, Google elected to do nothing and to continue to allow Tiny Lab to keep its DFF Gaming Apps in the Designed for Families program, and to market its apps—on Google's online

¹⁵¹ *Id.*

marketplace, Google Play—as being appropriate and safe for children, despite having affirmative knowledge that this is not the case.

3. Defendants Violate Their Own Privacy Commitments.

206. As alleged herein, Defendants fail to comply with their own privacy commitments. While SDK Defendants maintain privacy policies, these policies expressly disclaim their respective SDK’s suitability for child-directed apps, or make statements about complying with privacy laws and norms that have been proven false by forensic analysis. This applies to the SDK Defendants’ privacy policies in effect at all times relevant to this action. Similarly, at all times relevant to this action, and in all operative versions of its privacy policy, Tiny Lab has designed and implemented its privacy policy to confuse and obfuscate its actions, rather than to provide parents with meaningful notice.

V. CLAIMS FOR RELIEF

COUNT I

**Children’s Online Privacy Protection Act
15 U.S.C. §§ 6501, *et seq.*
(as to the SDK Defendants and Tiny Lab)**

207. The State repeats and realleges all preceding paragraphs contained herein.

208. The Attorney General of the State of New Mexico is authorized to bring a civil action in the name of the State against Defendants to enforce regulations prescribed by COPPA and to secure remedies for violations of such regulations. *See* 15 U.S.C. § 6504.

209. Defendants collected Personal Information from New Mexico children under the age of 13 through the Tiny Lab Gaming Apps, which Defendants operate and which are directed to children.

210. In numerous instances, in connection with the acts and practices described above, Defendants collected, used, and/or disclosed Personal Information from children (as defined under 16 C.F.R. § 312.2) in violation of COPPA, including, but not limited to, by:

a. Failing to provide sufficient notice of the information Defendants collect, or is collected on their behalf, online from children, how they use such information, their disclosure practices, and all other required content, in violation of Section 312.4(d) of COPPA, 16 C.F.R. § 312.4(d);

b. Failing to provide direct notice to parents of the information Defendants collect, or information that has been collected on Defendants' behalf, online from children, how they use such information, their disclosure practices, and all other required content, in violation of Section 312.4(b) and (c) of COPPA, 16 C.F.R. § 312.4(b)-(c);

c. Failing to obtain verifiable parental consent before any collection or use of Personal Information from children, in violation of Section 312.5 of COPPA, 16 C.F.R. § 312.5; and

d. Failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of Personal Information collected from children, in violation of Section 312.8 of COPPA, 16 C.F.R. § 312.8.

211. Each SDK Defendant knew that its SDK was embedded in one or more Tiny Lab Gaming App. On information and belief, and consistent with industry custom and each SDK Defendant's general practices, each SDK Defendant specifically contracted with Tiny Lab to embed its SDK in the Gaming Apps.

212. Each SDK Defendant knew that the Gaming Apps were directed to children, as is obvious and indisputable from a cursory review of the Gaming Apps, their marketing, and Tiny Lab's specific representations about the Gaming Apps, including but not limited to the Gaming Apps' target audience being comprised of kids and toddlers.

213. Each SDK Defendant knew that it was receiving Personal Data (including Personal Information as that term is defined under COPPA) from the devices of children playing a Gaming App.

214. Each SDK Defendant, on information and belief and consistent with industry custom and each SDK's general practices, communicated with Tiny Lab concerning the monetization of the Personal Data (including Personal Information as that term is defined under COPPA) it was receiving via the Gaming Apps.

215. Each collection, use, or disclosure of a New Mexico child's Personal Data in which Defendants violated COPPA in one or more ways described above constitutes a separate violation for which the State seeks: (a) an injunction enjoining the practice and requiring compliance with COPPA, (b) damages, restitution, or other compensation on behalf of residents of the State, and (c) such other relief as the Court may consider to be appropriate.

216. Prior to filing this action, the State provided to the FTC written notice of this action and a copy of this Complaint, consistent with the requirements of 15 U.S.C. § 6504.

COUNT II

Violations of the New Mexico Unfair Practices Act N.M. Stat. Ann. §§ 57-12-1, *et seq.* (as to the SDK Defendants and Tiny Lab)

217. The State repeats and realleges all preceding paragraphs contained herein.

218. Pursuant to Section 1303(c) of COPPA, 15 U.S.C. § 6502(c), a violation of COPPA constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of the FTC Act.

219. Section 57-12-4 of the New Mexico Unfair Practices Act (UPA) provides that “[i]t is the intent of the legislature that in construing Section 3 [N.M. Stat. Ann. § 57-12-3] of the Unfair Practices Act the courts to the extent possible will be guided by the interpretations given by the federal trade commission and the federal courts.”

220. As such, Defendants have engaged in unfair or deceptive acts or practices in violation of N.M. Stat. Ann. § 57-12-1 *et seq.*

221. Additionally, Defendants have made material misrepresentations and omissions, both directly and indirectly, related to the privacy-invasive and unlawful behaviors and practices detailed herein.

222. Defendants have made material misrepresentations and omissions directly through, *inter alia*, public-facing documents such as websites, privacy policies, marketing materials, app interfaces, and public statements, in which Defendants omit or otherwise conceal the full extent of the privacy- and COPPA-violative conduct detailed herein.

223. Similarly, Defendants have made material misrepresentations and omissions indirectly through, *inter alia*, representations and warranties as to, *inter alia*, the COPPA-compliant and privacy-protective nature of the Gaming Apps (and their underlying technologies), the lawful nature and use of the SDK Defendants' SDKs (and related technologies), and the suitability of the Gaming Apps for children, generally.

224. As such, Defendants have engaged in additional unfair or deceptive acts or practices in violation of N.M. Stat. Ann. § 57-12-1 *et seq.*

225. Defendants' unfair and/or deceptive acts or practices alleged herein may have, tend to, or actually have deceived or misled New Mexico consumers. Further, Defendants have taken advantage of the lack of knowledge, ability, experience, or capacity of New Mexico consumers to the detriment of those consumers.

226. Each wrongful act or practice committed by or engaged in by Defendants in violation of the statute is an unfair, deceptive, and unconscionable act or practice in the conduct of trade or commerce, which is unlawful under the UPA.

227. Defendants' violations were, and are, willful, deceptive, unfair, and unconscionable. Defendants are aware of the violations, yet have failed to adequately and affirmatively take steps to cure the misconduct.

228. Defendants' willful violations justify assessing civil penalties of up to \$5,000 for each violation of the UPA.

229. The State has determined that Defendants are using, and have used, methods, acts, and practices prohibited by the UPA, such that the imposition of an injunction against Defendants prohibiting the conduct set forth herein is in the public interest. Therefore, to prevent Defendants from continuing to engage in the violations as set forth herein, the State hereby seeks temporary and permanent injunctions prohibiting Defendants from engaging in the unfair, deceptive, and unconscionable policies, practices, and conduct described in this Complaint.

230. Defendant is liable to the State for restitution, in an amount to be determined at trial, arising out of Defendants' deceptive and/or unfair methods, acts, and practices.

COUNT III

Violations of the New Mexico Unfair Practices Act N.M. Stat. Ann. §§ 57-12-1, *et seq.* (as to Defendant Google)

231. The State repeats and realleges all preceding paragraphs contained herein.

232. Defendant Google has represented that 86 of Tiny Lab's Gaming Apps are compliant with its Designed for Families ("DFF") program and, by extension, that these Gaming Apps are suitable and safe for children, complying with all applicable privacy laws, including COPPA.

233. Defendant has and has had actual knowledge of the acts and practices described herein, which make plain the fact that the Gaming Apps are *not* compliant with the guidelines set forth in DFF.

234. Despite this fact, Defendant continues to market Gaming Apps as DFF compliant and, more broadly, as being suitable and safe for children.

235. As such, Defendant has engaged in unfair or deceptive acts or practices in violation of N.M. Stat. Ann. § 57-12-1 *et seq.*

236. Defendant's unfair and/or deceptive acts or practices alleged herein may have, tend to, or actually have deceived or misled New Mexico consumers. Further, Defendant has taken advantage of the lack of knowledge, ability, experience, or capacity of New Mexico consumers to the detriment of those consumers.

237. Each wrongful act committed by Defendant in violation of the statute is an unfair, deceptive, and unconscionable act or practice in the conduct of the trade or commerce, which is unlawful under the UPA.

238. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable. Defendant is aware of the violations, yet has failed to adequately and affirmatively take steps to cure the misconduct.

239. Defendant's willful violations justify assessing civil penalties of up to \$5,000 for each violation of the Act.

240. The State has determined that Defendant is using, and has used, methods, acts, and practices prohibited by the UPA, such that the imposition of an injunction against Defendant prohibiting the conduct set forth herein is in the public interest. Therefore, to prevent Defendant from continuing to engage in the violations as set forth herein, the State hereby seeks temporary and permanent injunctions prohibiting Defendant from engaging in the unfair, deceptive, and unconscionable policies, practices, and conduct described in this Complaint.

241. Defendant is liable to the State for restitution, in an amount to be determined at trial, arising out of Defendant's deceptive and/or unfair methods, acts, and practices.

COUNT IV

Intrusion Upon Seclusion (as to the SDK Defendants and Tiny Lab)

242. The State repeats and realleges all preceding paragraphs contained herein.

243. New Mexico brings this claim in its *parens patriae* capacity pursuant to New Mexico's quasi-sovereign interest in the health and well-being of its residents. New Mexico possesses an interest in this matter apart from the interests of private parties. New Mexico acts herein as a representative of its citizens to redress injuries that affect the general population of New Mexico in a substantial way.

244. Citizens of the State of New Mexico have reasonable expectations of privacy in their mobile devices and their online behavior, generally. New Mexico citizens' private affairs include their behavior on their mobile devices as well as any other behavior that may be monitored by the surreptitious tracking employed or otherwise enabled by the Gaming Apps.

245. The reasonableness of such expectations of privacy is supported by Defendants' unique position to monitor New Mexico citizens' behavior through their access to these individuals' private mobile devices. It is further supported by the surreptitious, highly-technical, and non-intuitive nature of Defendants' tracking.

246. Defendants intentionally intruded on and into New Mexico citizens' solitude, seclusion, or private affairs by intentionally designing the Gaming Apps and the embedded SDKs to surreptitiously obtain, improperly gain knowledge of, review, and/or retain New Mexico citizens' activities through the monitoring technologies and activities described herein.

247. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, the legislation enacted by Congress including COPPA itself, rules promulgated and enforcement actions undertaken by the FTC, and countless studies, op-eds, and articles decrying the online tracking of children. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing New Mexico citizens' Personal

Information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Defendants' conduct is the fact that Defendants' principal goal was to surreptitiously monitor New Mexico citizens—in one of the most private spaces available to an individual in modern life—and to allow third-parties to do the same.

248. New Mexico citizens were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

249. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by New Mexico citizens.

250. As a result of Defendants' actions, the State seeks injunctive relief in the form of Defendants' cessation of tracking practices in violation of COPPA and destruction of all personal data obtained in violation of COPPA.

251. As a result of Defendants' actions, the State seeks nominal and punitive damages in an amount to be determined at trial. The State seeks punitive damages because Defendants' actions—which were malicious, oppressive, and willful—were calculated to injure New Mexico citizens and made in conscious disregard of New Mexico citizens' rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

VI. PRAYER FOR RELIEF

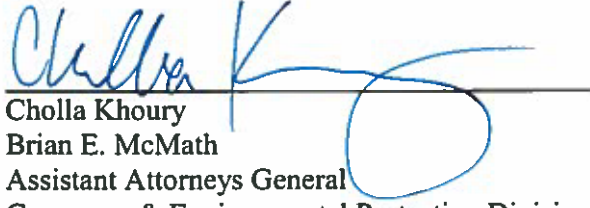
WHEREFORE, the State respectfully requests that this Court:

- a. Enter a permanent injunction to prevent future violations of COPPA, the FTC Act, and the UPA.
- b. Award the State monetary civil penalties from Defendants;
- c. Award the cost of investigation and reasonable attorneys' fees; and
- d. Award other and additional relief the Court may determine to be just and proper.

September 11, 2018

Respectfully submitted,

**ATTORNEY GENERAL OF NEW MEXICO
HECTOR H. BALDERAS**



Cholla Khoury
Brian E. McMath
Assistant Attorneys General
Consumer & Environmental Protection Division
New Mexico Office of the Attorney General
P.O. Drawer 1508
Santa Fe, NM 87504-1508
Phone: (505) 717-3531
Fax: (505) 318-1050
ckhoury@nmag.gov
bmcmath@nmag.gov
Attorneys for Plaintiff