Patrick Carey, (Bar No. 30862)
Mark Todzo, (Bar No. 168389)
LEXINGTON LAW GROUP
503 Divisadero Street
San Francisco, California 94105
Telephone: (415) 913-7800
pcarey@lexlawgroup.com
mtodzo@lexlawgroup.com

David S. Golub, (*pro hac vice* forthcoming)
Steven L. Bloch (*pro hac vice* forthcoming)
Ian W. Sloss (*pro hac vice* forthcoming)
Jennifer Sclar (*pro hac vice* forthcoming)
Johnathan Seredynski (*pro hac vice* forthcoming)
SILVER GOLUB & TEITELL LLP
One Landmark Square, 15th Floor
Stamford, Connecticut 06901
Telephone: (203) 325-4491
isloss@sgtlaw.com
sbloch@sgtlaw.com
jsclar@sgtlaw.com
jseredynski@sgtlaw.com

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

A.B., a minor, by and through his guardian JEN TURNER, C.D.1, C.D.2, and C.D.3 minors, by and through their guardian KIRENDA JOHNSON, E.F.1, and E.F.2, by and through their guardian BARABRA HAYDEN-SEAMAN, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

GOOGLE LLC, ADMOB GOOGLE INC., and ADMOB, INC.,

Defendants.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs A.B., by and through his guardian Jen Turner, C.D.1, C.D.2, and C.D.3, by and through their guardian Kirenda Johnson, and E.F.1, and E.F.2., by and through their guardian Barbara Hayden-Seaman (collectively, "Plaintiffs"), hereby allege the following against Google LLC ("Google"), AdMob Google Inc., and AdMob, Inc. (the AdMob entities are referred to jointly as "AdMob", and collectively with Google, "Defendants") on behalf of themselves and all others similarly situated. Plaintiffs' complaint is based on personal knowledge, information and belief, the investigation of counsel, and public sources.

NATURE OF ACTION

1. This action arises out of the Defendants' unlawful invasion of privacy and violation of the reasonable expectations of privacy of millions of children under the age of 13. Through apps directed at children, Defendants knowingly and intentionally collected personal information without parental consent to track and profile the children using these apps and target them with highly lucrative behavioral advertising at the expense of the children's privacy rights and in violation of well-established privacy protections, societal norms, and the laws embodying those protections.

2. Defendant Google designed, developed, maintains, and markets Android, a "mobile operating system" used on a reported 2.5 billion tablets, phones, and other mobile devices ("Android Device(s)") worldwide, including over 130 million in the United States.

3. Google also designed, developed, maintains, and markets a digital software marketplace and distribution hub application on Android called the Google Play Store, which enables Android Device users to download software, or applications ("Apps or Android Apps") that run on Google's Android operating system.

4. Defendants AdMob Google Inc. and AdMob, Inc. are mobile advertising companies owned by Google which enable Android App developers to show advertisements to users of their Apps.

To accomplish this, AdMob designed, developed, maintains, and markets (including through Google), the AdMob software development kit, or "SDK".

5. The AdMob SDK provides Android App developers with code to include in their Android Apps which (1) enables Google and AdMob to collect data, including persistent identifiers, from the Android App users; and (2) shows advertisements to Android App users while they are using those Apps based on the persistent identifiers collected. AdMob pays developers for the ability to track their users and show advertisements to users within their Apps.

6. All of this activity serves one purpose: to collect as much data as possible about an individual so that AdMob and Google can make money showing that individual (and other children like him or her) highly-targeted advertisements.

7. Advertisers pay AdMob to advertise on the AdMob network because of its vast reach and the precision with which AdMob can target specific demographics. These features are a direct result of AdMob's extensive tracking of every user of an Android App in which the AdMob SDK is embedded.

8. To build as vast and lucrative an advertising network as possible, AdMob pays Android App developers to incorporate the AdMob SDK into their Android Apps and show ads to users of their Apps via the AdMob network.

9. The revenue App developers earn from AdMob enables App developers to offer their Apps for free to users. App developers are readily willing to forego charging users to download their Apps in exchange for the substantially greater advertising revenue App developers earn through AdMob.

10. Defendants and Android App developers are incentivized to maximize the number of users using Android Apps and to know as much about those users as possible, which enables each to maximize the revenue earned through targeted, behavioral advertising.

11. Google designed, developed, and in or about April 2015 began marketing the "Designed for Families" program ("DFF") on the Google Play Store. Google developed DFF to give parents

confidence that Apps their children were using were safe and age-appropriate through a vigorous vetting process.

12. To be included in DFF, each Android App had to submit an application and certify compliance with the DFF program requirements. Google then "review[ed] the submission to make sure that it me[t] the [Designed for Families] program's guidelines," and adhered to Google's content policy and terms of App developer agreements. If Google determined that the submitted Apps met the "stringent legal and policy bar" that Google's "specialized operations review" required, Google labeled the App as family friendly and included the App in DFF.[1]

13. In particular, Google represented it required that Apps included in the DFF program which displayed ads "compl[ied] with applicable legal obligations relating to advertising to children" and that "[a]ds displayed to child audiences d[id] not involve interest-based advertising."[2]

14. Google imposed these requirements because the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501, *et seq.,* protects children under 13 years of age from having their personal information ("Personal Information") collected, unless their parent has first given verifiable consent. Since 2013, persistent identifiers have been included within the definition of Personal Information that operators of child-directed websites and online services are barred by COPPA from collecting from children under 13 without parental consent. And Google expressly required the Android Apps in the DFF program to be "compliant with COPPA."[3]

15. In addition, thirty-four (34) states, including California, have firmly rooted protections against unwarranted invasions of privacy by recognizing the common law right to be free from intrusion

[1] https://techcrunch.com/2015/04/14/google-plays-new-program-designed-for-families-will-highlight-pre-approved-kid-safe-apps/
[2] Families and COPPA, Designed for Families, https://perma.cc/ML9K-TETX (archived Dec. 13, 2018).
[3] Families and COPPA, Designed for Families, https://perma.cc/ML9K-TETX (archived Dec. 13, 2018).

upon seclusion, as formulated by § 652B of the Restatement (Second) of Torts, which prohibits intentional intrusion upon the solitude or seclusion of another or his or her private affairs or concerns.

16. Based on COPPA and the societal norms embodied therein, bedrock, long-standing privacy protections, Google's guidelines and requirements concerning the DFF program and the standards for the Android Apps included in the DFF program, as well as the inherent characteristics of the Android App games themselves, parents and their children had a reasonable expectation of privacy in the children's online behavior and activities and the mobile devices utilized by the children and that the games that appeared in the DFF section of the Google Play Store that were directed primarily to children complied with applicable legal obligations as confirmed by Google.

17. DFF benefited Defendants and App developers alike. The DFF program provided young children using Google's Android Devices with easy access to games they would be interested in, which in turn grew Android App developers' user base. DFF also provided Defendants with easy access to a demographic coveted by advertisers: young children.

18. Millions of Apps were submitted to Google for inclusion in the DFF program by developers, reviewed by Google, and approved for DFF program inclusion. Many of these Apps, including Fun Kid Racing, GummyBear and Friends Speed Racing, and Monster Truck Racing explicitly noted in their applications to DFF and elsewhere (including on Apps and/or their websites) that the Apps were intended for and directed towards children under the age of 13. Plaintiffs played many Apps Google included in its DFF program, including Fun Kid Racing, Monster Truck Racing, and GummyBear and Friends Speed Racing.

19. Unbeknownst to Plaintiffs and their parents but known to Defendants, while Google implemented strict guidelines and standards for the DFF program, and publicly represented that DFF Apps complied with COPPA and other applicable laws regarding data collection and interest-based advertising, Defendants were surreptitiously exfiltrating the personal information of the children under

the age of 13 playing those Android App games (the very children the games were designed for) in violation of COPPA and privacy protections of children.

20. Google knew it was exfiltrating personal information of children under 13 because Google reviewed each and every App included in the DFF program, owned and operated the advertising platform that served behavioral advertising to children under 13 as they played the DFF apps (and still does), and was, in fact, informed by independent researchers that these Apps were operating in violation of COPPA.

21. Further, as described below, forensic testing performed by the New Mexico Attorney General's Office – following that independent research – revealed that the AdMob SDK collects highly-sensitive personal data, including a child's precise location within +/- 5 meters and was constantly updating that data to maintain accuracy.

22. Notwithstanding their knowing and intentional conduct aimed at these minor children, Defendants did not disclose that it was collecting the personal information of children under 13 and did not obtain parental consent for the collection of the personal information or the tracking, profiling, and targeting of children under 13 using that information for behavioral advertising (or any other purposes).

23. As described in greater detail below, Defendants' actions violated laws governing and the privacy rights and reasonable expectations of privacy of Plaintiffs and other similarly-situated young children under 13—and their parents and guardians—and constituted unlawful, unfair, and deceptive trade practices.

24. Accordingly, Plaintiffs bring this action on behalf of themselves and the classes (as defined below) of similarly-situated minors under the age of 13 whose privacy rights have been violated by Defendants, for disgorgement of Defendants' ill-gotten gains, compensatory, actual, and statutory damages, restitution, punitive damages, and injunctive relief and/or equitable relief to require Defendants permanently delete, destroy or otherwise sequester the Personal Information unlawfully

collected without parental consent and to provide a complete audit and accounting of the uses of the Personal Information by Defendants, App developers and any other third parties.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative members defined below, and minimal diversity exists because the majority of putative class members are citizens of a state different from Defendants.

26. This Court has specific personal jurisdiction over Defendants Google LLC, AdMob Google Inc., and AdMob, Inc. because they purposefully direct their conduct toward California, transact business in this District and in California, engage in conduct that has had and continues to have a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the United States, including those in this District and in California, and purposely availed themselves of the laws of California. Additionally, this Court has general personal jurisdiction over Google and the AdMob entities because they are headquartered in and have their principal places of business in California.

27. This Court also has jurisdiction pursuant to 28 U.S.C. §1332(d), because the amount in controversy exceeds $75,000 and is between citizens of different states.

28. Venue is proper in this District pursuant to 28 U.S.C. §1391(b) because a substantial portion of the conduct described in this Complaint was carried out in this District. Furthermore, Defendants are headquartered in this District.

INTRADISTRICT ASSIGNMENT

29. Assignment to the San Jose Division is proper under Northern District of California Civil Local Rule 3-2 (c) because a substantial part of the events or omissions which give rise to the claims asserted herein occurred in Santa Clara County and Defendants principal places of business are located

in Santa Clara County, California. Under Civil Local Rule 3-2 (e), all civil actions which arise in the County of Santa Clara shall be assigned to the San Jose Division.

PARTIES

30. Plaintiff A.B. is a natural person and is a U.S. citizen, domiciled in the State of California. A.B. was under the age of 13 during the relevant time period. A.B.'s parent and legal guardian is Jen Turner, who is also a U.S. citizen, domiciled in the State of California.

31. Plaintiff C.D.1 is a natural person and is a U.S. citizen, domiciled in the State of Florida. C.D.1 is under the age of 13. C.D.1's parent and legal guardian is Kirenda Johnson, who is also a resident and citizen of the State of Florida.

32. Plaintiff C.D.2 is a natural person and is a resident and citizen of the State of Florida. C.D.2 is under the age of 13. C.D.2's parent and legal guardian is Kirenda Johnson, who is also a U.S. citizen, domiciled in the State of Florida

33. Plaintiff C.D.3 is a natural person and is U.S. citizen, domiciled in the State of Florida. C.D.3 is under the age of 13. C.D.3's parent and legal guardian is Kirenda Johnson, who is also a U.S. citizen, domiciled in the State of Florida.

34. Plaintiff E.F.1 is a natural person and is U.S. citizen, domiciled in the State of New York. E.F.1 is under the age of 13. E.F.1's parent and legal guardian is Barbara Hayden-Seaman, who is also a U.S. citizen, domiciled in the State of New York.

35. Plaintiff E.F.2 is a natural person and is a U.S. citizen, domiciled in the State of New York. E.F.2 is under the age of 13. E.F.2's parent and legal guardian is Barbara Hayden-Seaman, who is also a U.S. citizen, domiciled in the State of New York.

36. Defendant Google, LLC is a business incorporated under the laws of the state of Delaware with its principal place of business in Mountain View, California. Google is a wholly-owned subsidiary of Alphabet, Inc.

37. Defendants AdMob Google Inc. and AdMob, Inc. are wholly-owned subsidiaries of Google, incorporated under the laws of the state of Delaware. The AdMob entities run a mobile advertising business and maintain its principal place of business in Mountain View, California.

BACKGROUND

I. GOOGLE'S DATA COLLECTION AND ADVERTISING ACTIVITES

A. GOOGLE

38. Google is a multinational corporation known primarily for the design, development, and operation of the world's most visited internet webpage: www.google.com ("Google.com"). Google.com hosts a search engine that catalogues websites and organizes information on the internet to allow Google users to search the contents of the internet as catalogued by Google.

39. Beyond Google.com, Google has developed or acquired, and currently operates, a vast collection of software, services, and technology devices. Specifically, Google operates hundreds of software applications and online cloud services which are offered to the public at no charge, such as Google's email service Gmail, Google's cloud storage service Google Drive, Google's web browser Chrome, video sharing platform YouTube, and Google's Android mobile device operating system and related mobile applications.[4]

40. In addition to Google's software applications, operating systems, and cloud services, Google manufactures mobile phones, earbuds, watches, laptops, speakers, cameras, thermostats, Wi-Fi routers, as well as accessories for those devices.

41. Each of Google's software applications, web services, and devices, including the Android operating system and the Google Play Store, is designed with one thing in mind: collecting as much

[4] As of the date of filing, Google listed over 100 "products" on its webpage: https://about.google/intl/en_us/products/#all-products

personal, sensitive data about individuals' behavior and interests, on the internet and beyond, as possible.

42. Google wants to obtain this data to support Google's advertising business. Advertising is *by far* Google's primary source of revenue. For example, in 2021, $209 billion out of Google's $256 billion in revenue came from advertising.[5]

43. Google grew its advertising business by leveraging the popularity of Google.com's search engine and acquiring the website advertising company DoubleClick. These actions led to Google's creation of an internet website-based surveillance network capable of tracking user's activity across websites which makeup over 80% of the "traditional internet" (*i.e.,* websites visited via web browser on desktop and laptop computers).[6]

44. Google's surveillance network operates as follows: a website that uses Google's advertising services (DoubleClick) embeds code into its website which (1) allows Google to collect the personally identifying information (PII) of each visitor to that website, including the visitors' IP address and/or IMEI number, and other device and location data specific to that user; and (2) shows that user advertisements based on the information Google had learned about that user based on, among other things, the PII it collected from that user when he or she visited the webpage(s).

45. Then, when that user visits *another* website that has opted to use Google's advertising services, the other website that uses Google's advertising services sends Google the same IP address or IMEI number or information that matched a particular visitor, and Google knows that individual has visited both websites.

---

[5] https://www.statista.com/statistics/266249/advertising-revenue-of-google/; https://www.statista.com/statistics/266206/googles-annual-global-revenue/.

[6] Steven Englehardt & Arvin Narayanan, *Online Tracking: A 1-million-site Measurement and Analysis*, Princeton University WebTAP Project, http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf (accessed Oct. 21, 2019) (emphasis added).

46. Google uses this information to build detailed individual profiles which include identifiers that correlate with individual users. Most individuals have no idea that Google is tracking their activity across 80% (or more) of the internet.

47. The data Google gathers is stitched into a single profile of a user which gives Google the most accurate, up-to-date, snapshot of a user's attributes and behaviors. Google uses this data to deliver targeted advertisements to users as they visit websites on the internet or use other internet-connected services. User profiles such as those developed by Google have been called the "holy grail" of advertising[7] and allow Google to charge advertisers increased advertising rates.

B. GOOGLE'S ANDROID ECOSYSTEM: ANDROID, GOOGLE PLAY STORE, AND ADMOB

1. ANDROID

48. Google's tracking on the traditional internet pales in comparison, however, to Google's tracking activities on Android mobile devices.

49. Individuals' internet use began to change with the introduction of the internet-connected mobile smartphones. For example, Apple's introduction of the iPhone, together with Apple's iOS operating system and iOS Apps, gave individuals the option to communicate and seek information via smartphone apps, rather than through traditional websites accessed via desktop browser. This threatened to divert internet users from "Google's internet," accessed via desktop web browser, to Apple's (or any other smartphone operating system developer's) internet, accessed via iOS and iOS apps, which threatened Google's access to data and an advertising audience.

50. Google responded by developing Android, its own mobile operating system with countless (and often hidden) ways to track Android Device users' activities and exfiltrate their data.

[7] Randell Cotta, Sr., *Overcoming the Last Hurdle in the Quest for the "Holy Grail" of Marketing*, KD NUGGETS, https://www.kdnuggets.com/2017/02/quest-holy-grail-marketing.html (accessed Oct. 21, 2019).

51. Google then offered Android for free to mobile device manufacturers such as Samsung and LG, saving them the time and expense of having to find or develop their own mobile operating system, in exchange for giving Google access to the information of the purchasers/users of Samsung or LG mobile devices.

52. Google could do this because it knew, from Google's established website advertising model, that it could make far more money exfiltrating users' data for advertising purposes than it ever could charging manufacturers' a licensing fee to use Android on their devices.

53. Android is now the most widely used mobile operating system in the world. As of May 18, 2021, there were 3 billion active Android devices (meaning devices that had been used in the previous month), compared with, for example, Apple's 2 billion active iOS users.

54. Thus, billions of people globally access the internet via Google's proprietary, internet-connected Android ecosystem, including over 130 million users in the U.S.[8]

55. In order to generate more data and learn more about Android users, Google devised numerous ways to cause Android users to further engage with their Android devices so that Google could track that activity and use that data for advertising purposes. The primary way Google accomplished this was through the development of the application now named Google Play Store.

2. GOOGLE PLAY STORE

56. Google Play Store ("Google Play") is a digital distribution service developed and operated by Google, launched in 2008 as Android Marketplace and later rebranded to Google Play Store.

57. Google Play functions as a mobile application that runs on Google's Android mobile operating system and comes preinstalled on every mobile Android device.

[8] https://earthweb.com/how-many-people-use-android/

58. Google Play's purported purpose is to provide Android device users with additional Android software applications, adding functionality to, or new ways to use, Android devices. The types of Apps available on Google Play include, but are not limited to, Apps which enable users to learn the weather, enjoy music, read books, and play games, among other things.

59. As of December 29, 2022, there were 3.8 million apps available in the Google Play Store.[9] In 2021, over 111 billion App downloads occurred via the Google Play Store.[10]

60. Of the 3.8 million apps available in the app store, only 116,750 require purchase, while over *3.6 million are offered for free*.[11]

61. As with Android, Google's primary motivation for developing Google Play was to gain access to more user data in order to build more detailed profiles about internet users and serve them lucrative advertising.

62. As with Android, Google's efforts were successful. Google successfully encouraged software developers to create Android Apps, which Apps primarily were offered for free. Google compensated developers of the Apps by paying them to allow advertising on their Apps, which Google served using data that Google collected.

63. In 2021 alone, the use of content creators for Google's ad network generated $32 billion dollars of revenue for Google.[12] Overall, mobile advertisers reportedly spent $288 billion in 2021, including $117 billion in the U.S.[13]

---

[9] https://42matters.com/google-play-statistics-and-trends.

[10] https://www.statista.com/statistics/734332/google-play-app-installs-per-year/.

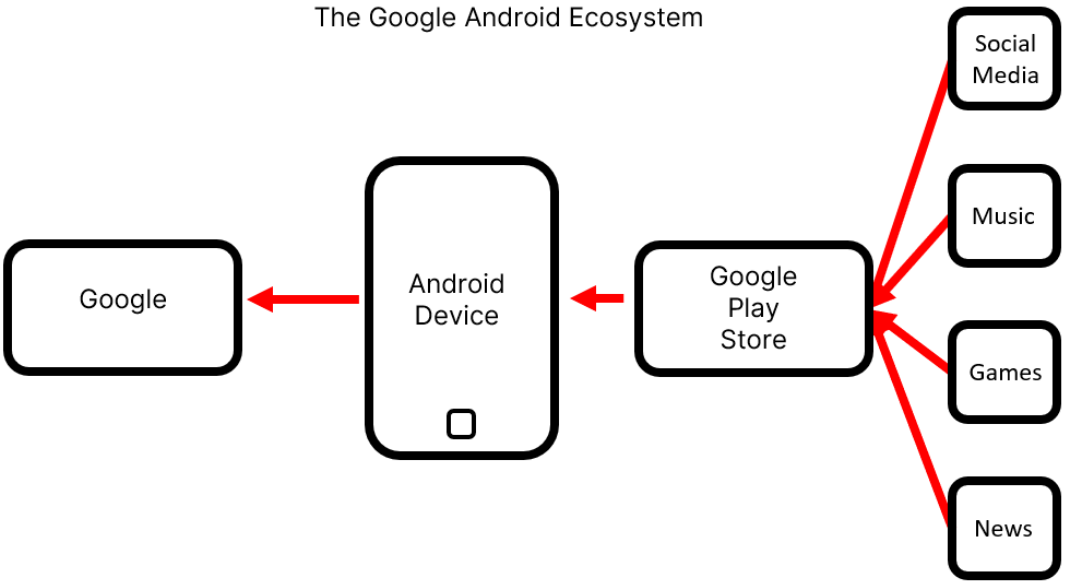
[11] https://42matters.com/google-play-statistics-and-trends.

[12] https://www.oberlo.com/statistics/how-does-google-make-money#:~:text=Google's%20second%2Dbiggest%20income%20source,Google's%20third%2Dlargest%20income%20source.

[13] https://www.businessofapps.com/ads/research/mobile-app-advertising-cpm-rates/#:~:text=According%20to%20Statista%2C%20globally%20mobile%20advertising%20spend%20rose,by%20%24227%20in%202020%20to%20%24288%20in%202021

64. Google's development of Android and Google Play gave Google complete control over a mobile internet with the following structure:

FIGURE 1



65. And Google uses its control of the Android digital ecosystem to exfiltrate and track unique and persistent identifiers to track individuals' activity and behavior interacting with Android and any Android App.

3. ADMOB

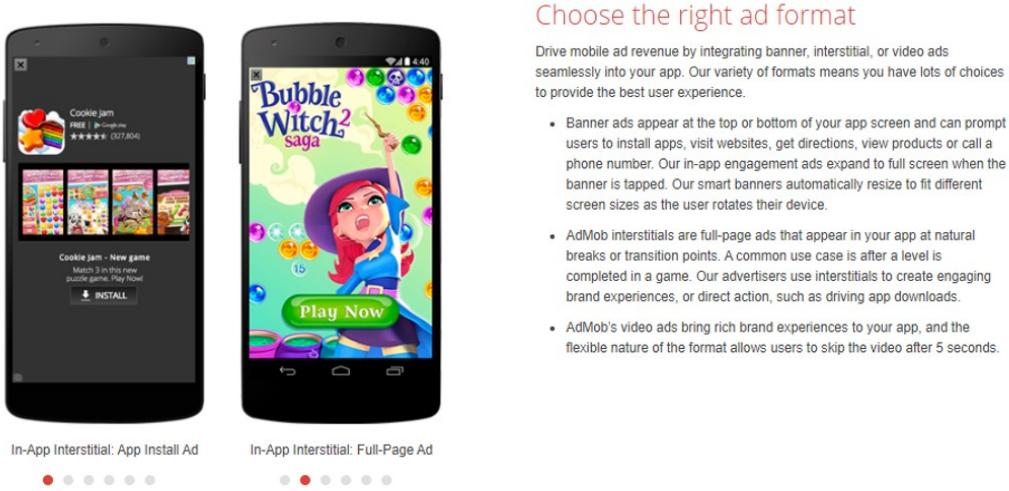
66. Google uses the data—including unique and persistent identifiers—it collects to determine which advertisements users are most likely to respond to. Google then charges advertisers for the ability to show advertisements to users based on insights Google has gained from the data collected from Android users.

67. Google shows advertisements to Android App users via AdMob, which Google acquired in 2009 for $750 million.

68. Google described AdMob and the purpose behind Google's AdMob acquisition as follows (Google Play Store was previously known as Android Marketplace):

> In addition to search, another key way that people access information is through mobile websites (accessed through a browser) and mobile apps (available through Apple's App Store, the **Android Marketplace** and more).
>
> Mobile display and text ads make it easy for publishers and developers to make money from their mobile websites and apps, and enable advertisers to extend the reach of their campaigns to relevant mobile content. In this area, AdMob has been a real pioneer and has innovated at a tremendous pace, building a successful business and working with thousands of advertisers, publishers and developers.
>
> **AdMob was one of the first companies to serve ads inside mobile applications on the Android and iPhone platforms.** They've developed a host of engaging and creative ad units for Android and iPhone apps—for example, interactive video ad units and expandable rich media ads. Google has also been developing new features for in-app ads. For example, last week, we announced that we'll be making "click-to-call" ad formats available to developers who run AdSense in their mobile apps. With Google and AdMob starting to work together, there's lots more innovation to come in this area.
> …
>
> It's clear that mobile advertising is growing incredibly fast with lots of businesses innovating at great speed. Every day, more marketers are looking to take advantage of the mobile-specific capabilities, extended reach, great returns and value that mobile advertising provides. Advertisers are now starting to see mobile as an essential part of their overall campaigns, not just a silo-ed experiment on the side.

69. Google immediately brought AdMob under Google's umbrella, hosting AdMob on Google's own website at www.google.com/admob, and promoting its benefits, including the following, imagery of Apps directed towards young children, sending the message that AdMob could help developers of those Apps make money:



70. AdMob is the Android equivalent of Google's website advertising service DoubleClick and allows Android App developers to monetize their Apps by, for example, selling ad space within their Apps for small banners to appear when a user is playing an App, or having a pop-up appear between game levels.

71. When an App developer "monetizes" their App with AdMob, AdMob collects data on the App's users, including the following types of data:

a. **Device identifiers**: this includes device ID, Android ID, and other identifiers which allow AdMob to determine which particular device the App is being used on.

b. **Location Data**: this includes location data acquired via GPS, Wi-Fi, and cellular networks.

c. **App usage data**: this includes data relating to the duration or frequency of app usage.

d. **In-app behavior data**: this includes data on behavior such as in-app purchasing, or in game behavior.

e. **Cookies**: AdMob uses cookies to track user behavior across multiple apps and websites. So if a user interacts with one App using AdMob, AdMob will draw on that behavior to show that user ads even when it begins using a second App which has integrated AdMob.

72. AdMob promised App 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."

73. RTB is synonymous with targeted advertising and relies on user profiling and the sharing of PII between advertisers, ad networks, and ad publishers.

74. The following is an example of how monetizing an App through AdMob works:

a. **AdMob SDK App Integration**: An App developer that wishes to make money via advertising includes the AdMob SDK code in the App to allow the App to communicate with AdMob server's, sending AdMob information about the App users and receiving display ads back.

b. **Developer Select Display Ad Unit**: Once the SDK is integrated, the app developer can create "Display Ad Units" in the AdMob dashboard. These specific locations in the app where ads will be displayed, such as banners, interstitials, or rewarded video ads.

c. **App Ad Request**: When a user opens the app and an ad unit is triggered, the Android App sends an ad request to AdMob's servers.

d. **AdMob Ad Selection**: AdMob's servers then use personal information, including device identifiers and users' location, to select the most relevant ad to display. This process can take a few forms, one of which involves Real Time Bidding, or RTB, where advertisers instantaneously submits "bids" to place their ads in a given display ad unit based on the personal information exfiltrated about the user, and other information. The advertiser with the winning big pays AdMob to have their ad placed.

e. **AdMob Ad Delivery & Display**: Once AdMob selects an ad to display, it sends the ad to the App and displays it within the designated ad unit.

f. **Revenue**: AdMob shares the revenue they get from advertisers with App developers, and pays App developers money for each ad interaction, which can be, *inter alia*, clicking on a banner, or simply watching a video. The exact amount of money AdMob shares for each interaction depends on factors such as the ad type, source, and user information used.

75. The AdMob SDK embedded within an Android App sends a users' PII back to AdMob, where AdMob analyzes, stores, and uses the data to build increasingly-detailed profiles of users. It is also shared with and sold to myriad third-parties so that each can continue to build their own profiles.

76. During the relevant period, the AdMob SDK was incorporated into over one million apps, facilitating 200 billion ad requests per month, and resulted in over $3.5 billion dollars being paid to App developers, most of whom did not charge users for their Apps.[14]

77. Google makes tens of billions of dollars in ad revenue per year solely from its sale of ads in the Google network, for example through AdMob, including $23 billion in 2020 alone.[15]

II. THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998

78. Congress passed COPPA in 1998 in response to concerns that children's online activities were being tracked by operators of websites and online services. Specifically, COPPA is intended to "maintain the security of personally identifiable information of children collected online" and to "protect children's privacy by limiting the collection of personal information from children without parental consent."[16] COPPA provides, in pertinent part, that:

> It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed [by the Federal Trade Commission].
>
> 15 U.S.C. § 6502(a).

79. COPPA applies to any operator of a commercial website or online service directed to children under thirteen years of age 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. The FTC has interpreted COPPA's definition of "website or online service" to include "mobile apps that send or receive information online (like network-connected games, social networking apps, or apps that deliver

[14] https://admob.google.com/home/ (as it appeared on Sept. 4, 2018).
[15] https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html.
[16] 144 CONG. REC. S12787.

behaviorally-targeted ads)."[17] In addition, the FTC has interpreted COPPA's definition of "website or online service" directed to children to include individual channels on a general audience platform. Defendants' activities vis-à-vis Android-serving applications are thus included under COPPA's regulation.

80. Further, according to the FTC, "content creators and channel owners" are both "standalone 'operators' under COPPA, subject to strict liability for COPPA violations."[18] And the FTC considers third parties with actual knowledge that is collecting personal information from users of a child-directed site or service as operators under COPPA.

81. In order to determine whether a website or online service is "directed to children" the FTC will:

> [C]onsider [the website's or online service's] subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children.
>
> 16 CFR § 312.2.

82. Websites or online services that collect personal information from users of other child-directed websites or online services are deemed as "child-directed" if the website or online service "has actual knowledge that it is collecting personal information directly from users of another Web site or online service directed to children." 16 C.F.R. § 312.2.

---

[17] https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business.

[18] Statement of Joseph J. Simons & Christine S. Wilson, *Regarding FTC and People of the State of New York v. Google LLC and YouTube, LLC*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/system/files/documents/public_statements/1542922/simons_wilson_google_youtube_statement.pdf (accessed Oct. 21, 2019).

83. COPPA defines a "child" as an individual under the age of thirteen. 15 U.S.C. § 6501(a). In relevant part, the FTC regulations require an operator to disclose information collection practices and "obtain verifiable parental consent for [any] collection, use, or disclosure of personal information from children." Id. § 6502(b)(1)(A); see 16 C.F.R. § 312.5(a).

84. COPPA prohibits the collection of the following information ("Personal Information") from children under thirteen without parental consent:

a. full name;

b. home or physical address;

c. online contact information such as an email address or other identifier;

d. telephone number;

e. social security number;

f. persistent identifier that can be used to recognize a user over time and across different sites, including a cookie number, an IP address, a processor or device serial number, or a unique device identifier;

g. Photo, video, or audio file containing a child's image or voice; and

h. Geolocation information sufficient to identify a street name and city or town.

85. COPPA thus prohibits, *inter alia*, the collection of persistent identifiers for behavioral advertising absent notice and verifiable parental consent. 16 C.F.R. §§ 312.5(c)(7), 312.2.

86. Violations of COPPA and the accompanying FTC regulations "shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under" 15 U.S.C. § 57a.

87. In 2013, COPPA was enhanced (the "2013 COPPA Enhancement") to provide further protection for children against online tracking and to "giv[e] parents greater control over the online collection of their children's personal information." The 2013 enhancement widened the definition of

children's "Personal Information" to include "persistent identifiers" such as cookies that track a child's activity online, geolocation information, photos, videos, and audio recordings.

88. The 2013 COPPA Enhancement was the culmination of two years of rulemaking by the Federal Trade Commission ("FTC") and reflected society's growing recognition of the surreptitious surveillance tactics used by advertising companies to track children and advertise to them via mobile apps.

89. For example, the FTC published a 2012 report entitled *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (the "FTC Kids Mobile App Report") addressing privacy dangers for children using mobile apps. The report warned that companies like Google and AdMob (advertising platform operators) link persistent identifiers and geolocation data they collect with additional Personal Information such as name, address, and email address—allowing those entities and their partners to identify individual users whom they profile with indisputably individual specificity.

90. The FTC Kids Mobile App Report additionally cites a forensic analysis of app behavior, showing that:

> [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 other 29 apps by matching the unique, persistent device ID.[19]

[19] 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-notmaking-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).

91. By expressly including persistent identifiers and geolocation data in COPPA's definition of Personal Information, the FTC intended to deter advertising companies and advertising network operators from exploiting young children via mobile app tracking, profiling, and advertising.

III. GOOGLE'S DESIGNED FOR FAMILIES PROGRAM

92. Google tapped into the societal, governmental, and familial concerns articulated above that companies will take advantage of vulnerable children reflected in COPPA by creating a special program for Google Play – the Designed for Families (DFF) program – which certified that certain Apps were appropriate for families and children.

93. Google announced the DFF program with the following blog post:

> There are thousands of Android developers creating experiences for families and children — apps and games that broaden the mind and inspire creativity. These developers, like PBS Kids, Tynker and Crayola, carefully tailor their apps to provide high quality, age appropriate content; from optimizing user interface design for children to building interactive features that both educate and entertain.
>
> Google Play is committed to the success of this emerging developer community, so today we're introducing a new program called Designed for Families, which allows developers to designate their apps and games as family-friendly. Participating apps will be eligible for upcoming family-focused experiences on Google Play that will help parents discover great, age-appropriate content and make more informed choices.

94. Google stated that Apps which opted into the DFF program would be required to meet a "stringent legal and policy bar" and "will need to undergo a specialized operations review"[20] to ensure compliance with the DFF program's rules, including, *inter alia*, data collection and ad targeting, and the Apps were required to comply with COPPA and all other applicable children's privacy regulations.[21]

[20] https://techcrunch.com/2015/04/14/google-plays-new-program-designed-for-families-will-highlight-pre-approved-kid-safe-apps/

[21] https://techcrunch.com/2015/04/14/google-plays-new-program-designed-for-families-will-highlight-pre-approved-kid-safe-apps/

95. Google required App developers to expressly warrant, *inter alia*, that their Apps met the following criteria Google established:

> 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.
> 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.
> …
>
> Ad targeting and data collection
>
> Ads displayed to child audiences must comply with laws relating to advertising to kids. For example. Your app must disable interest-based advertising and remarketing, and should comply with child relevant regulations and industry standards for all countries where the app is distributed.

96. Google also required App developers to categorize their Apps as either "not primarily directed to children" (*i.e.*, mixed-audience) or "designed for children."

97. The intended audience a developer chose had important ramifications. If an App developer declared their App directed towards children, Google's bar on showing interest-based advertising to users of the App would apply. However, if an App developer designated their app as mixed-audience or "not primarily directed to children," the App was allowed to show interest-based or

"behavioral" advertising to all users on the theory that it was a mixed-audience service and thus not subject to COPPA.

98. Significantly, Google warned that noncompliance with these requirements could result in expulsion from either or both the DFF program and Google Play:

> Apps in the Designed for Families program that do not maintain compliance with the Designed for Families Program Requirements in addition to the Designed for Families Addendum may be rejected form the Designed for Families program or removed from the Google Play Store.

IV. GOOGLE'S PATTERN AND PRACTICE OF DATA MISCONDUCT AND PRIVACY VIOLATIONS

99. Google's surveillance practices have led to a litany of fines and settlements with private parties and governmental entities and regulators:

a. On October 24, 2011, Google entered into a settlement with the Federal Trade Commission for using deceptive tactics and violating its own privacy policy when it launched Buzz, its social networking feature; the settlement barred Google from future privacy misrepresentations, required it to implement a comprehensive privacy program, and subjected it to independent privacy audits for 20 years[22].

b. On August 9, 2012, Google paid $22.5 million to settle FTC charges that Google had not adequately disclosed Google's practices regarding its tracking cookies to users of Apple's Safari Internet browser, in violation of Google's 2011 settlement with the FTC.[23]

c. On November 18, 2013, Google entered into a $17 million settlement with attorneys general from 37 states and the District of Columbia to resolve allegations that the company had circumvented privacy settings pertaining to Safari, Apple Inc.'s Web browser.[24]

d. On January 21, 2019, Google was fined $57M by France's data protection authority, the CNIL, for failing to comply with GDPR transparency and consent rules, including

[22] https://www.ftc.gov/news-events/news/press-releases/2011/10/ftc-gives-final-approval-settlement-google-over-buzz-rollout.
[23] https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented-privacy-assurances-users-apples.
[24] https://www.reuters.com/article/google-settle/google-to-pay-17-million-to-settle-states-safari-probe-idINDEE9AH0G620131118.

by not informing users that the ad tracking they are asked to consent to is occurring across numerous devices and services.[25]

e. In September 2019, Google, and its subsidiary YouTube, paid $170 million to settle allegations by the FTC and the New York Attorney General. The settlement required Google and YouTube to pay $136 million to the FTC and $34 million to New York for allegedly violating COPPA.[26]

f. On March 11, 2020, Sweden's Data Protection Authority (DPA) fined Google $8 million for "failure to comply" with Europe's General Data Protection Regulation ("GDPR") as a result of Google's failure to adequately remove search result links under right-to-be-forgotten requests after the DPA had instructed Google to honor these requested in 2017.[27]

g. On May 18, 2022, the Spanish Agency for Data Protection (AEPD) fined Google €10 million, its highest fine to date, for the violation of Articles 6 and 17 of GDPR, following two complaints and subsequent investigation from the AEPD. The AEDP noted that the complaints concerned the transfer of requests related to the removal of content from Google's various products and platforms, including the Google search engine and YouTube, to a third party, the 'Lumen Project.' Specifically, the AEPD explained that to enable the removal of content, Google required users that used the relevant forms to accept the transfer of copies of content removal requests to 'lumendatabase.org,' on which they would, subsequently be published.[28]

h. On August 12, 2022, the Federal Court of Australia ordered Google to pay $60 million in fines for misleading Australian Android users as to how and when it would collect and use their personal data[29].

i. On September 14, 2022, South Korea's Personal Information and Protection Commission fined Google $50 million for not clearly informing users or obtaining their consent as they collected information about their online activities when they used other websites or services outside their own platforms. This data was used to analyze their interests and create individually customized advertisements.[30]

---

[25] https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/.
[26] https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law.
[27] https://edpb.europa.eu/news/national-news/2020/swedish-data-protection-authority-imposes-administrative-fine-google_en.
[28] https://www.dataguidance.com/news/spain-aepd-fines-google-10m-unlawful-transfer-personal.
[29] https://www.smh.com.au/business/consumer-affairs/google-fined-60m-for-misleading-android-users-about-data-collection-20220812-p5b9hg.html.
[30] https://apnews.com/article/technology-south-korea-252a9cc71f0875575340ade7265af951.

j. On September 28, 2022, Google agreed to a $100M settlement in class action lawsuit, *Rivera, et al. v. Google*. The lawsuit alleges that Google violated Illinois law by collecting and storing biometric data of individuals who, while residing in Illinois, appeared in a photograph in the photograph sharing and storage service known as Google Photos.[31]

k. On October 4, 2022, Arizona Attorney General Mark Brnovich announced a historic $85 million settlement with Google for deceptively obtaining users' location data to make billions of dollars in profit.[32]

l. On November 14, 2022, Google agreed to a $391.5 million settlement to resolve litigation brought by a 40-state coalition of attorneys general for charges that Google misled users into thinking they had turned off location tracking in their account settings even as the company continued collecting that information.[33]

m. As of December 30, 2022, Google was ordered to pay $9.5 million of the total settlement amount of $29.5 million to the District of Columbia after it sued the company alleging that it tracked users' locations without their permission.[34]

n. As of January 3. 2023, Google is to pay Indiana $20 million to resolve the state's lawsuit regarding Google's allegedly deceptive location tracking practices.[35]

o. On Jan 5, 2023, Google agreed to pay $23 million to resolve a consolidated, California-based class-action lawsuit brought by consumers for sharing the contents of their queries with advertisers or other third parties without their permission. The proposed settlement also requires Google to provide extra disclosures to users about search term-sharing practices. The settlement is awaiting court approval.[36]

SUBSTANTIVE ALLEGATIONS

I. GOOGLE TARGETED CHILDREN UNDER THIRTEEN VIA THE DESIGNED FOR FAMILES PROGRAM

100. Children are among the most valuable demographics for advertisers to reach for at least two reasons. First, children are easily influenced. It is for this very reason, and based on their inherent

[31] https://www.law360.com/articles/1534091/google-s-100m-bipa-deal-gets-final-approval.
[32] https://www.azag.gov/press-release/attorney-general-mark-brnovich-achieves-historic-85-million-settlement-google.
[33] https://www.nytimes.com/2022/11/14/technology/google-privacy-settlement.html.
[34] https://www.visitor-analytics.io/en/blog/google-location-tracking-without-consent/.
[35] https://www.wthr.com/article/news/local/google-to-pay-indiana-20-million-to-resolve-privacy-lawsuit/531-48ebaee6-ee2b-4f2f-9009-d71e43aaaab7.
[36] *See In re Google Referrer Header Privacy Litig*., Case No. 10-cv-04809 (N.D. Cal.).

vulnerabilities, children enjoy special protections from invasion of privacy, including from those such as advertisers seeking to influence them. While COPPA codified protections for children under 13 regarding surreptitious tracking online without parental consent, state common laws have long protected against unreasonable, unwarranted, and offensive intrusions into children's privacy.

101. Second, children influence the spending habits of their entire families. For example, in 2008, it was estimated that American children under 12 directly influence over 700 billion dollars in family spending a year, a figure that has since increased. Additionally, recent studies show that 80% of parents believe that kids play a role in household purchasing decisions, with an outsized influence over purchases of toys (92%), electronics (68%), clothing (88%), food (87%), entertainment (91%), travel (84%).[37] Unfortunately, this influence is why unscrupulous advertising companies such as Google target children.

102. Recognition of the value of children under thirteen as an advertising audience is why Google developed the "honeytrap" DFF program. DFF was designed in response to what Google anticipated would be a reluctance on the part of parents to allow their children to have access to apps on Android devices, because of the ubiquity of surveillance-based ads within the Android ecosystem.

103. Google brazenly made no attempt to hide who they were targeting with the DFF program:

> The Designed for Families program is designed to be inclusive of apps ***that are made for kids*** as well as those that can be enjoyed by the entire family. ***General audience apps that have no specific benefit or relevance for audiences under the age of thirteen will not be accepted into the program***. To participate, there are specific guidelines and policies your apps need to meet, which are assessed in an app content review.[38]

[37] https://insights.paramount.com/post/kids-are-engaged-consumers-who-exert-a-powerful-influence-on-family-purchases/

[38] https://web.archive.org/web/20150623031124/http://developer.android.com/distribute/googleplay/families/about.html.

104. Google further stated that the DFF program was established in order to "help[] developers connect with families on Google Play" and to "help parents discover great, age-appropriate content and make more informed choices" regarding their children's Android App use.

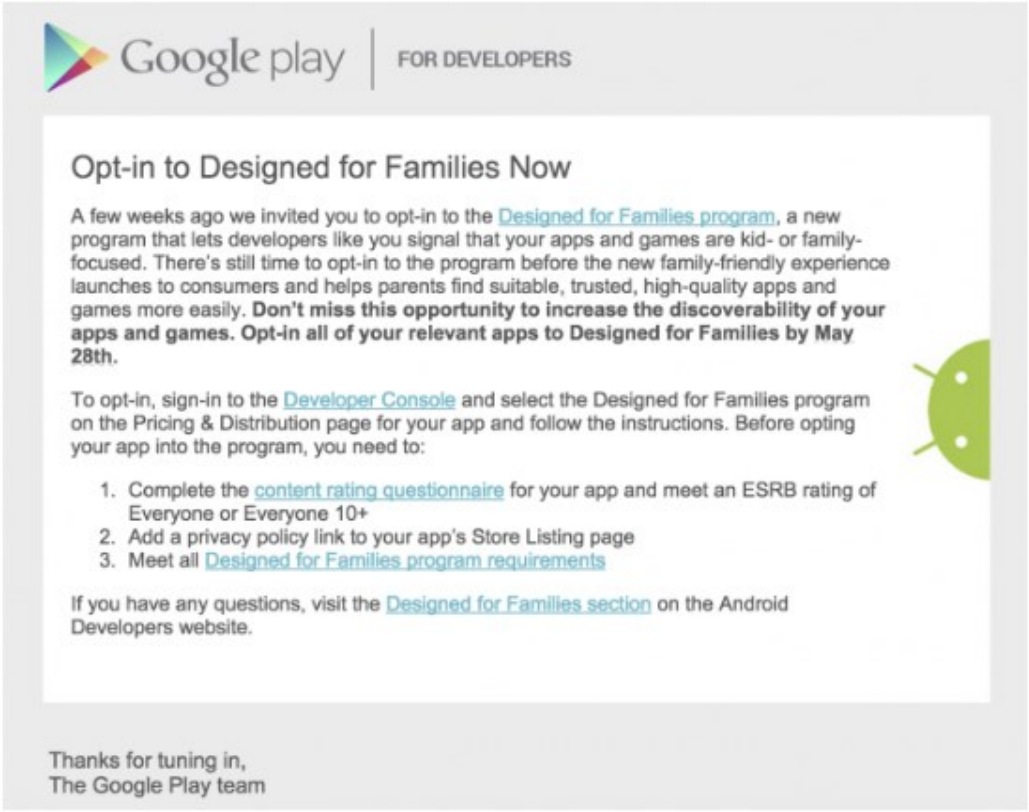
II. GOOGLE INCENTIVIZED APP DEVELOPERS TO MAKE CHILD-DIRECTED CONTENT

105. After conceiving of the DFF program. Google needed to generate content for it. Google incentivized App developers to make child-directed Apps for the DFF program in two ways:

(1) by promising App developers greater visibility (and thus more downloads and users) via the DFF program's special perks; and

(2) providing a way for App developers to monetize those downloads and users.

106. For example, shortly after launching the DFF program, Google sent the following email to App developers:



Google play | FOR DEVELOPERS

Opt-in to Designed for Families Now

A few weeks ago we invited you to opt-in to the Designed for Families program, a new program that lets developers like you signal that your apps and games are kid- or family-focused. There's still time to opt-in to the program before the new family-friendly experience launches to consumers and helps parents find suitable, trusted, high-quality apps and games more easily. **Don't miss this opportunity to increase the discoverability of your apps and games. Opt-in all of your relevant apps to Designed for Families by May 28th.**

To opt-in, sign-in to the Developer Console and select the Designed for Families program on the Pricing & Distribution page for your app and follow the instructions. Before opting your app into the program, you need to:

1. Complete the content rating questionnaire for your app and meet an ESRB rating of Everyone or Everyone 10+
2. Add a privacy policy link to your app's Store Listing page
3. Meet all Designed for Families program requirements

If you have any questions, visit the Designed for Families section on the Android Developers website.

Thanks for tuning in,
The Google Play team

107. Google promised App developers DFF Apps would be specially featured and thus easily found by children:

> If you've built great apps designed for kids or families, the family discovery experience on Google Play is a great way to surface them to parents.
>
> Developers are invited to opt-in these apps and games to the new Designed for Families program. Apps that meet the program requirements will be featured through Google Play's family-friendly browse and search experiences so that parents can find suitable, trusted, high-quality apps and games more easily.
>
> Designed for Families expands 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.[39]

108. Google also offered special privileges to DFF Apps designed to increase their visibility to children under 13, including:

a. **Search:** Only apps and games opted-in to the Designed for Families program will show up in searches initiated from the Family section in Apps Home. They'll also be more visible when users search for family or kid related content from anywhere in the Play store.

b. **Browse**: The Family star button on Apps and Games Home points to an enhanced discovery experience for parents looking for family appropriate content. The new Family section includes uniquely merchandised content, new categories, and age-based browsing. Participating apps will receive this additional visibility on top of their existing categories, rankings, and reviews elsewhere on the Google Play store.

c. **Character pages**: Parents can now discover content for popular characters from around the globe in one place, including apps, games, movies, tv shows, books, and even music. This provides a powerful way for parents to discover content from familiar brands and beloved characters, and allows you to reach a highly relevant and targeted audience.

d. **Merchandising**: The family sections include their own merchandised collections. The themed collections on these pages are curated to ensure quality and limited only to content accepted into the Designed for Families program.

---

[39] https://web.archive.org/web/20150623031124/http://developer.android.com/distribute/googleplay/families/about.html

e. **Badging**: Apps participating in Designed for Families are marked with the family star badge, which reflects the target age you select for your apps and serves as a signal of quality for parents.[40]

109. The special features and privileges afforded to DFF Apps were meant to increase the downloads and usage of the DFF Apps which would in turn translate into more advertising revenue for the App developers and Google.

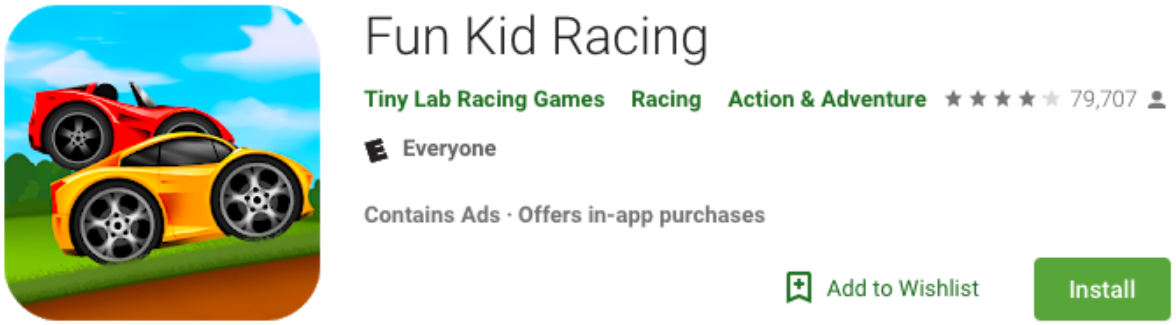
110. The incentives Google offered caused App developers to create Apps for the DFF program intentionally designed to attract children under thirteen (as the DFF program required), including content featuring cartoons, cars, racing, and children songs, such as that included in Fun Kid Racing, GummyBear and Friends Speed Racing, and Monster Truck Racing (among many others).

111. As just one example, in response to Google's efforts, App developer Tiny Lab Productions submitted 86 Apps which were accepted into Google's DFF program and made available to download in the Google Play Family section. These Apps are listed in Exhibit A, and include the following apps downloaded and used by Plaintiffs during the relevant time period: Fun Kid Racing, GummyBear and Friends Speed Racing, and Monster Truck Racing.

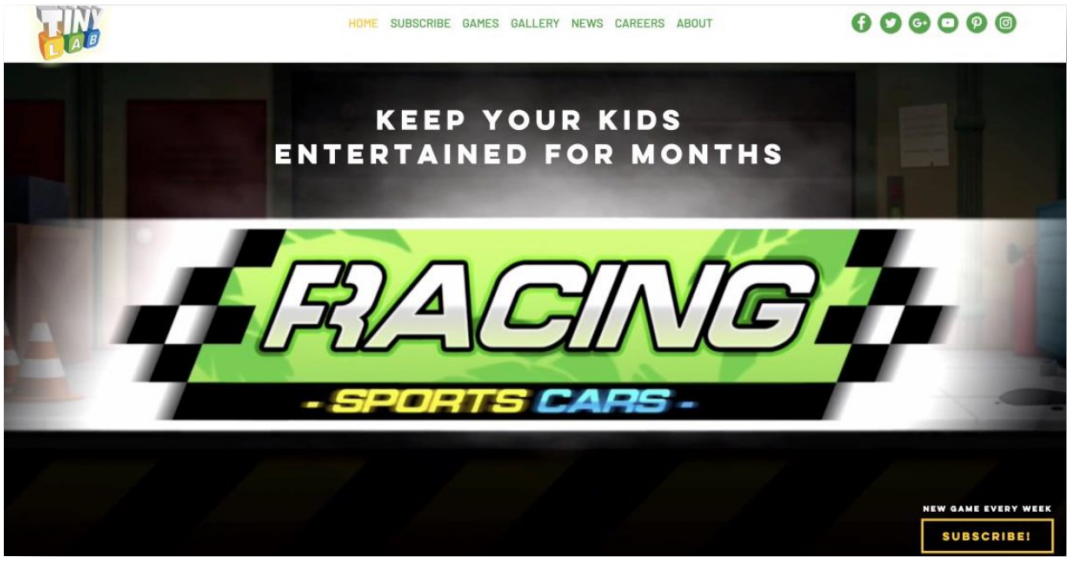
112. As shown in Exhibit A, which is a list of all Tiny Lab DFF Apps, nearly all of the Tiny Lab DFF Apps had names clearly indicating the Apps were directed towards children and had features clearly meant to attract children such as Fun Kid Racing.

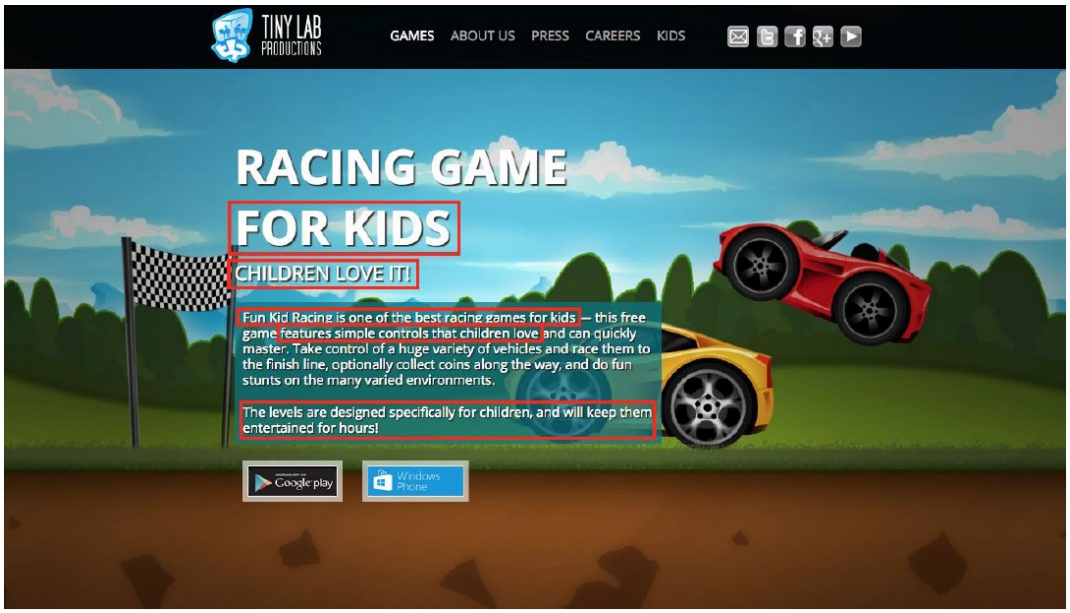
113. Fun Kid Racing was presented to individuals who accessed the Family section of Google Play as follows:

40 https://web.archive.org/web/20150623031124/http://developer.android.com/distribute/googleplay/families/about.html



114. Beyond the inherent characteristics of the name, Tiny Lab took additional steps to promote Fun Kid Racing as specifically meant for children by, for example, explicitly stating that the Apps were meant "for kids" on their website:





A. GOOGLE REVIEWED EACH DFF APP SUBMISSION TO ENSURE ONLY CHILD-DIRECTED CONTENT WAS APPROVED BECAUSE GOOGLE WANTED TO LURE CHILDREN UNDER THIRTEEN TO ANDROID.

115. Because the purpose of the DFF program was to build a child audience for advertisers, Google explicitly stated as part of its guidelines that Google did not want App developers to submit general audience apps "that have no specific benefit or relevance for audiences under the age of thirteen" for inclusion in the DFF program and that Google would not accept such Apps into the DFF program.

116. While Google represented that review of Apps submitted for inclusion in the DFF program was to ensure that children were protected, in reality, Google conducted its review to ensure the Apps included in the DFF program would successfully attract children because Google did not want the DFF program to be full of Apps that were not effective at drawing in children – a lucrative advertising audience.

117. Thus, Google reviewed each DFF App submission to ensure that the App provided a specific benefit to children under thirteen or was relevant to children under thirteen.

B. GOOGLE'S "SPECIFIC BENEFIT" OR "RELEVANT" REQUIREMENTS MEANT THAT ALMOST EVERY APP IN THE DFF PROGRAM WAS "CHILD-DIRECTED" PURSUANT TO COPPA

118. Google's requirements that Apps have a "specific benefit" or "relevance" for children under thirteen meant that most of the DFF Apps which Google reviewed are, under Section 312.2, considered "child-directed content" for purposes of COPPA.

119. Section 312.2 of COPPA states that the determination of whether an App is "directed to children" depends on factors such as the App's "subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics… as well as whether advertising promoting or appearing on the App is directed to children." Competent and reliable empirical evidence regarding audience composition as well as the intended audience should be considered.

120. Google itself currently summarizes this determination as follows:

> **What is "made for kids" content?**
>
> According to the FTC's guidance on the Children's Online Privacy Protection Act (COPPA), a video is made for kids if:
>
> - Children are the primary audience.
> - Children are not the primary audience, but the video is still directed to children based on factors such as the subject matter of the video, whether the video has an emphasis on kids characters, themes, toys or games, and more.
>
> Learn more about determining if your content is "made for kids", and check out our frequently asked questions on the topic.

121. Because any App "made for kids" or "that can be enjoyed by the entire family" or provides a "specific benefit or relevance for audiences under the age of thirteen" is considered "child-directed" as defined under COPPA, and because Google certified that every App included in the DFF program met these criteria, Google had actual knowledge that every DFF App was "child-directed" as defined under COPPA.

122. According to FTC guidance, even if children are not the primary audience but the website or online service targets children as one of its audiences, the service is "directed to children" under COPPA and compliance is required for children under 13.[41]

III. GOOGLE INCENTIVIZED APP DEVELOPERS TO MISCATEGORIZE THEIR APPS AND BAIT AND EXPLOIT CHILDREN FOR PROFIT

123. Google successfully incentivized App developers to create child-directed content. As of March 2018, approximately 5,855 child-directed apps had been voluntarily submitted to and accepted into the DFF program and had achieved a cumulative install count of 4.5 billion installs, an average of approximately 750,000 installs per DFF App.

124. To monetize this exposure, DFF App developers had two choices: (1) charge users a fee to download and/or use the app; or (2) allow free download and use of the App but show advertising to users to earn revenue.

125. For child-directed content, free-to-play Apps allowing behavioral advertising shown are generally considered the more lucrative option for App developers it avoids the friction of requiring children to ask for money to download and play the app and allows App developers to earn a continuous stream of advertising revenue exceeding a one-time fee.

126. But DFF App developers who chose the free-to-play model had to make one additional choice: how to categorize their DFF App.

127. If an App developer categorized an App as "intended primarily for children," Google would not permit the App to exfiltrate the data of the App's users and show behavioral advertising to those users, the most lucrative type of advertising for both Defendants and App developers.

[41] https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business

128. But, if an App developer categorized an App as "mixed-audience" or "not primarily intended for children," Google allowed the App—via the SDKs integrated into the App—to exfiltrate the data of all of the users of the App and show the users behavioral advertising.

129. Thus, both Defendants and DFF App developers stood to benefit economically from advertising revenue if a DFF App were permitted to be categorized as "mixed-audience" or "not primarily intended for children."

130. Unsurprisingly, Defendants' promises of more money in advertising revenue incentivized App developers to mis-categorize their Apps as mixed audience so that both App developers and Defendants could profit by exfiltrating the data of the App user children under thirteen and showing them behavioral advertising.

131. This ploy occurred notwithstanding Google's purported vetting of the Apps and the strict legal guidelines of the DFF program. Defendants and the App developers attempted to justify this behavior, despite COPPA's prohibition of it, by hiding behind the artifice that the Apps were intended for mixed audiences and not for children under thirteen. Thus, according to Defendants, Defendants had no obligation to comply with COPPA because they could not be charged with actual knowledge that children under thirteen were using the Apps.

132. This reasoning, of course, is belied by Google's stated purpose of, and legal requirements governing, the DFF program, which was "family friendly," "made for kids," designed in large part for children "under the age of thirteen," and the fact that the Apps were clearly intended for use by young children.

133. Defendants' conduct is further belied by their dealings with security researchers from the University of California in 2018. According to the Office of the Attorney General for the State of New Mexico (the "NM AG"), in the Spring of 2018, security researchers at the University of California, Berkeley (the "Berkeley Researchers") informed Defendants of rampant and what the Berkeley

Researchers believed to be unlawful, surreptitious tracking and data exfiltration by Apps included in Google's DFF program in violation of, *inter alia*, COPPA, using Tiny Lab as an example:

> 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.

134. According to the NM AG, Google responded by stating they could not detect or prevent the mischaracterization of Apps at scale but that the DFF Apps identified by the Berkeley Researchers were, in any event, not "designed primarily for children, but for families in general" and, therefore, were not violating COPPA by showing behavioral advertising to users of the Apps.

135. Again, Google's facile response was intended to evade liability for its unlawful conduct. Further, it betrays Google's pattern of business methods which elevate profits over compliance with the law and societal norms. This is evidenced in part by Google's history of settlements with regulators (and myriad lawsuits) for these types of practices as outlined herein, including the FTC regarding Google's practices in tracking children under 13 for behavioral advertising on Google's YouTube video

platform and the NM AG's office concerning Google's tracking practices through AdMob based on Tiny Lab Apps (and others).

136. As part of the settlement agreement entered into by Google, AdMob, and the NM AG on December 10, 2021, Google and AdMob agreed to implement the following changes to prevent mis-categorization of DFF Apps as "mixed-audience" or "not primarily intended for children":

> **Google Play** . . . **4.1.1. Policy Changes**. Google has revised its Google Play Families policies, including its "Designing Apps for Children and Families" and "Ads and Monetization" policies . . . Google will maintain these resources, along with Google Play Academy courses and additional Help Center articles (sample descriptions of which are attached hereto as Exhibit 4) to help app developers create content for children in line with the revised policies.
>
> **4.1.2. TAC Form**. Google will require all app developers with active apps on Google Play to complete a Google Play Target Audience and Content ("TAC") form [. . .] to indicate the targeted age groups of apps submitted to Google Play.
>
> **4.1.3. ATK Rubric**. Google will implement, and update as necessary, a rubric with which to evaluate Google Play app submissions to help determine whether an app targets or appeals to kids ("ATK"), independent from an app developer's TAC submission(s).
>
> **4.1.3.1**. This rubric will take into account child-directed popular characters, images, and terms. The rubric will include, inter alia, criteria substantially similar to and consistent with the criteria currently set forth in the "Families" page of the Google Play Academy (https://play.google.com/console/about/families/), as well as the developer support page "Manage Target Audience and App Content Settings" (https://support.google.com/googleplay/androiddeveloper/answer/9867159?visit_id=637522057853722464- 2168424342&rd=1#age-groups&zippy=%2Cage-and-under%2Cages--). In addition, the State may provide a list of any child-directed characters, images, or terms to be considered for inclusion in this rubric.
>
> **4.1.3.2**. In the event that Google determines—via the ATK rubric—that an app may have been misclassified in the TAC submission, Google will require the developer to correct its TAC submission or change the content of the app to match the TAC submission.
>
> **AdMob**. Google will maintain a mechanism that will communicate the child-directed status of apps on Google Play to AdMob to help promote consistent treatment of those apps by AdMob. Within 30 days of an app's child-directed status being communicated to AdMob, AdMob will begin to treat the app and the data previously collected therefrom in a manner consistent with COPPA and other applicable legal obligations.

137. These mandatory changes can be summarized as ensuring that Google and AdMob comply with COPPA and the New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-1, *et seq.* (the "NMUPA")

138. Of course, had Google and AdMob not been knowingly violating COPPA and the NMUPA by incentivizing App developers to mis-categorize their Apps to exploit children for profit, these mandatory changes would have been unnecessary.

IV. ECONOMIC INCENTIVES DROVE GOOGLE AND ADMOB TO UNLAWFULLY TRACK, PROFILE, AND TARGET CHILDREN UNDER THIRTEEN AND SERVE THEM WITH BEHAVIORAL ADVERTISING

139. As illustrated in Google's response to the Berkeley Researchers and Google's subsequent settlement with the NM AG, Google used App developers' mis-categorization of their own DFF Apps to justify allowing third-party advertising platforms to exfiltrate the data of DFF App users and show them behavioral advertising for profit.

140. And worse, where AdMob was one of the SDKs integrated into a DFF App, Google itself, via AdMob, was the one doing the exfiltrating of Personal Information of all users of DFF Apps in which the AdMob SDK was installed, including from children under thirteen.

141. Google and AdMob knew at the time that their actions were resulting in the exfiltration data from millions of children under thirteen but engaged in this illicit conduct to earn billions of dollars in advertising revenue.

142. Because Google controlled the DFF program and required the DFF Apps to be child-directed to be included in the DFF program, Google (and thus AdMob) had actual knowledge that the Personal Information of DFF App users under thirteen was being collected.

143. Despite Defendants' actual knowledge that the core audience and/or user base of DFF Apps consisted of children under thirteen, Defendants exfiltrated the data of *every* DFF App user as long

as (1) the DFF App was categorized as "not primarily intended for children" by the App developer; and (2) AdMob was installed in the DFF App.

144. Defendants aggregated the data taken from DFF App users, including children under thirteen, with other data Google already possessed to build profiles of the children.

145. Defendants then used these extensive profiles to serve the children under thirteen using DFF Apps in which AdMob was integrated with behavioral advertising.

146. Defendants profited from every advertisement shown to DFF App users, including those shown to children under thirteen.

147. Google and AdMob knowingly engaged in this conduct despite the fact that many, if not the vast majority of, these users were children under thirteen, because of the enormous financial benefits to Defendants from advertising revenue, which, upon information and belief, far outweighed – according to their calculus – any potential fine(s) or penalty(ies).

148. Defendants' behavior was confirmed with respect to several DFF Apps, including Fun Kids Racing, by forensic analysis performed by the Office of the Attorney General for the State of New Mexico.

149. To analyze Fun Kid Racing, the NM AG executed the Fun Kid Racing App in an instrumented environment for an extended period of time, which allowed observation of the data flows of Fun Kid Racing.

150. NM AG's analysis confirmed that, despite Fun Kid Racing's inclusion in the DFF program and Google's actual knowledge that Fun Kid Racing was directed towards children under 13, Google caused the AdMob SDK to collect the following information from users of the DFF App Fun Kid Racing:

a. **Android Advertising ID ("AAID")**: An AAID is a unique identifier assigned to an Android device by Google. The AAID is used to exfiltrate user data and deliver behavioral advertising based on that data.

b. **International Mobile Equipment Identity ("IMEI")**: is a unique identification number assigned to every mobile device, including smartphones and tablets. The IMEI is a 15-digit number that is used to identify the device and its capabilities on a mobile network. IMEI serves as a device's fingerprint and can be used to track and identify it if it's lost or stolen. It cannot be reset by a user.

c. **Device IP Address:** An IP address, or Internet Protocol address, is a unique numerical identifier that is assigned to devices that are connected to a network that uses the Internet Protocol for communication. This address is used to identify and communicate with devices on the network, much like a telephone number is used to identify and connect with a person on a telephone network. Thus, recording the IP address of child's device means that Google can identify and locate that child on the internet and across multiple devices via the IP address.

d. **Device Manufacturer, make, and model**: The AdMob SDK exfiltrated the device manufacturer, the type of device and model number and combined this with other data points to track users across Apps and platforms and serve them with behavioral advertising.

e. **Device Operating System**: AdMob exfiltrated the operating system running on a device down to the version that was running on the user's device. When paired with other persistent identifiers, this information allows AdMob to track the user across Apps.

151. The result of the collection of this data, according to the NM AG, was that:

> "These apps can track where children live, play, and go to school with incredible precision . . . These multi-million-dollar tech companies partnering with app developers are taking advantage of New Mexican children, and the unacceptable risk of data breach and access from third parties who seek to exploit and harm our children will not be tolerated in New Mexico."[42]

152. Google, via AdMob, collected this information despite having actual knowledge that the Fun Kids Racing App was directed towards children under 13 and despite explicitly stating that Google intended the DFF program and Google Play Family section to be a place that offered content for children under the age of thirteen, a group that enjoys special protections from this very behavior.

153. Neither Google, nor AdMob obtained parental consent to collect this information as required by COPPA.

[42] https://gizmodo.com/new-mexico-sues-google-twitter-and-app-developers-ove-1829109436

154. Forensic testing further confirmed that Tiny Lab Productions incorporated the AdMob SDK into each of their 86 DFF Apps, including GummyBear and Friends Speed Racing and Monster Truck Racing, and that the AdMob SDK operated similarly in Fun Kid Racing in the other Tiny Lab Apps, including GummyBear and Friends Speed Racing and Monster Truck Racing.

155. Upon information and belief, the AdMob SDK was integrated into at least hundreds, if not thousands, of additional DFF Apps during the Class Period.

156. Google's settlement with the FTC regarding its tracking of children on Google's YouTube platform demonstrates Google's pattern and practice of using the "mixed-audience" pretext given that it likewise asserted the similarly unfounded justification in that case as well. There, Google purported it had no duty to comply with COPPA because, like here, many videos uploaded to the YouTube platform were categorized by the creators as intended for "mixed" or "general" audiences. Ultimately, however, Google paid $170 million in civil penalties and made mandatory revisions to its YouTube policies to resolve the FTC action.

157. Similarly, Google and AdMob were forced to pay $5 million to the NM AG to resolve claims that the *exact* behavior Plaintiffs allege in this complaint violated COPPA, the New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-1, *et seq.*, and constituted intrusions on New Mexico citizens' solitude, seclusion, or private affairs in violation of their reasonable expectations of privacy in their mobile devices and their online behavior.

158. As Google and AdMob's settlement with the NM AG makes clear, Google and AdMob's practices with respect to the DFF program not only violate COPPA, but also independently violate the state statutes prohibiting unfair and deceptive business practices modeled or patterned after, and/or which take interpretive guidance from, the FTC Act (the "Little FTC Acts"), including those enacted by California, Florida, and New York.

159. These violations of COPPA and Little FTC Acts allowed Defendants to make billions of dollars in advertising revenue *and* have given Defendants an invaluable and significant "first mover" advantage that cannot be undone.

160. Defendants operate the first and second-most visited websites in the world and the most popular mobile operating system in the world. As a result of their unlawful conduct, Defendants' algorithms now incorporate ill-gotten data gleaned from billions of instances of children's online activity. The deep insights gleaned from these viewing sessions will enable the Defendants to keep children using Apps and will solidify the Defendants' dominance in the market for child-related content.

V. DEFENDANTS' TRACKING, PROFILING, TARGETING AND EXPLOITATION OF CHILDREN WITHOUT PARENTAL CONSENT VIOLATED PLAINTIFFS' AND CLASS MEMBERS' REASONABLE EXPECTATIONS OF PRIVACY AND IS HIGHLY OFFENSIVE

161. Defendants' conduct in violating privacy rights and reasonable expectations of privacy of Plaintiffs and Class members is particularly egregious because Defendants violated laws designed to protect a group—children—that society has long recognized as vulnerable to exploitation and manipulation.

162. Parents' interest in the care, custody, and control of their children is one of the most fundamental liberty interests recognized by society. It has long been recognized that parents should maintain control over who interacts with their children and how.

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

164. In fact, as discussed above, the FTC's enhancements of COPPA in 2013 reflect the specific concern with mobile app tracking and reflect the offensiveness with which society regards this behavior.

165. Children develop the ability to use smartphones and tablets by the age of two. Almost every family with a child younger than eight in America has a smartphone (95%) and/or tablet (78%) in the household.[43]

166. Often, children are given their own devices, with a 2015 study finding that 75% of children in the United States had their own tablet, smartphone, or iPod.[44]

167. Nearly all parents in the United States (94%) say their children under 13 use online apps, with top apps used being video streaming (64%), video gaming (58%) and show/movie streaming (58%).[45]

168. Four in five parents (80%) whose children under 13 use online apps say they worry about their children's privacy when using those apps,[46] with the top concern (69%) being data tracking.[47]

169. Nearly 3 in 4 parents whose children under 13 use online apps (73%) say they are concerned about their children's location being tracked by those apps; those residing in urban or rural areas are more likely than those residing in suburban areas to share this sentiment (88% and 87% vs. 73%).[48]

170. More than three-quarters (77%) of parents are concerned about protecting their family's digital privacy.[49]

[43] https://www.commonsensemedia.org/press-releases/new-research-by-common-sense-finds-major-spike-in-mobile-media-use-and-device-ownership-by-children-age.
[44] Dangers of YouTube for Kids, THE ATLANTIC (Nov. 2018), https://www.theatlantic.com/magazine/archive/2018/11/raised-by-youtube/570838/.
[45] https://www.pixalate.com/blog/childrens-online-privacy-harris-poll-recap.
[46] *Id.*
[47] https://www.cdpinstitute.org/news/childrens-privacy-data-tracking-is-a-big-concern-for-parents-and-trust-levels-in-companies-are-low/.
[48] https://www.pixalate.com/blog/childrens-online-privacy-harris-poll-recap.
[49] https://trustedfuture.org/childrens-digital-privacy-and-safety.

171. 73% of parents are concerned about personal data being collected by third parties, without their consent.[50]

172. And parents also recognize the importance of protecting their children's identity (90%), location (88%), health data (87%), age (85%), school records (85%), and browsing history (84%).[51]

173. Additionally, 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 federal law and state common law.[52] The parents who were polled responded as follows when asked whether they agreed or disagreed with the following statements:

174. "It is okay for advertisers to track and keep a record of a child's behavior online if they give the child free content."

a. 5 percent strongly agree

b. 3 percent somewhat agree

c. 15 percent somewhat disagree

d. 75 percent strongly disagree

e. 3 percent do not know or refused to answer

175. "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."

a. 3 percent strongly agree.

b. 17 percent somewhat agree.

c. 10 percent somewhat disagree

---

[50] *Id.*
[51] *Id.*
[52] *See, e.g.*, https://www.democraticmedia.org/sites/default/files/COPPA%20Executive%20Summary%20and%20Findings.pdf.

d. 69 percent strongly disagree

e. 1 percent do not know or refused to answer

176. "It is okay for advertisers to collect information about a child's location from that child's mobile phone."

a. 6 percent strongly agree

b. 3 percent somewhat agree

c. 7 percent somewhat disagree

d. 84 percent strongly disagree

e. less than 1 percent do not know or refused to answer

177. "Before advertisers put tracking software on a child's computer, advertisers should receive the parent's permission."

a. 89 percent strongly agree

b. 5 percent somewhat agree

c. 2 percent somewhat disagree

d. 4 percent strongly disagree

e. less than 1 percent do not know or refused to answer

178. "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?"

a. 93 percent said it was a good idea

b. 6 percent said it was a bad idea

c. 1 percent did not know or refused to answer.

179. This proliferation of internet-connected device usage by children under thirteen, coupled with the concerns expressed by parents renders Defendants' conduct highly offensive and an egregious breach of social norms.

180. Defendants' unlawful collection of Personal Information and manipulative advertising tactics substantially impact the amount of time children under thirteen spent using DFF Apps.

181. The behavioral advertising shown to children using miscategorized child-directed DFF Apps subjected an already-vulnerable population to the impact of advertising which easily influences adults.

182. Defendants exploited children under thirteen for financial gain by luring them with child-directed content and manipulating them into remaining engaged with DFF Apps to the detriment of their mental health, so that they could earn advertising revenue.

183. Defendants benefit from increased mobile device usage. The longer and more often a child plays DFF Apps, the more data Defendants can exfiltrate and the more advertisements they can show the child.

184. Defendants have thus also been incentivized to develop ways to addict children to Apps, which advertisers like AdMob refer to as "retention."

185. AdMob markets their ability to help App developers such as Tiny Lab and others in which the AdMob SDK was installed increase user retention, and thus increase the advertisements shown to users and the revenue earned through behavioral advertising.

186. Children are specifically targeted as part of this effort, and Defendants' retention services are fueled by children's Personal Information.

187. To enhance retention, AdMob uses the Personal Information of children under thirteen, analyzes their behavior, and uses trigger events—both within the Apps and across the Internet—that will encourage them to play the Apps more often and for longer periods.

188. Defendants then continue to entice children under thirteen to continue to play Apps, often to their detriment, all to increase Defendants' own revenue.

189. This exploitation and manipulation of children constitutes unfair, deceptive, unlawful, and unconscionable conduct, and an egregious invasion of privacy.

190. By failing to (1) obtain parental consent, (2) disclose to parents the nature of their data collection practices, and (3) take other steps to preclude the capture of children's Personal Information, Defendants have breached the privacy rights and reasonable expectations of privacy of Plaintiffs and the millions of other minors who used DFF Apps and were shown behavioral advertisements in contravention 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.

V. VALUE OF PERSONAL INFORMATION

191. Plaintiffs and the Classes and Subclasses have been deprived of, and thereby lost, the economic value of their Personal Information. There is a market for this Personal Information. As the advertising revenue figures outlined herein demonstrate, this information has tremendous value to Google, AdMob and the App developers who share in the advertising revenue. On the open market, PII is often mined, compiled, and resold by data brokers.[53] Further, there is a market for consumers to monetize Personal Information and the behavioral preferences that Defendants have usurped. Multiple published analyses and studies have placed a value in excess of $200 on an individual's Personal Information;[54] for example, one individual sold his data for $2,733 on Kickstarter.[55] Surveys have

[53] https://www.visualcapitalist.com/much-personal-data-worth/.
[54] Can you Put a Price on Your Personal Data, June 28, 2019, NYTimes, https://www.nytimes.com/2019/06/28/technology/data-price-big-tech.html
[55] *"How Much Is Your Personal Data Worth?"*, THE GUARDIAN (April 22, 2014), https://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth.

shown that American adults place significant value on their data and would not willingly transfer it over without significant compensation.[56]

192. A child's Personal Information has equivalent (or potentially greater) value than that of an adult to companies like Google. As described above, a child is more susceptible to being influenced by advertisements as they often cannot tell the difference between content and advertisements. In addition, Google and AdMob may be able to utilize children's Personal Information to show them behavioral advertising for the duration of their lives. Plaintiffs and the Classes and Subclasses can no longer realize the full economic value of their Personal Information because their Personal Information has already been collected, analyzed, acted upon, and monetized by Defendants.

VI. ALLEGATIONS RELATING TO PLAINTIFFS

A. PLAINTIFF A.B.

193. At all relevant times, Plaintiff A.B. used Android Apps included in the DFF program.

194. A.B. used monetized Android Apps included in the DFF program, including Fun Kid Racing and Monster Truck Racing.

195. Defendants (and App developers) collected and enabled collection of A.B.'s Personal Information for the purposes of tracking, profiling, and targeting A.B. with advertisements as he used the Android Apps.

196. Neither the Defendants nor the App developers obtained verifiable parental consent prior to the collection of A.B.'s Personal Information.

197. Neither Plaintiff A.B. nor his parent and guardian Jen Turner could have reasonably discovered this conduct earlier through investigation. Plaintiff A.B. is a minor unable to consent to or

[56] https://simpletexting.com/personal-data-value/.

understand Defendants' tracking of personal information, and Defendants concealed their tracking, profiling, and targeting of A.B.

198. The tracking, profiling, and targeting of A.B. without parental consent by the Defendants and these App developers is highly offensive and constitutes an invasion of A.B.'s privacy.

B. PLAINTIFFS C.D.1, C.D.2, AND C.D.3

199. At all relevant times, Plaintiffs C.D.1, C.D.2, and C.D.3 used Android Apps included in the DFF program.

200. C.D.1, C.D.2, and C.D.3 used monetized Android Apps, included in the DFF program, including Fun Kid Racing.

201. Defendants (and App developers) collected and enabled collection of C.D.1's, C.D.2's, and C.D.3's Personal Information for the purposes of tracking, profiling, and targeting C.D.1, C.D.2, and C.D.3 with advertisements as they used the Android Apps.

202. Neither the Defendants nor the App developers obtained verifiable parental consent prior to the collection of C.D.1's, C.D.2's, and C.D.3's Personal Information.

203. Neither Plaintiffs C.D.1, C.D.2, and C.D.3 nor their parent and guardian Kirenda Johnson could have reasonably discovered this conduct earlier through investigation. Plaintiffs C.D.1, C.D.2, and C.D.3 are minors unable to consent to or understand Defendants' tracking of personal information, and Defendants concealed their tracking, profiling, and targeting of C.D.1, C.D.2, and C.D.3.

204. The tracking, profiling, and targeting of C.D.1, C.D.2, and C.D.3 without parental consent by the Defendants and these App developers is highly offensive and constitutes an invasion of C.D.1's, C.D.2's, and C.D.3's privacy.

C. PLAINTIFFS E.F.1 AND E.F.2

205. At all relevant times, Plaintiffs E.F.1 and E.F.2 used Android Apps included in the DFF program.

206. E.F.1 and E.F.2 used monetized Android Apps included in the DFF program including Fun Kid Racing and GummyBear and Friends Speed Racing.

207. Defendants (and App developers) collected and enabled collection of E.F.1's and E.F.2's Personal Information for the purposes of tracking, profiling, and targeting E.F.1 and E.F.2 with advertisements as he used the Android Apps.

208. Neither the Defendants nor the App developers obtained verifiable parental consent prior to the collection of E.F.1's and E.F.2's Personal Information.

209. Neither Plaintiffs E.F.1 and E.F.2 nor their parent and guardian Barbara Hayden-Seaman could have reasonably discovered this conduct earlier through investigation. Plaintiffs E.F.1 and E.F.2 are minors unable to consent to or understand Defendants' tracking of personal information, and Defendants concealed their tracking, profiling, and targeting of E.F.1 and E.F.2.

210. The tracking, profiling, and targeting of E.F.1 and E.F.2 without parental consent by the Defendants and these App developers is highly offensive and constitutes an invasion of E.F.1's and E.F.2's privacy.

TOLLING AND ESTOPPEL

I. DISCOVERY RULE TOLLING

211. Plaintiffs, the Classes, and the Subclasses had no way of knowing about Defendants' conduct with respect to the collection and impermissible and unauthorized use of, and profit from, the Personal Information of Plaintiffs and the members of the Classes and Subclasses.

212. Neither Plaintiffs nor any other members of the Classes and Subclasses, through the exercise of reasonable diligence, could have discovered the conduct alleged herein. Further, Plaintiffs and the members of the Classes and Subclasses did not discover, and did not know of, facts that would have caused a reasonable person to suspect, that Defendants were engaged in the conduct alleged herein.

II. FRAUDULENT CONCEALMENT TOLLING

213. By failing to provide notice of the collection and use of the Personal Information and obtain verifiable consent, in violation of COPPA and societal norms and conventions, Defendants concealed their conduct and the existence of the claims asserted herein from Plaintiff and the members of the Classes and Subclasses.

214. Upon information and belief, Defendants intended by their acts to conceal the facts and claims from Plaintiffs and members of the Classes and Subclasses. Plaintiffs and the members of the Classes and Subclasses were unaware of the facts alleged herein without any fault or lack of diligence on their part and could not have reasonably discovered Defendants' conduct. For this reason, any statute of limitations that otherwise may apply to the claims of Plaintiff or members of the Classes and Subclasses should be tolled.

III. ESTOPPEL

215. Despite their duties and obligations under COPPA and state common law, Defendants failed to provide notice of the collection and use of the Personal Information or obtain verifiable consent, in breach and violation thereof.

216. Defendants are therefore estopped from relying on any statutes of limitations in defense of this action.

CLASS ACTION ALLEGATIONS

217. Plaintiffs bring this action as a class action pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3).

218. All Plaintiffs, A.B., C.D.1, C.D.2, C.D.3, E.F.1, and E.F.2., by and through their parents and guardians, seek certification of a claim for violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*., on behalf of a class defined as follows:

> **Nationwide UCL Class**: all persons residing in the United States who were younger than the age of 13 when they used the Android Apps, and from whom Defendants collected, used, or disclosed Personal Information without first obtaining verified parental consent during the applicable statute of limitations period.

219. Plaintiff A.B., by and through his parent and guardian, seeks class certification of claims for the common law privacy cause of action for "Intrusion Upon Seclusion," on behalf of a class defined as follows:

> **The Intrusion Upon Seclusion Class**: all persons residing in the States of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia who were younger than the age of 13 when they used the Android Apps, and from whom Defendants collected, used, or disclosed Personal Information without first obtaining verified parental consent during the applicable statute of limitations period.

220. Plaintiff A.B., by and through his parent and guardian, seeks class certification of claims for violation of the State of California Constitution Right to Privacy and the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*., as well as a claim for Unjust Enrichment, on behalf of a California Subclass defined as follows:

> **The California Subclass**: all persons residing in the State of California who were younger than the age of 13 when they used the Android Apps, and from whom Defendants collected, used, or disclosed Personal Information without first obtaining verified parental consent during the applicable statute of limitations period.

221. Plaintiffs C.D.1, C.D.2, and C.D.3, by and through their parent and legal guardian, seek certification of a claim for violations of Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. § 501.201, *et seq*., as well as a claim for Unjust Enrichment, on behalf of a Florida Subclass defined as follows:

> **The Florida Subclass:** all persons residing in the State of Florida who were younger than the age of 13 when they used the Android Apps, and from whom Defendants collected, used, or disclosed Personal Information without first obtaining verified parental consent during the applicable statute of limitations period.

222. Plaintiffs E.F.1 and E.F.2, by and through their parent and legal guardian, seek certification of a claim for violations of NY Gen. Bus. Law § 349, as well as Unjust Enrichment, on behalf of a New York Subclass defined as follows:

> **The New York Subclass:** all persons residing in the State of New York who were younger than the age of 13 when they used the Android Apps, and from whom Defendants collected, used, or disclosed Personal Information without first obtaining verified parental consent during the applicable statute of limitations period.

223. Excluded from the Classes and Subclasses are: (a) any Judge or Magistrate Judge presiding over this action and members of their staff, as well as members of their families; (b) Defendants and Defendants' predecessors, parents, successors, heirs, assigns, subsidiaries, and any entity in which any Defendant or its parents have a controlling interest, as well as Defendants' current or former employees, agents, officers, and directors; (c) persons who properly execute and file a timely request for exclusion from the Classes or Subclasses; (d) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (e) counsel for Plaintiff and Defendants; and (f) the legal representatives, successors, and assigns of any such excluded persons.

224. **Ascertainability**. The proposed Classes and Subclasses are readily ascertainable because they are defined using objective criteria so as to allow class members to determine if they are part of a Class or Subclasses. Further, the Classes and Subclasses can be readily identified through records maintained by Defendants.

225. **Numerosity (Rule 23(a)(1))**. The Classes and Subclasses are so numerous that joinder of individual members herein is impracticable. The exact number of Classes or Subclass members, as herein identified and described, is not known, but App download and usage figures indicate that Defendants have collected information on millions of children (if not more).

226. **Commonality (Rule 23(a)(2))**. Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Classes and Subclasses members, including the following:

a. Whether Defendants collected the Personal Information of children under thirteen;

b. Whether Defendants had knowledge they were collecting the Personal Information of children under the age of thirteen;

c. Whether Defendants obtained verifiable parental consent to collect the Personal Information of children under the age of thirteen;

d. Whether the collection of Personal Information of children under the age of thirteen is highly offensive to a reasonable person;

e. Whether the collection of Personal Information of children under the age of thirteen without parental consent is sufficiently serious and unwarranted as to constitute an egregious breach of social norms;

f. Whether Defendants' conduct violated COPPA;

g. Whether Defendants' conduct constituted an invasion of privacy based on common law protection against intrusion upon seclusion;

h. Whether Defendants' conduct constitutes a violation of the State of California Constitution right to privacy;

i. Whether Defendants' conduct was unlawful, unfair, and/or deceptive;

j. Whether Defendants' conduct violated the California Unfair Competition Law;

k. Whether Defendants' conduct violated the Florida Deceptive and Unfair Trade Practices Act;

l. Whether Defendants' conduct violated New York General Business Law;

m. Whether Plaintiffs and the Classes and Subclasses are entitled to monetary damages and the measure of those damages;

n. Whether Plaintiffs and the Classes and Subclasses are entitled to restitution, disgorgement and/or other equitable and injunctive relief;

o. Whether Defendants were unjustly enriched by their conduct;

p. Whether Defendants' fraudulently concealed their conduct; and

q. Whether Plaintiffs and the Classes and Subclasses are entitled to injunctive or other equitable relief.

227. **Typicality (Rule 23(a)(3))**. Plaintiffs' claims are typical of the claims of the other members of the proposed Classes and Subclasses. Plaintiffs and members of the Classes and Subclasses suffered an invasion of privacy as a result of Defendants' wrongful conduct that is uniform across the Classes and Subclasses.

228. **Adequacy (Rule 23(a)(3))**. Plaintiffs have and will continue to fairly and adequately represent and protect the interests of the Classes and Subclasses. Plaintiffs have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interest that is antagonistic to those of the Classes and Subclasses, and Defendants have no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes and Subclasses, and they have the resources to do so. Neither Plaintiffs nor Plaintiffs' counsel has any interest adverse to those of the other members of the Classes and Subclasses.

229. **Substantial Benefits**. This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Classes and Subclasses is impracticable. The prosecution of separate actions by individual members of the Classes and Subclasses would impose heavy burdens upon the Courts and defendants, would create a risk of inconsistent or varying adjudications of the questions of law and fact common to members of the Classes and Subclasses, and would be dispositive of the interests of the other members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests. This proposed class action presents fewer management difficulties than individual litigation and provides the benefits of single adjudication,

economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

230. Plaintiffs reserve the right to revise the foregoing class allegations and definitions of the Classes and Subclasses based on new information learned and legal developments following additional investigation, discovery, or otherwise, and/or in order to accommodate any of the Court's manageability concerns.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code § 17200 ("UCL") (Brought on Behalf of All Plaintiffs and the Nationwide UCL Class, and on Behalf of Plaintiff A.B. and the California Subclass, Against All Defendants)

231. Plaintiffs incorporate the foregoing allegations and the allegations in the Second Claim for Relief and Fourth Claim for Relief as if fully set forth herein.

232. Defendants at all relevant times knowingly violated legal duties and public policy by collecting the Personal Information of children under 13 and tracking, profiling, and targeting those children with behavioral advertising for Defendants' financial gain. Defendants' conduct is unlawful, unfair, and/or deceptive under the UCL. Further, Defendants' conduct, which affected members of the UCL Class and the California Subclass, occurred in and emanated from California, where Defendants are headquartered.

233. As outlined herein, Defendants at all times had actual knowledge that the Android Apps were not compliant with the guidelines and requirements in Google's DFF program, which mandated adherence to COPPA and other applicable privacy-related laws. Further, Defendants at all times had actual knowledge and specifically intended that the AdMob SDKs embedded in the Android Apps enabled and effectuated the exfiltration of Personal Information from Plaintiffs and children under 13

using the Android Apps and the tracking, profiling, and targeting of those children for lucrative behavioral advertising.

234. In addition, as outlined herein, Google broadly promoted, marketed, and represented in numerous ways that the DFF program and the Apps included in the program were suitable and safe and designed for children and legally compliant, including in public-facing websites, privacy policies and program requirements, marketing materials, App interfaces, and other public statements and materials, and internally acknowledged and advised its App developer partners the same. For example:

> The DFF program had a "strict legal and policy bar," requiring that Apps displaying ads "comply with all legal obligations relating to advertising to children," "Ads displayed to child audiences do not involve interest-based advertising," Apps submitted to the DFF program were "compliant with COPPA and other relevant statutes," and that "Ads displayed to child audiences must comply with laws relating to advertising to kids," and the App "must disable interest-based advertising;"
>
> Google warned that non-compliance with DFF guidelines and requirements could result in expulsion of the App from the DFF program;
>
> Google stated that DFF was designed to be "inclusive of apps that are made for kids," and that "apps that have no specific benefit or relevance for audiences under the age of thirteen will not be accepted into the program;"
>
> Google stated that "Apps that meet the [DFF] program requirements will be featured through Google Play's family-friendly browse and search experiences so that parents can find suitable, trusted, high-quality apps and games more easily."
>
> Google sated that the DFF program "helps parents easily find your family-friendly apps and games" and "create[s] a trusted environment that empowers parents to make informed decisions and engage with [App developer] content."
>
> The DFF program provided privileges to DFF Apps/games that opted in to DFF, touting that only those Apps/games "[would] show up in searches initiated from the family section in Apps Home," and be "more visible" when "users search for family or kids related content from anywhere in the [Google] Play store."
>
> The DFF program implemented a "Family star button on Apps and Games Home point[ed] to an enhanced discovery experience for parents looking for family appropriate content," and "Apps participating in [DFF] are marked with the family star badge, which reflects the target age you select for your apps and serves as a signal of quality for parents."

235. In addition, the Android Apps were child-directed as defined under COPPA. Given the inherent characteristics, content, and features of the Android Apps offered and available in the DFF program in the Google Play Store, including the names, designs, cartoon elements, and children's themes and songs, were plainly intended for and meant to attract children and, in particular, children under 13, through which Defendants intended to and did collect Personal Information to serve these children behavioral advertising for substantial commercial gain. And, in fact, Defendants, "operators" as defined under COPPA and FTC regulations, collected Personal Information from children under 13 through the Android Apps, which were directed to children.

236. In particular, Defendants systematically collected, used, and/or disclosed Personal Information from children under 13 in violation of COPPA to serve them targeted, behavioral advertising by *inter alia*:

a. Failing to provide sufficient notice of the information Defendants collected, or the information that was collected on Defendants' behalf, online from children under 13, how Defendants used 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 collected, or the information that was collected on Defendants' behalf, online from children under 13, how Defendants used 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 under 13, in violation of Section 312.5 of COPPA, 16 C.F.R. § 312.5; and

c. Failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of Personal Information collected from children under 13, in violation of Section 312.8 of COPPA, 16 C.F.R. § 312.8.

237. Violations of COPPA and the accompanying FTC regulations "shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under 15 U.S.C. § 57a(a)(1)(B)." 15 U.S.C. § 6502(c). These rules define unfair or deceptive acts or practices in or

affecting commerce within the meaning of 15 U.S.C. § 45(a)(1), which is the model for the various consumer protection statutes in the several states, including the UCL.[57]

238. Accordingly, Defendants engaged in business acts and practices deemed "unlawful" under the UCL predicated on their violations of COPPA and the FTC regulations. For the same reasons and based on Defendants' unlawful tracking, targeting, and profiling of Plaintiffs and UCL Class and California Subclass Members without obtaining parental consent, defendants engaged in business acts and practices deemed "unlawful" in violation of state common laws protecting invasion of privacy and prohibiting intrusion upon seclusion and the California Constitutional Right to Privacy, Cal. Const. Art. 1, § 1.

239. Defendants also engaged in business acts or practices deemed "unfair" under the UCL, because, as outlined herein, Defendants failed to disclose that they were tracking, profiling, and targeting children, including Plaintiffs and UCL Class and California Subclass Members, through the collection of Personal Information, and that they were profiting from this conduct through behavioral (interest-based) advertising. Unfair acts under the UCL have been interpreted using three different tests: (1) whether the public policy which is a predicate to a consumer unfair competition action under the unfair prong of the UCL is tethered to specific constitutional, statutory, or regulatory provisions; (2) whether the gravity of the harm to the consumer caused by the challenged business practice outweighs the utility of the defendant's conduct; and (3) whether the consumer injury is substantial, not outweighed by any countervailing benefits to consumers or competition, and is an injury that consumers themselves could not reasonably have avoided.

240. Defendants' conduct is unfair under each of these tests. As outlined herein, Defendants' conduct violates COPPA and FTC regulations and the policies underlying privacy laws. The gravity of

[57] See 16 C.F.R. § 312.1 (COPPA "prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure or personal information from and about children on the internet.").

the harm of Defendants' secret tracking, profiling, and targeting of children is significant and there is no corresponding benefit to consumers or competition from Defendants' conduct. Finally, because Plaintiffs and UCL Class and California Subclass Members were minors unable to consent to or understand Defendants' conduct—and because their parents and guardians did not consent to this conduct and were misled by their belief that Defendants would follow applicable laws and societal expectations about children's privacy as well as Defendants' statements, policies, and promotion —they could not have avoided the harm.

241. The parents and guardians of Plaintiffs and the members of the UCL Class and California Subclass reasonably expected that Defendants would respect children's privacy online, in accordance with their own policies and guidelines, statements, and representations, societal expectations and public policy, as well as state and federal statutes and regulations including COPPA and Federal Trade Commission regulations. As outlined herein, the Android App games are marketed, promoted, and represented as safe and suitable for children, predicated on, *inter alia*, (i) their offering and availability and promotion and marketing in the DFF program in the Family section of the Google Play Store and the representations and statements concerning the DFF program and the Family section of the Google Play Store, (ii) the public statements marketing and promoting the games as suitable and appropriate for children by the Android App developers, and (iii) the inherent characteristics, content, and features of Android App games, which were designed for children.

242. At the same time, Defendants have (i) at all relevant times known that children under the age of 13 use the Android Apps, (ii) actively sought to increase use of the Apps by these children, and (iii) sought to exploit, for commercial purposes and gain, the millions of children under the age of 13 using the Android Apps. Defendants' knowledge of the widespread use of the Apps by children (which Defendants have expressly touted in their advertising sales efforts) and their concealment and failure to disclose the exfiltration of Personal Information from such children and that they were tracking,

profiling, and targeting these children and/or profiting from this conduct through lucrative behavioral advertising, while promoting, representing, and purporting to ensure that the Android Apps comply with law and societal expectation, are likely to and, in fact, did deceive Plaintiffs and members of the UCL Class and California Subclass and their parents or guardians. Defendants' conduct therefore constitutes deceptive business practices in violation of the UCL.

243. Defendants' misrepresentations and omissions were explicit and implicit. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers such as the parents or guardians of Plaintiffs and UCL Class and California Subclass Members about the terms under which their children were using the Apps as well as the fact that Defendants were collecting and profiting from the Personal Information of children under the age of thirteen without their parents and guardians' knowledge or consent.

244. Defendants had a duty to disclose the above-described facts due to the important public interest in securing the privacy of young children's Personal Information and the fact that young children are unable to fully protect their own interests. Parents and guardians of Plaintiffs and UCL Class and California Subclass Members placed trust in Defendants as reputable companies which represent that they comply with applicable laws and societal interests in safeguarding children's Personal Information. Additionally, Defendants exclusively knew and understood the extent of their collection of Personal Information, and the parents or guardians of Plaintiffs and UCL Class and Subclass Members could not reasonably have discovered—and were unaware of—Defendants' secret tracking, profiling, and targeting.

245. Defendants invaded Plaintiff's and UCL Class and California Subclass Members' privacy without their or their parents and guardians' consent.

246. Because Defendants held themselves out as complying with law and public policy regarding children's privacy rights, the parents or guardians of Plaintiffs and UCL Class and California Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions.

247. Defendants' conduct is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, and there are no greater countervailing benefits to consumers or competition. Further, Plaintiffs and UCL Class and California Subclass Members could not have reasonably avoided injury because Defendants took advantage of the lack of knowledge, ability, experience, and/or capacity of consumers to their detriment.

248. Plaintiffs, and UCL Cass and California Subclass Members, were harmed by Defendants' violations of Cal. Bus. & Prof. Code §17200. Defendants' practices were a substantial factor and caused injury in fact and actual damages to Plaintiffs and UCL Class and California Subclass Members. As a direct and proximate result of Defendants' deceptive acts and practices, and unlawful and unfair conduct in violation of Cal. Bus. & Prof. Code §17200, Plaintiffs and UCL Class and California Subclass Members have suffered and will continue to suffer an ascertainable loss of money or property, real or personal, and monetary and non-monetary damages, as described herein, including the loss of the value or diminishment in value of their Personal Information and the loss of the ability to control the use of their Personal Information, which allowed Defendants to profit at the expense of Plaintiffs and UCL Class and California Subclass Members.

249. As outlined herein, there is tangible value in Plaintiffs' and UCL Class and California Subclass Members' Personal Information has tangible value. Plaintiffs' and UCL Class and California Subclass Members have lost the opportunity to receive value in exchange for their Personal Information.

250. Defendants' monetization of the Plaintiffs' and UCL Class and California Subclass Members' Personal Information demonstrates that there is a market for their Personal Information.

251. Plaintiffs' and UCL Class and California Subclass Members' Personal Information is now in the possession of Defendants, who have used and will use it for their financial gain.

252. Plaintiffs' and the UCL Class and California Subclass Members' injury was the direct and proximate result of Defendants' conduct described herein. The Defendants' retention of UCL Class and California Subclass Members' Personal Information presents a continuing risk to them as well as the general public.

253. Plaintiffs, individually and on behalf of the UCL Class and California Subclass, seek: (1) an injunction requiring Defendants to permanently delete, destroy or otherwise sequester the Personal Information collected without parental consent, requiring Defendants to provide a complete audit and accounting of the uses of the Personal Information by Defendants, App developers and any other third parties, and other appropriate injunctive relief; (2) compensatory restitution of Plaintiffs' and the UCL Class and California Subclass Members' money and property lost as a result of Defendants' acts of unfair competition; (3) disgorgement of Defendants' profits and unjust gains; and (4) reasonable attorney's fees (pursuant to Cal. Code of Civ. Proc. § 1021.5).

SECOND CLAIM FOR RELIEF

INTRUSION UPON SECLUSION
(Brought on Behalf of Plaintiff A.B. and the Intrusion Upon Seclusion Class Against All Defendants)

254. Plaintiff A.B. incorporates the foregoing allegations as if fully set forth herein.

255. Plaintiff A.B.'s and the Intrusion Upon Seclusion Class members' private affairs include their behavior on their mobile devices, online, as well as any other behavior that may be monitored by the surreptitious and deceptive tracking employed or otherwise enabled by or through the Android Apps.

256. The parents and guardians of Plaintiff A.B. and members of the Intrusion Upon Seclusion Class have reasonable expectations of privacy in their mobile devices and their online behavior, generally. As outlined herein, these expectations stemmed from Google's policies and

guidelines, statements, and representations, societal expectations, and public policy, as well as state and federal statutes and regulations including COPPA and Federal Trade Commission regulations. Further, these expectations stemmed from the fact that the Android App games are marketed, promoted, and represented as safe and suitable for children, predicated on, *inter alia*, (i) their offering and availability and promotion and marketing in the DFF program in the Family section of the Google Play Store and the representations and statements concerning the DFF program and the Family section of the Google Play Store, (ii) the public statements marketing and promoting the games as suitable and appropriate for children by the Android App developers, and (iii) the inherent characteristics, content, and features of Android App games, which were designed for children. The expectations of the parents and guardians of Plaintiff A.B. and members of the Intrusion Upon Seclusion Class includes that the Defendants would not track their children's activity across the Internet and exfiltrate their Personal Information, without consent, in order for the Defendants to earn substantial profits through targeted behavioral advertising.

257. As children under the age of 13, Plaintiff A.B. and the members of the Intrusion Upon Seclusion Class lacked the ability to form expectations about reasonable privacy or to consent to Defendants' actions.

258. Defendants intentionally intruded on and into Plaintiff A.B.'s and the Intrusion Upon Seclusion Class members' solitude, seclusion, or private affairs by intentionally and surreptitiously obtaining, improperly gaining knowledge of, reviewing, and/or retaining Plaintiff A.B.'s and the Intrusion Upon Seclusion Class members' activities (and Personal Information) through the collection, monitoring, and tracking activities described herein.

259. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, countless consumer surveys, studies, and op-eds decrying the online tracking of children, centuries of common law, state and federal statutes and regulations including COPPA and FTC regulations,

legislative commentaries, enforcement actions undertaken by the FTC, industry standards and guidelines, and scholarly literature on consumers' reasonable expectations.

260. These societal expectations and laws created a duty that Defendants owed to Plaintiff A.B. and the members of the Intrusion Upon Seclusion Class. Defendants breached that duty by tracking and monitoring children and profiting from the behavioral advertising served to them.

261. Defendants' intrusion into the sacrosanct relationship between parent and child and subsequent commercial exploitation of children's special vulnerabilities online also contributes to the highly offensive nature of Defendants' activities.

262. Plaintiff A.B. and the members of the Intrusion Upon Seclusion Class were harmed by the intrusion into their private affairs as outlined in detail in this Complaint. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff A.B. and members of the Intrusion Upon Seclusion Class.

263. Plaintiff A.B. and members of the Intrusion Upon Seclusion Class therefore seek (1) an injunction requiring Defendants to permanently delete, destroy or otherwise sequester the Personal Information collected without parental consent, requiring Defendants to provide a complete audit and accounting of the uses of the Personal Information by Defendants, App developers and any other third parties, and other appropriate injunctive relief; and (2) compensatory and punitive damages in an amount to be determined at trial. Plaintiff A.B. and Intrusion Upon Seclusion Class members seek punitive damages because Defendants' actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff A.B. and Intrusion Upon Seclusion Class members and made in conscious disregard of Plaintiff A.B.'s and Intrusion Upon Seclusion Class members' rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

THIRD CLAIM FOR RELIEF

CALIFORNIA UNJUST ENRICHMENT

(Brought on behalf of Plaintiff A.B. and the California Subclass against all Defendants)

264. Plaintiff A.B. incorporates the foregoing allegations as if fully set forth herein.

265. By virtue of the unlawful, unfair, and deceptive conduct alleged herein, Defendants knowingly realized hundreds of millions of dollars in revenue from the use and/or sale of Personal Information of Plaintiff A.B. and the California Subclass members for advertising and commercialization purposes.

266. This Personal Information, the value of the Personal Information, and/or the attendant revenue from the use and profit by Defendants, were monetary benefits conferred upon Defendants by Plaintiff A.B. and the California Subclass members.

267. As a result of Defendants' conduct, Plaintiff A.B. and the California Subclass members suffered actual damages based on the loss of the value of their Personal Information and the lost profits from the use of the Personal information.

268. It would be inequitable and unjust to permit Defendants to retain the substantial economic benefits (financial and otherwise) they obtained from and/or at the expense of Plaintiff A.B. and the California Subclass members.

269. Defendants will be unjustly enriched if they are permitted to retain the economic benefits conferred upon them by Plaintiff A.B. and the California Subclass members through Defendants obtaining Plaintiff A.B.'s and the California Subclass members' Personal Information and the value thereof, and profiting from the unlawful, unauthorized, and impermissible use of the Personal Information of Plaintiff A.B. and the California Subclass members.

270. Plaintiff A.B. and the California Subclass members are therefore entitled to recover the amounts realized by Defendants at their expense.

271. Plaintiff A.B. and the California Subclass members have no adequate remedy at law.

272. Plaintiff A.B. and the California Subclass members are entitled to restitution, disgorgement, and/or the imposition of a constructive trust to recover the amount of Defendants' ill-gotten gains, and/or other sums as may be just and equitable.

FOURTH CLAIM FOR RELIEF

CALIFORNIA CONSTITUTIONAL RIGHT TO PRIVACY, CAL. CONST. ART.1, § 1.

(Brought on behalf of Plaintiff A.B. and the California Subclass against all Defendants)

273. Plaintiff A.B. incorporates the foregoing allegations as if fully set forth herein.

274. Plaintiff A.B.'s and the California Subclass Members' private affairs include their behavior on their mobile devices and computers, as well as any other online behavior that may be monitored by the surreptitious tracking employed or otherwise enabled by Defendants.

275. The parents and guardians of Plaintiff A.B. and the California Subclass Members have reasonable expectations of privacy in their children's mobile devices and their online behavior and activities, generally. As outlined herein, these expectations stemmed from Google's policies and guidelines, statements, and representations, societal expectations, and public policy, as well as state and federal statutes and regulations including COPPA and Federal Trade Commission regulations. Further, these expectations stemmed from the fact that the Android App games are marketed, promoted, and represented as safe and suitable for children, predicated on, *inter alia*, (i) their offering and availability and promotion and marketing in the DFF program in the Family section of the Google Play Store and the representations and statements concerning the DFF program and the Family section of the Google Play Store, (ii) the public statements marketing and promoting the games as suitable and appropriate for children by the Android App developers, and (iii) the inherent characteristics, content, and features of Android App games, which were designed for children. The expectations of the parents and guardians of Plaintiff A.B. and members of the Intrusion Upon Seclusion Class includes that the Defendants would

not track their children's activity across the Internet and exfiltrate their Personal Information, without consent, in order for the Defendants to earn substantial profits through targeted behavioral advertising.

276. As minor children, Plaintiff A.B. and California Subclass Members lack the ability to form expectations about reasonable privacy or to consent to Defendants' actions. Plaintiff A.B. and California Subclass Members rely on their parents for such determinations.

277. Defendants intentionally intruded on and into Plaintiff A.B.'s and the California Subclass Members' solitude, seclusion, or private affairs by intentionally and surreptitiously obtaining, improperly gaining knowledge of, reviewing, and/or retaining Plaintiff A.B.'s and the California Subclass Members' activities through the monitoring and tracking activities described herein.

278. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, countless consumer surveys, studies, and op-eds decrying the online tracking of children, centuries of common law, state and federal statutes and regulations, legislative commentaries, enforcement actions undertaken by the FTC, industry standards and guidelines, and scholarly literature on consumers' reasonable expectations.

279. These societal expectations and laws created a duty that Defendants owed to Plaintiff A.B. and California Subclass Members. Defendants breached that duty by tracking and monitoring children, and Defendants breached that duty by profiting from the behavioral advertising served to them.

280. Defendants' intrusion into the sacrosanct relationship between parent and child and subsequent commercial exploitation of children's special vulnerabilities online also contributes to the highly offensive nature of Defendants' activities.

281. Defendants' conduct as aforesaid violated Plaintiff A.B.'s and the California Subclass Members' right to privacy, as guaranteed by ART. 1, § 1 of the California Constitution.

282. Plaintiff A.B. and the California Subclass Members were harmed by the intrusion into their private affairs as outlined in detail in this Complaint. Defendants' actions and conduct complained

of herein were a substantial factor in causing the harm suffered by Plaintiff A.B. and the California Subclass Members.

283. Plaintiff A.B. and members of the California Subclass therefore seek (1) an injunction requiring Defendants to permanently delete, destroy or otherwise sequester the Personal Information collected without parental consent, requiring Defendants to provide a complete audit and accounting of the uses of the Personal Information by Defendants, App developers and any other third parties, and other appropriate injunctive relief; and (2) compensatory and punitive damages in an amount to be determined at trial. Plaintiff A.B. and the California Subclass members seek punitive damages because Defendants' actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff A.B. and California Subclass members and made in conscious disregard of the rights of Plaintiff A.B. and California Subclass members. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

FIFTH CLAIM FOR RELIEF

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Fla. Stat. § 501.201, *et seq.*
(Brought on behalf of Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass against all Defendants)

284. Plaintiffs C.D.1, C.D.2, and C.D.3 incorporate the foregoing allegations as if fully set forth herein.

285. Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass Members are or were residents of Florida and/or used the Apps in Florida.

286. Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass Members are "consumers," as defined by Fla. Stat. § 501.203(7) and the conduct at issue was within "trade or commerce" as defined by Fla. Stat. § 501.203(8), in that Defendants advertised, offered for sale, sold or distributed goods or services, or any property whether tangible or intangible, or any other article, commodity or

thing of value, in Florida and/or engaged in trade or commerce directly or indirectly affecting the people of Florida..

287. FDUTPA, Fla. Stat. § 501.204 provides that "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."

288. Defendants at all relevant times knowingly violated legal duties and public policy by collecting the Personal Information of children under 13 and tracking, profiling, and targeting those children with behavioral advertising for Defendants' financial gain. As outlined herein, Defendants at all times had actual knowledge that the Android Apps were not compliant with the guidelines and requirements in Google's DFF program, which mandated adherence to COPPA and other applicable privacy-related laws. Further, Defendants at all times had actual knowledge and specifically intended that the AdMob SDKs embedded in the Android Apps enabled and effectuated the exfiltration of Personal Information from Plaintiffs and children under 13 using the Android Apps and the tracking, profiling, and targeting of those children for lucrative behavioral advertising.

289. As outlined herein, Google broadly promoted, marketed, and represented in numerous ways that the DFF program and the Apps included in the program as suitable and safe and designed for children and legally compliant, including in public-facing websites, privacy policies and program requirements, marketing materials, App interfaces, and other public statements and materials, and internally acknowledged and advised its App developer partners the same. For example:

> The DFF program had a "strict legal and policy bar," requiring that Apps displaying ads "comply with all legal obligations relating to advertising to children," "Ads displayed to child audiences do not involve interest-based advertising," Apps submitted to the DFF program were "compliant with COPPA and other relevant statutes," and that "Ads displayed to child audiences must comply with laws relating to advertising to kids," and the App "must disable interest-based advertising;"
>
> Google warned that non-compliance with DFF guidelines and requirements could result in expulsion of the App from the DFF program;

> Google stated that DFF was designed to be "inclusive of apps that are made for kids," and that "apps that have no specific benefit or relevance for audiences under the age of thirteen will not be accepted into the program;"
>
> Google stated that "Apps that meet the [DFF] program requirements will be featured through Google Play's family-friendly browse and search experiences so that parents can find suitable, trusted, high-quality apps and games more easily."
>
> Google sated that the DFF program "helps parents easily find your family-friendly apps and games" and "create[s] a trusted environment that empowers parents to make informed decisions and engage with [App developer] content."
>
> The DFF program provided privileges to DFF Apps/games that opted in to DFF, touting that only those Apps/games "[would] show up in searches initiated from the family section in Apps Home," and be "more visible" when "users search for family or kids related content from anywhere in the [Google] Play store."
>
> The DFF program implemented a "Family star button on Apps and Games Home point[ed] to an enhanced discovery experience for parents looking for family appropriate content," and "Apps participating in [DFF] are marked with the family star badge, which reflects the target age you select for your apps and serves as a signal of quality for parents."

290. In addition, the inherent characteristics, content, and features of the Android Apps offered and available in the DFF program in the Google Play Store, including the names, designs, cartoon elements, and children's themes and songs, were plainly intended for and meant to attract children and, in particular, children under 13, through which Defendants intended to and did collect Personal Information to serve these children behavioral advertising for substantial commercial gain.

291. In addition, the Android Apps were child-directed as defined under COPPA. Given the inherent characteristics, content, and features of the Android Apps offered and available in the DFF program in the Google Play Store, including the names, designs, cartoon elements, and children's themes and songs, were plainly intended for and meant to attract children and, in particular, children under 13, through which Defendants intended to and did collect Personal Information to serve these children behavioral advertising for substantial commercial gain. And, in fact, Defendants, "operators" as defined under COPPA and FTC regulations, collected Personal Information from children under 13 through the Android Apps, which were directed to children.

292. In particular, Defendants systematically collected, used, and/or disclosed Personal Information from children under 13 in violation of COPPA to serve them targeted, behavioral advertising by *inter alia*:

a. Failing to provide sufficient notice of the information Defendants collected, or the information that was collected on Defendants' behalf, online from children under 13, how Defendants used 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 collected, or the information that was collected on Defendants' behalf, online from children under 13, how Defendants used 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 under 13, 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 under 13, in violation of Section 312.8 of COPPA, 16 C.F.R. § 312.8.

293. Violations of COPPA and the accompanying FTC regulations "shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under 15 U.S.C. § 57a(a)(1)(B)." 15 U.S.C. § 6502(c). These rules define unfair or deceptive acts or practices in or affecting commerce within the meaning of 15 U.S.C. § 45(a)(1), which is the model for the various consumer protection statutes in the several states, including the FDUTPA.[58]

294. In addition, Fla. Stat. § 501.204 provides that "[i]t is the intent of the Legislature that, in construing subsection (1), due consideration and great weight shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to s. 5(a)(1) of the Federal Trade Commission Act, 15 U.S.C. s. 45(a)(1) as of July 1, 2017.

[58] See 16 C.F.R. § 312.1 (COPPA "prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure or personal information from and about children on the internet.").

295. Accordingly, Defendants have engaged in unfair or deceptive acts or practices in violation of Fla. Stat. § 501.201 *et seq*.

296. Defendants additionally made material misrepresentations and omissions regarding the invasions of privacy and unlawful conduct and practices outlined herein that constituted unfair or deceptive acts or practices in violation of Fla. Stat. § 501.201 *et seq*.

297. Parents and guardians of Plaintiffs C.D.1, C.D.2, and C.D.3 and the members of the Florida Subclass reasonably expected that Defendants would respect children's privacy online, in accordance with their own policies and guidelines, statements, and representations, societal expectations and public policy, as well as state and federal statutes and regulations including COPPA and Federal Trade Commission regulations. As outlined herein, the Android App games are marketed, promoted, and represented as safe and suitable for children, predicated on, *inter alia*, (i) their offering and availability and promotion and marketing in the DFF program in the Family section of the Google Play Store and the representations and statements concerning the DFF program and the Family section of the Google Play Store, (ii) the public statements marketing and promoting the games as suitable and appropriate for children by the Android App developers, and (iii) the inherent characteristics, content, and features of Android App games, which were designed for children.

298. At the same time, Defendants have (i) at all relevant times known that children under the age of 13 use the Android Apps, (ii) actively sought to increase use of the Apps by these children, and (iii) sought to exploit, for commercial purposes and gain, the millions of children under the age of 13 using the Android Apps. Defendants' knowledge of the widespread use of the Apps by children (which Defendants have expressly touted in their advertising sales efforts) and their concealment and failure to disclose the exfiltration of Personal Information from such children and they were tracking, profiling, and targeting these children and/or profiting from this conduct through lucrative behavioral advertising, while at the same time promoting, representing, and purporting to ensure that the Android Apps comply

with law and societal expectation, are likely to and, in fact, did deceive Plaintiffs C.D.1, C.D.2, and C.D.3 and members of the Florida Subclass and their parents or guardians.

299. Defendants' misrepresentations and omissions were explicit and implicit. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers such as the parents or guardians of Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass Members about the terms under which their children were using the Apps as well as the fact that Defendants were collecting and profiting from the Personal Information of children under the age of thirteen without their parents and guardians' knowledge or consent.

300. Defendants had a duty to disclose the above-described facts due to the important public interest in securing the privacy of young children's Personal Information and the fact that young children are unable to fully protect their own interests. Parents and guardians of Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass Members placed trust in Defendants as reputable companies, which represent that they comply with applicable laws and societal interests in safeguarding children's Personal Information. Additionally, Defendants exclusively knew and understood the extent of their collection of Personal Information, and the parents or guardians of Plaintiffs C.D.1, C.D.2, and C.D.3 and Florida Subclass Members could not reasonably have discovered—and were unaware of—Defendants' secret tracking, profiling, and targeting.

301. Defendants' conduct is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, and there are no greater countervailing benefits to consumers or competition. Further, Plaintiffs and Florida Subclass Members could not have reasonably avoided injury because Defendants took advantage of the lack of knowledge, ability, experience, and/or capacity of consumers to their detriment.

302. Defendants willfully engaged in the deceptive, misleading, and unlawful acts described herein and knew or recklessly disregarded the fact that they violated Fla. Stat. § 501.201, *et seq*.

303. Plaintiffs C.D.1, C.D.2, and C.D.3 and Florida Subclass Members were harmed by Defendants' practices, which were a substantial factor and caused injury in fact and actual damages to Plaintiffs C.D.1, C.D.2, and C.D.3 and Florida Subclass Members. As a direct and proximate result of Defendants' unlawful, unfair, and deceptive acts and practices in violation of Fla. Stat. § 501.201, *et seq*., Plaintiffs and Florida Subclass Members have suffered and will continue to suffer an ascertainable loss of money or property, real or personal, and monetary and non-monetary damages, as described herein, including the loss of the value or diminishment in value of their Personal Information and the loss of the ability to control the use of their Personal Information, which allowed Defendants to profit at the expense of Plaintiffs C.D.1, C.D.2, and C.D.3 and Florida Subclass Members.

304. As outlined herein, there is tangible value in Plaintiffs C.D.1, C.D.2, and C.D.3' s and Florida Subclass Members' Personal Information has tangible value. Plaintiffs C.D.1, C.D.2, and C.D.3 and Florida Subclass Members have lost the opportunity to receive value in exchange for their Personal Information.

305. Defendants' monetization of Plaintiffs C.D.1, C.D.2, and C.D.3's and Florida Subclass Members' Personal Information demonstrates that there is a market for their Personal Information.

306. Plaintiffs C.D.1, C.D.2, and C.D.3's and Florida Subclass Members' Personal Information is now in the possession of Defendants, who have used and will use it for their financial gain.

307. Defendants' retention of Plaintiffs C.D.1, C.D.2, and C.D.3's and Florida Subclass Members' Personal Information presents a continuing risk to them as well as the general public.

308. Florida Plaintiffs and Florida Subclass Members seek relief for the injuries they have suffered as a result of Defendants' unconscionable, unfair, and deceptive acts and practices, as provided by Fla. Stat. § 501.211 and applicable law, including all actual damages and attorneys' fees, as well as an injunction requiring Defendants to permanently delete, destroy or otherwise sequester the Personal

Information collected without parental consent, requiring Defendants to provide a complete audit and accounting of the uses of the Personal Information by Defendants, App developers and any other third parties, and other appropriate injunctive and/or declaratory relief.

SIXTH CLAIM FOR RELIEF

FLORIDA UNJUST ENRICHMENT
(On Behalf of the Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclasses)

309. Plaintiffs C.D.1, C.D.2, and C.D.3 incorporate the foregoing allegations as if fully set forth herein.

310. By virtue of the unlawful, unfair, and deceptive conduct alleged herein, Defendants knowingly realized hundreds of millions of dollars in revenue from the use and/or sale of Personal Information of Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass members for advertising and commercialization purposes.

311. This Personal Information, the value of the Personal Information, and/or the attendant revenue from the use and profit by Defendants, were monetary benefits conferred upon Defendants by Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass members.

312. As a result of Defendants' conduct, Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass members suffered actual damages based on the loss of the value of their Personal Information and the lost profits from the use of the Personal information.

313. It would be inequitable and unjust to permit Defendants to retain the substantial economic benefits (financial and otherwise) they obtained from and/or at the expense of Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass.

314. Defendants will be unjustly enriched if they are permitted to retain the economic benefits conferred upon them by Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass members through Defendants obtaining Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass members' Personal

Information and the value thereof, and profiting from the unlawful, unauthorized, and impermissible use of the Personal Information of Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass members.

315. Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass members are therefore entitled to recover the amounts realized by Defendants at their expense.

316. Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass members are entitled to restitution, disgorgement, and/or the imposition of a constructive trust to recover the amount of Defendants' ill-gotten gains, and/or other sums as may be just and equitable.

SEVENTH CLAIM FOR RELIEF

NEW YORK CONSUMER PROTECTION LAW
N.Y. Gen. Bus. Law § 349 *et seq*.
(Brought on behalf of Plaintiffs E.F.1 and E.F.2 and the New York Subclass against All Defendants)

317. Plaintiffs E.F.1 and E.F.2 incorporate the foregoing allegations as if fully set forth herein.

318. Plaintiffs E.F.1 and E.F.2 and New York Subclass Members are or were residents of New York and/or used the Apps in New York.

319. At all times mentioned herein, Defendants engaged in "trade" or "commerce" in New York in that they engaged in the advertising, offering for sale, sale, and distribution of property or any other articles, commodities, or things of value in New York.

320. Defendants engaged in consumer-oriented acts through the offering, promoting, and/or distributing of the Apps and supporting hardware and software, which significantly impacted the public because the Android Apps are used nationwide, including in New York, and there are millions of users, including Plaintiffs E.F.1 and E.F.2 and New York Subclass Members.

321. N.Y. Gen. Bus. Law § 349(a) provides "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

322. Defendants violated N.Y. Gen. Bus. Law § 349 by engaging in the deceptive or unfair acts or practices proscribed by N.Y. Gen. Bus. Law § 349 outlined herein.

323. Defendants at all relevant times knowingly violated legal duties and public policy by collecting the Personal Information of children under 13 and tracking, profiling, and targeting those children with behavioral advertising for Defendants' financial gain. As outlined herein, Defendants at all times had actual knowledge that the Android Apps were not compliant with the guidelines and requirements in Google's DFF program, which mandated adherence to COPPA and other applicable privacy-related laws. Further, Defendants at all times had actual knowledge and specifically intended that the AdMob SDKs embedded in the Android Apps enabled and effectuated the exfiltration of Personal Information from Plaintiffs and children under 13 using the Android Apps and the tracking, profiling, and targeting of those children for lucrative behavioral advertising.

324. As outlined herein, Google broadly promoted, marketed, and represented in numerous ways that the DFF program and the Apps included in the program as suitable and safe and designed for children and legally compliant, including in public-facing websites, privacy policies and program requirements, marketing materials, App interfaces, and other public statements and materials, and internally acknowledged and advised its App developer partners the same. For example:

> The DFF program had a "strict legal and policy bar," requiring that Apps displaying ads "comply with all legal obligations relating to advertising to children," "Ads displayed to child audiences do not involve interest-based advertising," Apps submitted to the DFF program were "compliant with COPPA and other relevant statutes," and that "Ads displayed to child audiences must comply with laws relating to advertising to kids," and the App "must disable interest-based advertising;"
>
> Google warned that non-compliance with DFF guidelines and requirements could result in expulsion of the App from the DFF program;
>
> Google stated that DFF was designed to be "inclusive of apps that are made for kids," and that "apps that have no specific benefit or relevance for audiences under the age of thirteen will not be accepted into the program;"

> Google stated that "Apps that meet the [DFF] program requirements will be featured through Google Play's family-friendly browse and search experiences so that parents can find suitable, trusted, high-quality apps and games more easily."
>
> Google sated that the DFF program "helps parents easily find your family-friendly apps and games" and "create[s] a trusted environment that empowers parents to make informed decisions and engage with [App developer] content."
>
> The DFF program provided privileges to DFF Apps/games that opted in to DFF, touting that only those Apps/games "[would] show up in searches initiated from the family section in Apps Home," and be "more visible" when "users search for family or kids related content from anywhere in the [Google] Play store."
>
> The DFF program implemented a "Family star button on Apps and Games Home point[ed] to an enhanced discovery experience for parents looking for family appropriate content," and "Apps participating in [DFF] are marked with the family star badge, which reflects the target age you select for your apps and serves as a signal of quality for parents."

325. In addition, the inherent characteristics, content, and features of the Android Apps offered and available in the DFF program in the Google Play Store, including the names, designs, cartoon elements, and children's themes and songs, were plainly intended for and meant to attract children and, in particular, children under 13, through which Defendants intended to and did collect Personal Information to serve these children behavioral advertising for substantial commercial gain. And, in fact, Defendants, "operators" as defined under COPPA and FTC regulations, collected Personal Information from children under 13 through the Android Apps, which were directed to children.

326. In particular, Defendants systematically collected, used, and/or disclosed Personal Information from children under 13 in violation of COPPA to serve them targeted, behavioral advertising by *inter alia*:

a. Failing to provide sufficient notice of the information Defendants collected, or the information that was collected on Defendants' behalf, online from children under 13, how Defendants used 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 collected, or the information that was collected on Defendants' behalf, online from children under 13, how Defendants used 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 under 13, 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 under 13, in violation of Section 312.8 of COPPA, 16 C.F.R. § 312.8.

327. Violations of COPPA and the accompanying FTC regulations "shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under 15 U.S.C. § 57a(a)(1)(B)." 15 U.S.C. § 6502(c). These rules define unfair or deceptive acts or practices in or affecting commerce within the meaning of 15 U.S.C. § 45(a)(1), which is the model for the various consumer protection statutes in the several states, including the GBL.[59]

328. Accordingly, Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in violation of NY GBL § 349.

329. Defendants additionally made material misrepresentations and omissions regarding the invasions of privacy and unlawful conduct and practices outlined herein that constituted deceptive, unfair, and unlawful trade acts or practices in violation of NY GBL § 349.

330. Parents and guardians of Plaintiffs E.F.1 and E.F.2 and the members of the New York Subclass reasonably expected that Defendants would respect children's privacy online, in accordance with their own policies and guidelines, statements, and representations, societal expectations and public policy, as well as state and federal statutes and regulations including COPPA and Federal Trade Commission regulations. As outlined herein, the Android App games are marketed, promoted, and represented as safe and suitable for children, predicated on, *inter alia*, (i) their offering and availability and promotion and marketing in the DFF program in the Family section of the Google Play Store and the representations and statements concerning the DFF program and the Family section of the Google

[59] See 16 C.F.R. § 312.1 (COPPA "prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure or personal information from and about children on the internet.").

Play Store, (ii) the public statements marketing and promoting the games as suitable and appropriate for children by the Android App developers, and (iii) the inherent characteristics, content, and features of Android App games, which were designed for children.

331. At the same time, Defendants have (i) at all relevant times known that children under the age of 13 use the Android Apps, (ii) actively sought to increase use of the Apps by these children, and (iii) sought to exploit, for commercial purposes and gain, the millions of children under the age of 13 using the Android Apps. Defendants' knowledge of the widespread use of the Apps by children (which Defendants have expressly touted in their advertising sales efforts) and their concealment and failure to disclose the exfiltration of Personal Information from such children and they were tracking, profiling, and targeting these children and/or profiting from this conduct through lucrative behavioral advertising, while at the same time promoting, representing, and purporting to ensure that the Android Apps comply with law and societal expectation, are likely to and, in fact, did deceive Plaintiffs E.F.1 and E.F.2 and members of the New York Subclass and their parents or guardians.

332. Defendants' misrepresentations and omissions were explicit and implicit. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers such as the parents or guardians of Plaintiffs E.F.1 and E.F.2 and the New York Subclass Members about the terms under which their children were using the Apps as well as the fact that Defendants were collecting and profiting from the Personal Information of children under the age of thirteen without their parents and guardians' knowledge or consent.

333. Defendants had a duty to disclose the above-described facts due to the important public interest in securing the privacy of young children's Personal Information and the fact that young children are unable to fully protect their own interests. Parents and guardians of Plaintiffs E.F.1 and E.F.2 and the New York Subclass Members placed trust in Defendants as reputable companies which represent that they comply with applicable laws and societal interests in safeguarding childrens'

Personal Information. Additionally, Defendants exclusively knew and understood the extent of their collection of Personal Information, and the parents or guardians of Plaintiffs E.F.1 and E.F.2 and New York Subclass Members could not reasonably have discovered—and were unaware of—Defendants' secret tracking, profiling, and targeting.

334. Defendants' conduct is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, and there are no greater countervailing benefits to consumers or competition. Further, Plaintiffs and New York Subclass Members could not have reasonably avoided injury because Defendants took advantage of the lack of knowledge, ability, experience, and/or capacity of consumers to their detriment.

335. Defendants willfully engaged in the deceptive, misleading, and unlawful acts described herein and knew or recklessly disregarded the fact that they violated NY GBL § 349.

336. Plaintiffs E.F.1 and E.F.2 and New York Subclass Members were harmed by Defendants' practices, which were a substantial factor and caused injury in fact and actual damages to Plaintiffs E.F.1 and E.F.2 and New York Subclass Members. As a direct and proximate result of Defendants' unlawful, unfair, and deceptive acts and practices in violation of NY GBL § 349, Plaintiffs and New York Subclass Members have suffered and will continue to suffer an ascertainable loss of money or property, real or personal, and monetary and non-monetary damages, as described herein, including the loss of the value or diminishment in value of their Personal Information and the loss of the ability to control the use of their Personal Information, which allowed Defendants to profit at the expense of Plaintiffs E.F.1 and E.F.2 and New York Subclass Members.

337. As outlined herein, there is tangible value in Plaintiffs E.F.1 and E.F.2's and New York Subclass Members' Personal Information has tangible value. Plaintiffs E.F.1 and E.F.2 and New York Subclass Members have lost the opportunity to receive value in exchange for their Personal Information.

338. Defendants' monetization of Plaintiffs E.F.1 and E.F.2's and New York Subclass Members' Personal Information demonstrates that there is a market for their Personal Information.

339. Plaintiffs E.F.1 and E.F.2's and New York Subclass Members' Personal Information is now in the possession of Defendants, who have used and will use it for their financial gain.

340. Defendants' retention of Plaintiffs E.F.1 and E.F.2's and New York Subclass Members' Personal Information presents a continuing risk to them as well as the general public.

341. Plaintiffs E.F.1 and E.F.2 and New York Subclass Members seek relief for the injuries they have suffered as a result of Defendants' unlawful, unfair, and deceptive acts and practices, as provided by NY GBL § 349 and applicable law, including all actual damages and attorneys' fees and costs, treble damages, statutory damages, and restitution, as well as an injunction requiring Defendants to permanently delete, destroy or otherwise sequester the Personal Information collected without parental consent, requiring Defendants to provide a complete audit and accounting of the uses of the Personal Information by Defendants, App developers and any other third parties, and other appropriate injunctive and/or declaratory relief.

EIGHTH CLAIM FOR RELIEF

NEW YORK UNJUST ENRICHMENT
(On Behalf of Plaintiffs E.F.1 and E.F.2 and the New York Subclass)

342. Plaintiffs E.F.1 and E.F.2 incorporate the foregoing allegations as if fully set forth herein.

343. By virtue of the unlawful, unfair, and deceptive conduct alleged herein, Defendants knowingly realized hundreds of millions of dollars in revenue from the use and/or sale of Personal Information of Plaintiffs E.F.1 and E.F.2 and the New York Subclass members for advertising and commercialization purposes.

344. This Personal Information, the value of the Personal Information, and/or the attendant revenue from the use and profit by Defendants, were monetary benefits conferred upon Defendants by Plaintiffs E.F.1 and E.F.2 and the New York Subclass members.

345. As a result of Defendants' conduct, Plaintiffs E.F.1 and E.F.2 and the New York Subclass members suffered actual damages based on the loss of the value of their Personal Information and the lost profits from the use of the Personal information.

346. It would be inequitable and unjust to permit Defendants to retain the substantial economic benefits (financial and otherwise) they obtained from and/or at the expense of Plaintiffs E.F.1 and E.F.2 and the New York Subclass.

347. Defendants will be unjustly enriched if they are permitted to retain the economic benefits conferred upon them by Plaintiffs E.F.1 and E.F.2 and the New York Subclass members through Defendants obtaining Plaintiffs E.F.1 and E.F.2 and the New York Subclass members' Personal Information and the value thereof, and profiting from the unlawful, unauthorized, and impermissible use of the Personal Information of Plaintiffs E.F.1 and E.F.2 and the New York Subclass members.

348. Plaintiffs E.F.1 and E.F.2 and the New York Subclass members are therefore entitled to recover the amounts realized by Defendants at their expense.

349. Plaintiffs E.F.1 and E.F.2 and the New York Subclass members have no adequate remedy at law.

350. Plaintiffs E.F.1 and E.F.2 and the New York Subclass members are entitled to restitution, disgorgement, and/or the imposition of a constructive trust to recover the amount of Defendants' ill-gotten gains, and/or other sums as may be just and equitable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of themselves and the proposed Classes and Subclasses, respectfully request relief as follows:

A An order certifying this action as a class action, and certifying the Classes and Subclasses defined herein, designating Plaintiffs, as described above, as the representatives of the respective Classes

and Subclasses defined herein, and appointing Plaintiffs' counsel as counsel for the Classes and Subclasses;

B. An order declaring that Defendants' actions, as described above constitute: (i) a violation of California's Business & Professions Code as cited herein; (ii) breaches of the common law claim of intrusion upon seclusion as to the Intrusion Upon Seclusion Class; (iii) a violation of the right to privacy under the California Constitution, Article I, Section 1; (iv) a violation of the Florida Deceptive and Unfair Trade Practices Act, and the New York General Business Law, as cited herein; and (v) that Defendants' were unjustly enriched as a result of their actions.

C. A judgment awarding Plaintiffs and the members of the Classes and Subclasses appropriate relief, including actual, compensatory, and/or statutory damages, and punitive damages (as permitted by law), in an amount to be determined at trial;

D. A judgment awarding any and all equitable, injunctive, and declaratory relief as may be appropriate, including orders of disgorgement of Defendants' unlawful gains, and restitution.

E. A judgment awarding all costs, including experts' fees, attorneys' fees, and the costs of prosecuting this action, and other relief as permitted by law;

F. Pre-judgment and post-judgment interest, as permitted by law; and

G. Grant such other legal and equitable relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Respectfully submitted,

DATED: June 22, 2023

/s/ Patrick Carey

Mark Todzo, (Bar No. 168389)
Patrick Carey, (Bar No. 308623)
LEXINGTON LAW GROUP
503 Divisadero Street
San Francisco, CA 94117
Telephone: 415-913-7800

pcarey@lexlawgroup.com
mtodzo@lexlawgroup.com

David S. Golub
Steven L. Bloch
Ian W. Sloss
Jennifer Sclar
Johnathan Seredynski
SILVER GOLUB & TEITELL LLP
One Landmark Square, Floor 15
Stamford, Connecticut 06901
Telephone: (203) 325-4491
Fax: (203) 325-3769
isloss@sgtlaw.com
sbloch@sgtlaw.com
jsclar@sgtlaw.com
jseredynski@sgtlaw.com

Exhibit A

The following 86 DFF Apps were developed by Tiny Lab, incorporated the AdMob SDK, were submitted to the DFF Program by Tiny Lab, and accepted in to the DFF Program by Google:

1. Angry Bunny Race: Jungle Road
2. Arctic Roads: Car Racing Game
3. Automatron Galaxy Wars: Transform, Shoot and Drive
4. Baby Toilet Race: Cleanup Fun
5. Battleship of Pacific War: Naval Warfare
6. Bike Race Game: Traffic Rider of Neon City
7. Bike Race: Speed Racer of Night City
8. Bike Racing Show: Stunt & Drag
9. Car Games: Neon Rider Drives Sport Cars
10. Christmas Games: Santa Train Simulator
11. Cute Robotic Racing - Future Ccars
12. Desert Rally Trucks: Offroad Racing
13. DexLand
14. Dino World Speed Car Racing
15. Dinosaur Park Train Race
16. Dragon Fight: Boss Shooting Game
17. Dragon Panda Racing
18. Elite SWAT Car Racing: Army Truck Driving Game
19. Emergency Car Racing Hero
20. Extreme Car Driving: Race of Destruction
21. Fast Ambulance Racing - Medics!

22. Fast Cars: Formula Racing Grand Prix
23. Fire Fighters Racing: Fireman Drives Fire Truck
24. Forest Truck Simulator: Offroad & Log Truck Games
25. Fun Kid Racing
26. Fun Kid Racing - Jungle Cars
27. Fun Kid Racing - Madagascar
28. Fun Kid Racing - Motocross
29. Fun Kid Racing - Safari Cars
30. Fun Kid Racing City Builder
31. Fun Kid Racing Dinosaurs World
32. Fun Kid Racing Magic Forest
33. Fun Kids Train Racing Games
34. Fun School Race Games for Families
35. GummyBear and Friends speed racing
36. Halloween Cars: Monster Race
37. Halloween Town Racing
38. Happy Easter Bunny Racing
39. Ice Road Truck Driving Race
40. Interactive Police Car Racing
41. Jet Car Power Show: Max Speed Race
42. Jet Truck Racing: City Drag Championship
43. Jungle Monster Truck Adventure Race
44. Jungle Motocross Extreme Racing
45. Mad Road: Apocalypse Moto Race
46. Magic Circus Festival

47. Magic Elf Fantasy Forest Run
48. Mini Tanks World War Hero Race
49. Monster Bike Motocross
50. Monster Truck Police Racing
51. Monster Truck Racing
52. Monster Truck Winter Racing
53. Monster Trucks Action Race
54. MotoCross - Police Jailbreak
55. Motocross Games: Dirt Bike Racing
56. Motocross Kids - Winter Sports
57. Motorcycle Racer - Bike Games
58. Night City: Speed Car Racing
59. Paradise Island Summer Fun Run
60. Pet Friends Park Racing
61. Pirate Ship Shooting Race
62. Prehistoric Run Racing
63. RC Toy Cars Race
64. RollerCoaster Fun Park
65. Run Cute Little Pony Race Game
66. Safari Motocross Racing
67. Skater Boys - Skateboard Games
68. Slice the Cheese
69. Space Race - Speed Racing Cars
70. Sports Bikes Racing Show
71. Sports Cars Racing: Chasing Cars on Miami Beach
72. Summer Car Racing - Australia
73. Superheroes Car Racing

74. SUV Safari Racing: Desert Storm Adventure

75. Sweet Candy Racing

76. Tank Race: WW2 Shooting Game

77. Tractor Hill Racing

78. Tropical Island Boat Racing

79. Truck Driving Race US Route 66

80. Western Train Driving Race

81. Wild West Race

82. Winter Racing - Holiday Fun!

83. Winter Wonderland Snow Racing

84. Zombie Shooter Motorcycle Race

85. Zombie Shooting Race Adventure

86. Zombie Survival Games: Pocket Tanks Battle

Public court record.

This copy was downloaded from https://storage.courtlistener.com/recap/gov.uscourts.cand.414466/go
on 2026-10-19 and is hosted, unaltered, for reference at
https://chimo.ai/class-action/google-play-kids

Court: U.S. District Court, N.D. California
Case number: 5:23-cv-03101-PCP
Filed: 2023-06-22

Chimo hosts public court records for readers' reference; documents are
unaltered copies from the court docket or the court-approved settlement website.