

1 Patrick Carey, (Bar No. 30862)
2 Mark Todzo, (Bar No. 168389)
3 LEXINGTON LAW GROUP
4 503 Divisadero Street
5 San Francisco, California 94105
6 Telephone: (415) 913-7800
7 pcarey@lexlawgroup.com
8 mtodzo@lexlawgroup.com

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

22 *Attorneys for Plaintiffs and the Proposed Class*

23
24
25 **UNITED STATES DISTRICT COURT**
26
27 **NORTHERN DISTRICT OF CALIFORNIA**

28
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

1 Plaintiffs A.B., by and through his guardian Jen Turner, C.D.1, C.D.2, and C.D.3, by and through
2 their guardian Kirenda Johnson, and E.F.1, and E.F.2., by and through their guardian Barbara Hayden-
3 Seaman (collectively, “Plaintiffs”), hereby allege the following against Google LLC (“Google”),
4 AdMob Google Inc., and AdMob, Inc. (the AdMob entities are referred to jointly as “AdMob”, and
5 collectively with Google, “Defendants”) on behalf of themselves and all others similarly situated.
6 Plaintiffs’ complaint is based on personal knowledge, information and belief, the investigation of
7 counsel, and public sources.
8

9 **NATURE OF ACTION**

10 1. This action arises out of the Defendants’ unlawful invasion of privacy and violation of
11 the reasonable expectations of privacy of millions of children under the age of 13. Through apps
12 directed at children, Defendants knowingly and intentionally collected personal information without
13 parental consent to track and profile the children using these apps and target them with highly lucrative
14 behavioral advertising at the expense of the children’s privacy rights and in violation of well-established
15 privacy protections, societal norms, and the laws embodying those protections.
16

17 2. Defendant Google designed, developed, maintains, and markets Android, a “mobile
18 operating system” used on a reported 2.5 billion tablets, phones, and other mobile devices (“Android
19 Device(s)”) worldwide, including over 130 million in the United States.
20

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

25 4. Defendants AdMob Google Inc. and AdMob, Inc. are mobile advertising companies
26 owned by Google which enable Android App developers to show advertisements to users of their Apps.
27
28

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

3 5. The AdMob SDK provides Android App developers with code to include in their
4 Android Apps which (1) enables Google and AdMob to collect data, including persistent identifiers,
5 from the Android App users; and (2) shows advertisements to Android App users while they are using
6 those Apps based on the persistent identifiers collected. AdMob pays developers for the ability to track
7 their users and show advertisements to users within their Apps.
8

9 6. All of this activity serves one purpose: to collect as much data as possible about an
10 individual so that AdMob and Google can make money showing that individual (and other children like
11 him or her) highly-targeted advertisements.
12

13 7. Advertisers pay AdMob to advertise on the AdMob network because of its vast reach and
14 the precision with which AdMob can target specific demographics. These features are a direct result of
15 AdMob’s extensive tracking of every user of an Android App in which the AdMob SDK is embedded.
16

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

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

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

26 11. Google designed, developed, and in or about April 2015 began marketing the “Designed
27 for Families” program (“DFF”) on the Google Play Store. Google developed DFF to give parents
28

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

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

9
10 13. In particular, Google represented it required that Apps included in the DFF program
11 which displayed ads “compl[ied] with applicable legal obligations relating to advertising to children”
12 and that “[a]ds displayed to child audiences d[id] not involve interest-based advertising.”²

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

21
22 15. In addition, thirty-four (34) states, including California, have firmly rooted protections
23 against unwarranted invasions of privacy by recognizing the common law right to be free from intrusion
24

25
26
27 ¹ <https://techcrunch.com/2015/04/14/google-plays-new-program-designed-for-families-will-highlight-pre-approved-kid-safe-apps/>

28 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).

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

3 16. Based on COPPA and the societal norms embodied therein, bedrock, long-standing
4 privacy protections, Google’s guidelines and requirements concerning the DFF program and the
5 standards for the Android Apps included in the DFF program, as well as the inherent characteristics of
6 the Android App games themselves, parents and their children had a reasonable expectation of privacy
7 in the children’s online behavior and activities and the mobile devices utilized by the children and that
8 the games that appeared in the DFF section of the Google Play Store that were directed primarily to
9 children complied with applicable legal obligations as confirmed by Google.
10

11 17. DFF benefited Defendants and App developers alike. The DFF program provided young
12 children using Google’s Android Devices with easy access to games they would be interested in, which
13 in turn grew Android App developers’ user base. DFF also provided Defendants with easy access to a
14 demographic coveted by advertisers: young children.
15

16 18. Millions of Apps were submitted to Google for inclusion in the DFF program by
17 developers, reviewed by Google, and approved for DFF program inclusion. Many of these Apps,
18 including Fun Kid Racing, GummyBear and Friends Speed Racing, and Monster Truck Racing
19 explicitly noted in their applications to DFF and elsewhere (including on Apps and/or their websites)
20 that the Apps were intended for and directed towards children under the age of 13. Plaintiffs played
21 many Apps Google included in its DFF program, including Fun Kid Racing, Monster Truck Racing, and
22 GummyBear and Friends Speed Racing.
23

24 19. Unbeknownst to Plaintiffs and their parents but known to Defendants, while Google
25 implemented strict guidelines and standards for the DFF program, and publicly represented that DFF
26 Apps complied with COPPA and other applicable laws regarding data collection and interest-based
27 advertising, Defendants were surreptitiously exfiltrating the personal information of the children under
28

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

3 20. Google knew it was exfiltrating personal information of children under 13 because
4 Google reviewed each and every App included in the DFF program, owned and operated the advertising
5 platform that served behavioral advertising to children under 13 as they played the DFF apps (and still
6 does), and was, in fact, informed by independent researchers that these Apps were operating in violation
7 of COPPA.
8

9 21. Further, as described below, forensic testing performed by the New Mexico Attorney
10 General's Office – following that independent research – revealed that the AdMob SDK collects highly-
11 sensitive personal data, including a child's precise location within +/- 5 meters and was constantly
12 updating that data to maintain accuracy.
13

14 22. Notwithstanding their knowing and intentional conduct aimed at these minor children,
15 Defendants did not disclose that it was collecting the personal information of children under 13 and did
16 not obtain parental consent for the collection of the personal information or the tracking, profiling, and
17 targeting of children under 13 using that information for behavioral advertising (or any other purposes).
18

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

23 24. Accordingly, Plaintiffs bring this action on behalf of themselves and the classes (as
24 defined below) of similarly-situated minors under the age of 13 whose privacy rights have been violated
25 by Defendants, for disgorgement of Defendants' ill-gotten gains, compensatory, actual, and statutory
26 damages, restitution, punitive damages, and injunctive relief and/or equitable relief to require
27 Defendants permanently delete, destroy or otherwise sequester the Personal Information unlawfully
28

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

3 **JURISDICTION AND VENUE**

4 25. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §
5 1332(d), because the amount in controversy for the Class exceeds \$5,000,000 exclusive of interest and
6 costs, there are more than 100 putative members defined below, and minimal diversity exists because
7 the majority of putative class members are citizens of a state different from Defendants.
8

9 26. This Court has specific personal jurisdiction over Defendants Google LLC, AdMob
10 Google Inc., and AdMob, Inc. because they purposefully direct their conduct toward California, transact
11 business in this District and in California, engage in conduct that has had and continues to have a direct,
12 substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the
13 United States, including those in this District and in California, and purposely availed themselves of the
14 laws of California. Additionally, this Court has general personal jurisdiction over Google and the
15 AdMob entities because they are headquartered in and have their principal places of business in
16 California.
17

18 27. This Court also has jurisdiction pursuant to 28 U.S.C. §1332(d), because the amount in
19 controversy exceeds \$75,000 and is between citizens of different states.
20

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

24 **INTRADISTRICT ASSIGNMENT**

25 29. Assignment to the San Jose Division is proper under Northern District of California Civil
26 Local Rule 3-2 (c) because a substantial part of the events or omissions which give rise to the claims
27 asserted herein occurred in Santa Clara County and Defendants principal places of business are located
28

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

3 **PARTIES**

4 30. Plaintiff A.B. is a natural person and is a U.S. citizen, domiciled in the State of
5 California. A.B. was under the age of 13 during the relevant time period. A.B.'s parent and legal
6 guardian is Jen Turner, who is also a U.S. citizen, domiciled in the State of California.
7

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

11 32. Plaintiff C.D.2 is a natural person and is a resident and citizen of the State of Florida.
12 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.
13 citizen, domiciled in the State of Florida
14

15 33. Plaintiff C.D.3 is a natural person and is U.S. citizen, domiciled in the State of Florida.
16 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.
17 citizen, domiciled in the State of Florida.

18 34. Plaintiff E.F.1 is a natural person and is U.S. citizen, domiciled in the State of New York.
19 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
20 U.S. citizen, domiciled in the State of New York.
21

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

25 36. Defendant Google, LLC is a business incorporated under the laws of the state of
26 Delaware with its principal place of business in Mountain View, California. Google is a wholly-owned
27 subsidiary of Alphabet, Inc.
28

1 37. Defendants AdMob Google Inc. and AdMob, Inc. are wholly-owned subsidiaries of
2 Google, incorporated under the laws of the state of Delaware. The AdMob entities run a mobile
3 advertising business and maintain its principal place of business in Mountain View, California.
4

5 **BACKGROUND**

6 **I. GOOGLE'S DATA COLLECTION AND ADVERTISING ACTIVITIES**

7 **A. GOOGLE**

8
9 38. Google is a multinational corporation known primarily for the design, development, and
10 operation of the world's most visited internet webpage: www.google.com ("Google.com"). Google.com
11 hosts a search engine that catalogues websites and organizes information on the internet to allow Google
12 users to search the contents of the internet as catalogued by Google.

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

19
20 40. In addition to Google's software applications, operating systems, and cloud services,
21 Google manufactures mobile phones, earbuds, watches, laptops, speakers, cameras, thermostats, Wi-Fi
22 routers, as well as accessories for those devices.

23
24 41. Each of Google's software applications, web services, and devices, including the Android
25 operating system and the Google Play Store, is designed with one thing in mind: collecting as much
26

27
28

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

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

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

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

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

17 45. Then, when that user visits *another* website that has opted to use Google's advertising
18 services, the other website that uses Google's advertising services sends Google the same IP address or
19 IMEI number or information that matched a particular visitor, and Google knows that individual has
20 visited both websites.
21
22
23
24

25 ⁵ <https://www.statista.com/statistics/266249/advertising-revenue-of-google/>;
26 <https://www.statista.com/statistics/266206/googles-annual-global-revenue/>.

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

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

4 47. The data Google gathers is stitched into a single profile of a user which gives Google the
5 most accurate, up-to-date, snapshot of a user's attributes and behaviors. Google uses this data to deliver
6 targeted advertisements to users as they visit websites on the internet or use other internet-connected
7 services. User profiles such as those developed by Google have been called the "holy grail" of
8 advertising⁷ and allow Google to charge advertisers increased advertising rates.

9
10 **B. GOOGLE'S ANDROID ECOSYSTEM: ANDROID, GOOGLE PLAY STORE,**
11 **AND ADMOB**

12 **1. ANDROID**

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

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

22 50. Google responded by developing Android, its own mobile operating system with
23 countless (and often hidden) ways to track Android Device users' activities and exfiltrate their data.
24
25
26

27 _____
28 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).

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

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

8 53. Android is now the most widely used mobile operating system in the world. As of May
9 18, 2021, there were 3 billion active Android devices (meaning devices that had been used in the
10 previous month), compared with, for example, Apple’s 2 billion active iOS users.

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

13 55. In order to generate more data and learn more about Android users, Google devised
14 numerous ways to cause Android users to further engage with their Android devices so that Google
15 could track that activity and use that data for advertising purposes. The primary way Google
16 accomplished this was through the development of the application now named Google Play Store.
17

18
19 **2. GOOGLE PLAY STORE**

20 56. Google Play Store (“Google Play”) is a digital distribution service developed and
21 operated by Google, launched in 2008 as Android Marketplace and later rebranded to Google Play
22 Store.
23

24 57. Google Play functions as a mobile application that runs on Google’s Android mobile
25 operating system and comes preinstalled on every mobile Android device.
26
27

28

⁸ <https://earthweb.com/how-many-people-use-android/>

1 58. Google Play's purported purpose is to provide Android device users with additional
2 Android software applications, adding functionality to, or new ways to use, Android devices. The types
3 of Apps available on Google Play include, but are not limited to, Apps which enable users to learn the
4 weather, enjoy music, read books, and play games, among other things.
5

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

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

10 61. As with Android, Google's primary motivation for developing Google Play was to gain
11 access to more user data in order to build more detailed profiles about internet users and serve them
12 lucrative advertising.
13

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

18 63. In 2021 alone, the use of content creators for Google's ad network generated \$32 billion
19 dollars of revenue for Google.¹² Overall, mobile advertisers reportedly spent \$288 billion in 2021,
20 including \$117 billion in the U.S.¹³
21

23 ⁹ <https://42matters.com/google-play-statistics-and-trends>.

24 ¹⁰ <https://www.statista.com/statistics/734332/google-play-app-installs-per-year/>.

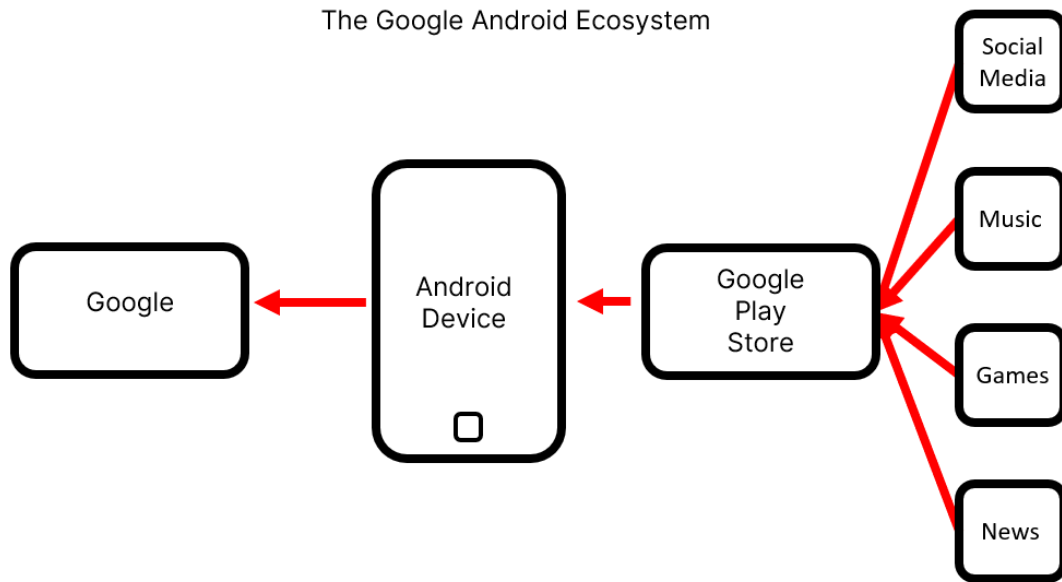
25 ¹¹ <https://42matters.com/google-play-statistics-and-trends>.

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

27 ¹³ <https://www.businessofapps.com/ads/research/mobile-app-advertising-cpm-rates/#:~:text=According%20to%20Statista%2C%20globally%20mobile%20advertising%20spend%20rose,by%200%24227%20in%202020%20to%20%24288%20in%202021>
28

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

3
4 **FIGURE 1**



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

19
20 **3. ADMOB**

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

25 67. Google shows advertisements to Android App users via AdMob, which Google acquired
26 in 2009 for \$750 million.
27
28

1 68. Google described AdMob and the purpose behind Google’s AdMob acquisition as
2 follows (Google Play Store was previously known as Android Marketplace):
3

4 In addition to search, another key way that people access information is through mobile websites
5 (accessed through a browser) and mobile apps (available through Apple’s App Store, the
6 **Android Marketplace** and more).

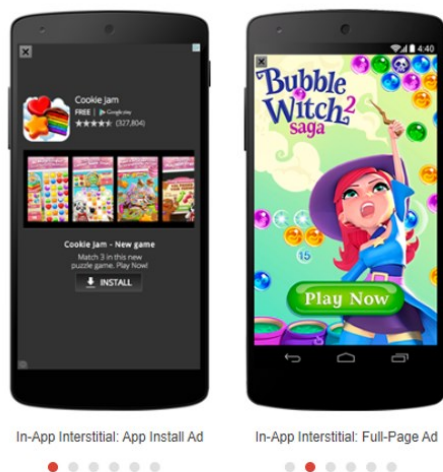
7 Mobile display and text ads make it easy for publishers and developers to make money from
8 their mobile websites and apps, and enable advertisers to extend the reach of their campaigns to
9 relevant mobile content. In this area, AdMob has been a real pioneer and has innovated at a
10 tremendous pace, building a successful business and working with thousands of advertisers,
11 publishers and developers.

12 **AdMob was one of the first companies to serve ads inside mobile applications on the**
13 **Android and iPhone platforms.** They’ve developed a host of engaging and creative ad
14 units for Android and iPhone apps—for example, interactive video ad units and
15 expandable rich media ads. Google has also been developing new features for in-app ads.
16 For example, last week, we announced that we’ll be making “click-to-call” ad formats
17 available to developers who run AdSense in their mobile apps. With Google and AdMob
18 starting to work together, there’s lots more innovation to come in this area.

19 ...

20 It’s clear that mobile advertising is growing incredibly fast with lots of businesses
21 innovating at great speed. Every day, more marketers are looking to take advantage of the
22 mobile-specific capabilities, extended reach, great returns and value that mobile
23 advertising provides. Advertisers are now starting to see mobile as an essential part of
24 their overall campaigns, not just a silo-ed experiment on the side.

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



Choose the right ad format

Drive mobile ad revenue by integrating banner, interstitial, or video ads seamlessly into your app. Our variety of formats means you have lots of choices to provide the best user experience.

- Banner ads appear at the top or bottom of your app screen and can prompt users to install apps, visit websites, get directions, view products or call a phone number. Our in-app engagement ads expand to full screen when the banner is tapped. Our smart banners automatically resize to fit different screen sizes as the user rotates their device.
- AdMob interstitials are full-page ads that appear in your app at natural breaks or transition points. A common use case is after a level is completed in a game. Our advertisers use interstitials to create engaging brand experiences, or direct action, such as driving app downloads.
- AdMob's video ads bring rich brand experiences to your app, and the flexible nature of the format allows users to skip the video after 5 seconds.

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:

- 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.
- Location Data:** this includes location data acquired via GPS, Wi-Fi, and cellular networks.
- App usage data:** this includes data relating to the duration or frequency of app usage.
- In-app behavior data:** this includes data on behavior such as in-app purchasing, or in game behavior.
- 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.

1 72. AdMob promised App developers that “[w]hen you monetize with AdMob you get
2 instant access to all of Google’s demand sources. This includes a million Google advertisers as well as
3 real-time bidding (RTB) buyers via the DoubleClick Ad Exchange.”

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

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

- 7
- 8 a. **AdMob SDK App Integration:** An App developer that wishes to make
9 money via advertising includes the AdMob SDK code in the App to allow the
10 App to communicate with AdMob server’s, sending AdMob information
11 about the App users and receiving display ads back.
 - 12 b. **Developer Select Display Ad Unit:** Once the SDK is integrated, the app
13 developer can create “Display Ad Units” in the AdMob dashboard. These
14 specific locations in the app where ads will be displayed, such as banners,
15 interstitials, or rewarded video ads.
 - 16 c. **App Ad Request:** When a user opens the app and an ad unit is triggered, the
17 Android App sends an ad request to AdMob’s servers.
 - 18 d. **AdMob Ad Selection:** AdMob’s servers then use personal information,
19 including device identifiers and users’ location, to select the most relevant ad
20 to display. This process can take a few forms, one of which involves Real
21 Time Bidding, or RTB, where advertisers instantaneously submits “bids” to
22 place their ads in a given display ad unit based on the personal information
23 exfiltrated about the user, and other information. The advertiser with the
24 winning big pays AdMob to have their ad placed.
 - 25 e. **AdMob Ad Delivery & Display:** Once AdMob selects an ad to display, it
26 sends the ad to the App and displays it within the designated ad unit.
 - 27 f. **Revenue:** AdMob shares the revenue they get from advertisers with App
28 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.

25 75. The AdMob SDK embedded within an Android App sends a users’ PII back to AdMob,
26 where AdMob analyzes, stores, and uses the data to build increasingly-detailed profiles of users. It is
27 also shared with and sold to myriad third-parties so that each can continue to build their own profiles.
28

1 76. During the relevant period, the AdMob SDK was incorporated into over one million
2 apps, facilitating 200 billion ad requests per month, and resulted in over \$3.5 billion dollars being paid
3 to App developers, most of whom did not charge users for their Apps.¹⁴
4

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

7 **II. THE CHILDREN’S ONLINE PRIVACY PROTECTION ACT OF 1998**

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

13
14 It is unlawful for an operator of a website or online service directed to children, or any operator
15 that has actual knowledge that it is collecting personal information from a child, to collect
16 personal information from a child in a manner that violates the regulations prescribed [by the
17 Federal Trade Commission].

18 15 U.S.C. § 6502(a).

19 79. COPPA applies to any operator of a commercial website or online service directed to
20 children under thirteen years of age and that (a) collects, uses, and/or discloses personal information
21 from children under 13 or (b) on whose behalf such information is collected or maintained. The FTC
22 has interpreted COPPA’s definition of “website or online service” to include “mobile apps that send or
23 receive information online (like network-connected games, social networking apps, or apps that deliver
24
25

26 _____
27 ¹⁴ <https://admob.google.com/home/> (as it appeared on Sept. 4, 2018).

28 ¹⁵ [https://www.cnn.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-
.html](https://www.cnn.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown.html).

¹⁶ 144 CONG. REC. S12787.

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

5
6 80. Further, according to the FTC, “content creators and channel owners” are both
7 “standalone ‘operators’ under COPPA, subject to strict liability for COPPA violations.”¹⁸ And the FTC
8 considers third parties with actual knowledge that is collecting personal information from users of a
9 child-directed site or service as operators under COPPA.

10 81. In order to determine whether a website or online service is “directed to children” the
11 FTC will:

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

18 16 CFR § 312.2.

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

23
24
25 _____
26 ¹⁷ <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business>.

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

1 83. COPPA defines a “child” as an individual under the age of thirteen. 15 U.S.C. § 6501(a).
2 In relevant part, the FTC regulations require an operator to disclose information collection practices and
3 “obtain verifiable parental consent for [any] collection, use, or disclosure of personal information from
4 children.” Id. § 6502(b)(1)(A); see 16 C.F.R. § 312.5(a).
5

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

- 8 a. full name;
- 9 b. home or physical address;
- 10 c. online contact information such as an email address or other identifier;
- 11 d. telephone number;
- 12 e. social security number;
- 13 f. persistent identifier that can be used to recognize a user over time and across different
14 sites, including a cookie number, an IP address, a processor or device serial number,
15 or a unique device identifier;
- 16 g. Photo, video, or audio file containing a child’s image or voice; and
- 17 h. Geolocation information sufficient to identify a street name and city or town.
18

19 85. COPPA thus prohibits, *inter alia*, the collection of persistent identifiers for behavioral
20 advertising absent notice and verifiable parental consent. 16 C.F.R. §§ 312.5(c)(7), 312.2.
21

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

24 87. In 2013, COPPA was enhanced (the “2013 COPPA Enhancement”) to provide further
25 protection for children against online tracking and to “giv[e] parents greater control over the online
26 collection of their children’s personal information.” The 2013 enhancement widened the definition of
27
28

1 children’s “Personal Information” to include “persistent identifiers” such as cookies that track a child’s
2 activity online, geolocation information, photos, videos, and audio recordings.

3 88. The 2013 COPPA Enhancement was the culmination of two years of rulemaking by the
4 Federal Trade Commission (“FTC”) and reflected society’s growing recognition of the surreptitious
5 surveillance tactics used by advertising companies to track children and advertise to them via mobile
6 apps.
7

8 89. For example, the FTC published a 2012 report entitled *Mobile Apps for Kids: Disclosures*
9 *Still Not Making the Grade* (the “FTC Kids Mobile App Report”) addressing privacy dangers for
10 children using mobile apps. The report warned that companies like Google and AdMob (advertising
11 platform operators) link persistent identifiers and geolocation data they collect with additional Personal
12 Information such as name, address, and email address—allowing those entities and their partners to
13 identify individual users whom they profile with indisputably individual specificity.
14

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

17 [O]ne ad network received information from 31 different apps. Two of these apps
18 transmitted geolocation to the ad network along with a device identifier, and the other 29
19 apps transmitted other data (such as app name, device configuration details, and the time
20 and duration of use) in conjunction with a device ID. The ad network could thus link the
21 geolocation information obtained through the two apps to all the other data collected
22 through the other 29 apps by matching the unique, persistent device ID.¹⁹

23
24 ¹⁹ Mobile Apps for Kids: Disclosures Still Not Making the Grade, Federal Trade Commission,
25 FTC Staff Report (Dec. 2012), at 10 n. 25 (emphasis added) (citing David Norris, Cracking the
26 Cookie Conundrum with Device ID, AdMonsters (Feb. 14, 2012) (available at
27 [https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-notmaking-
28 grade/121210mobilekidsappreport.pdf](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).

1 91. By expressly including persistent identifiers and geolocation data in COPPA’s definition
2 of Personal Information, the FTC intended to deter advertising companies and advertising network
3 operators from exploiting young children via mobile app tracking, profiling, and advertising.
4

5 **III. GOOGLE’S DESIGNED FOR FAMILIES PROGRAM**

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

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

11 There are thousands of Android developers creating experiences for families and children —
12 apps and games that broaden the mind and inspire creativity. These developers, like PBS Kids,
13 Tynker and Crayola, carefully tailor their apps to provide high quality, age appropriate content;
14 from optimizing user interface design for children to building interactive features that both
educate and entertain.

15 Google Play is committed to the success of this emerging developer community, so today we’re
16 introducing a new program called Designed for Families, which allows developers to designate
17 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.

18 94. Google stated that Apps which opted into the DFF program would be required to meet a
19 “stringent legal and policy bar” and “will need to undergo a specialized operations review”²⁰ to ensure
20 compliance with the DFF program’s rules, including, *inter alia*, data collection and ad targeting, and the
21 Apps were required to comply with COPPA and all other applicable children’s privacy regulations.²¹
22
23
24
25

26 _____
27 ²⁰ <https://techcrunch.com/2015/04/14/google-plays-new-program-designed-for-families-will-highlight-pre-approved-kid-safe-apps/>

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

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

3
4 Eligibility

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

9 ...

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

12 2.1 You comply with applicable legal obligations relating to advertising to children.

13 2.2 Ads displayed to child audiences do not involve interest-based advertising or
14 remarketing.

15 2.3 Ads displayed to child audiences present content that is appropriate for children.

16 2.4 Ads displayed to child audiences follow the Designed for Families ad format
17 requirements.

18 ...

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

22 ...

23 Ad targeting and data collection

24 Ads displayed to child audiences must comply with laws relating to advertising to kids. For
25 example. Your app must disable interest-based advertising and remarketing, and should comply
26 with child relevant regulations and industry standards for all countries where the app is
27 distributed.

28 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

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

3 98. Significantly, Google warned that noncompliance with these requirements could result in
4 expulsion from either or both the DFF program and Google Play:
5

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

10 **IV. GOOGLE’S PATTERN AND PRACTICE OF DATA MISCONDUCT AND PRIVACY**
11 **VIOLATIONS**

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

- 14 a. On October 24, 2011, Google entered into a settlement with the Federal Trade
15 Commission for using deceptive tactics and violating its own privacy policy when it
16 launched Buzz, its social networking feature; the settlement barred Google from future
17 privacy misrepresentations, required it to implement a comprehensive privacy
18 program, and subjected it to independent privacy audits for 20 years²².
- 19 b. On August 9, 2012, Google paid \$22.5 million to settle FTC charges that Google had
20 not adequately disclosed Google’s practices regarding its tracking cookies to users of
21 Apple’s Safari Internet browser, in violation of Google’s 2011 settlement with the
22 FTC.²³
- 23 c. On November 18, 2013, Google entered into a \$17 million settlement with attorneys
24 general from 37 states and the District of Columbia to resolve allegations that the
25 company had circumvented privacy settings pertaining to Safari, Apple Inc.’s Web
26 browser.²⁴
- 27 d. On January 21, 2019, Google was fined \$57M by France’s data protection authority,
28 the CNIL, for failing to comply with GDPR transparency and consent rules, including

25 ²² [https://www.ftc.gov/news-events/news/press-releases/2011/10/ftc-gives-final-approval-settlement-
26 google-over-buzz-rollout](https://www.ftc.gov/news-events/news/press-releases/2011/10/ftc-gives-final-approval-settlement-google-over-buzz-rollout).

27 ²³ [https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-
28 charges-it-misrepresented-privacy-assurances-users-apples](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](https://www.reuters.com/article/google-settle/google-to-pay-17-million-to-settle-states-safari-probe-idINDEE9AH0G620131118).

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

- 3 e. In September 2019, Google, and its subsidiary YouTube, paid \$170 million to settle
4 allegations by the FTC and the New York Attorney General. The settlement required
5 Google and YouTube to pay \$136 million to the FTC and \$34 million to New York
6 for allegedly violating COPPA.²⁶
- 7 f. On March 11, 2020, Sweden’s Data Protection Authority (DPA) fined Google \$8
8 million for “failure to comply” with Europe’s General Data Protection Regulation
9 (“GDPR”) as a result of Google’s failure to adequately remove search result links
10 under right-to-be-forgotten requests after the DPA had instructed Google to honor
11 these requested in 2017.²⁷
- 12 g. On May 18, 2022, the Spanish Agency for Data Protection (AEPD) fined Google €10
13 million, its highest fine to date, for the violation of Articles 6 and 17 of GDPR,
14 following two complaints and subsequent investigation from the AEPD. The AEPD
15 noted that the complaints concerned the transfer of requests related to the removal of
16 content from Google’s various products and platforms, including the Google search
17 engine and YouTube, to a third party, the ‘Lumen Project.’ Specifically, the AEPD
18 explained that to enable the removal of content, Google required users that used the
19 relevant forms to accept the transfer of copies of content removal requests to
20 ‘lumendatabase.org,’ on which they would, subsequently be published.²⁸
- 21 h. On August 12, 2022, the Federal Court of Australia ordered Google to pay \$60 million
22 in fines for misleading Australian Android users as to how and when it would collect
23 and use their personal data²⁹.
- 24 i. On September 14, 2022, South Korea’s Personal Information and Protection
25 Commission fined Google \$50 million for not clearly informing users or obtaining
26 their consent as they collected information about their online activities when they used
27 other websites or services outside their own platforms. This data was used to analyze
28 their interests and create individually customized advertisements.³⁰

23 ²⁵ <https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/>.

24 ²⁶ <https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law>.

25 ²⁷ https://edpb.europa.eu/news/national-news/2020/swedish-data-protection-authority-imposes-administrative-fine-google_en.

26 ²⁸ <https://www.dataguidance.com/news/spain-aepd-fines-google-10m-unlawful-transfer-personal>.

27 ²⁹ <https://www.smh.com.au/business/consumer-affairs/google-fined-60m-for-misleading-android-users-about-data-collection-20220812-p5b9hg.html>.

28 ³⁰ <https://apnews.com/article/technology-south-korea-252a9cc71f0875575340ade7265af951>.

- 1 j. On September 28, 2022, Google agreed to a \$100M settlement in class action lawsuit,
2 *Rivera, et al. v. Google*. The lawsuit alleges that Google violated Illinois law by
3 collecting and storing biometric data of individuals who, while residing in Illinois,
4 appeared in a photograph in the photograph sharing and storage service known as
5 Google Photos.³¹
- 6 k. On October 4, 2022, Arizona Attorney General Mark Brnovich announced a historic
7 \$85 million settlement with Google for deceptively obtaining users' location data to
8 make billions of dollars in profit.³²
- 9 l. On November 14, 2022, Google agreed to a \$391.5 million settlement to resolve
10 litigation brought by a 40-state coalition of attorneys general for charges that Google
11 misled users into thinking they had turned off location tracking in their account
12 settings even as the company continued collecting that information.³³
- 13 m. As of December 30, 2022, Google was ordered to pay \$9.5 million of the total
14 settlement amount of \$29.5 million to the District of Columbia after it sued the
15 company alleging that it tracked users' locations without their permission.³⁴
- 16 n. As of January 3, 2023, Google is to pay Indiana \$20 million to resolve the state's
17 lawsuit regarding Google's allegedly deceptive location tracking practices.³⁵
- 18 o. On Jan 5, 2023, Google agreed to pay \$23 million to resolve a consolidated,
19 California-based class-action lawsuit brought by consumers for sharing the contents
20 of their queries with advertisers or other third parties without their permission. The
21 proposed settlement also requires Google to provide extra disclosures to users about
22 search term-sharing practices. The settlement is awaiting court approval.³⁶

23 SUBSTANTIVE ALLEGATIONS

24 **I. GOOGLE TARGETED CHILDREN UNDER THIRTEEN VIA THE DESIGNED FOR** 25 **FAMILIES PROGRAM**

26 100. Children are among the most valuable demographics for advertisers to reach for at least
27 two reasons. First, children are easily influenced. It is for this very reason, and based on their inherent
28

24 ³¹ <https://www.law360.com/articles/1534091/google-s-100m-bipa-deal-gets-final-approval>.

25 ³² <https://www.azag.gov/press-release/attorney-general-mark-brnovich-achieves-historic-85-million-settlement-google>.

26 ³³ <https://www.nytimes.com/2022/11/14/technology/google-privacy-settlement.html>.

27 ³⁴ <https://www.visitor-analytics.io/en/blog/google-location-tracking-without-consent/>.

28 ³⁵ <https://www.wthr.com/article/news/local/google-to-pay-indiana-20-million-to-resolve-privacy-lawsuit/531-48ebae6-ee2b-4f2f-9009-d71e43aaaab7>.

³⁶ *See In re Google Referrer Header Privacy Litig.*, Case No. 10-cv-04809 (N.D. Cal.).

1 vulnerabilities, children enjoy special protections from invasion of privacy, including from those such as
2 advertisers seeking to influence them. While COPPA codified protections for children under 13
3 regarding surreptitious tracking online without parental consent, state common laws have long protected
4 against unreasonable, unwarranted, and offensive intrusions into children's privacy.
5

6 101. Second, children influence the spending habits of their entire families. For example, in
7 2008, it was estimated that American children under 12 directly influence over 700 billion dollars in
8 family spending a year, a figure that has since increased. Additionally, recent studies show that 80% of
9 parents believe that kids play a role in household purchasing decisions, with an outsized influence over
10 purchases of toys (92%), electronics (68%), clothing (88%), food (87%), entertainment (91%), travel
11 (84%).³⁷ Unfortunately, this influence is why unscrupulous advertising companies such as Google target
12 children.
13

14 102. Recognition of the value of children under thirteen as an advertising audience is why
15 Google developed the "honeytrap" DFF program. DFF was designed in response to what Google
16 anticipated would be a reluctance on the part of parents to allow their children to have access to apps on
17 Android devices, because of the ubiquity of surveillance-based ads within the Android ecosystem.
18

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

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

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

27 ³⁸

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

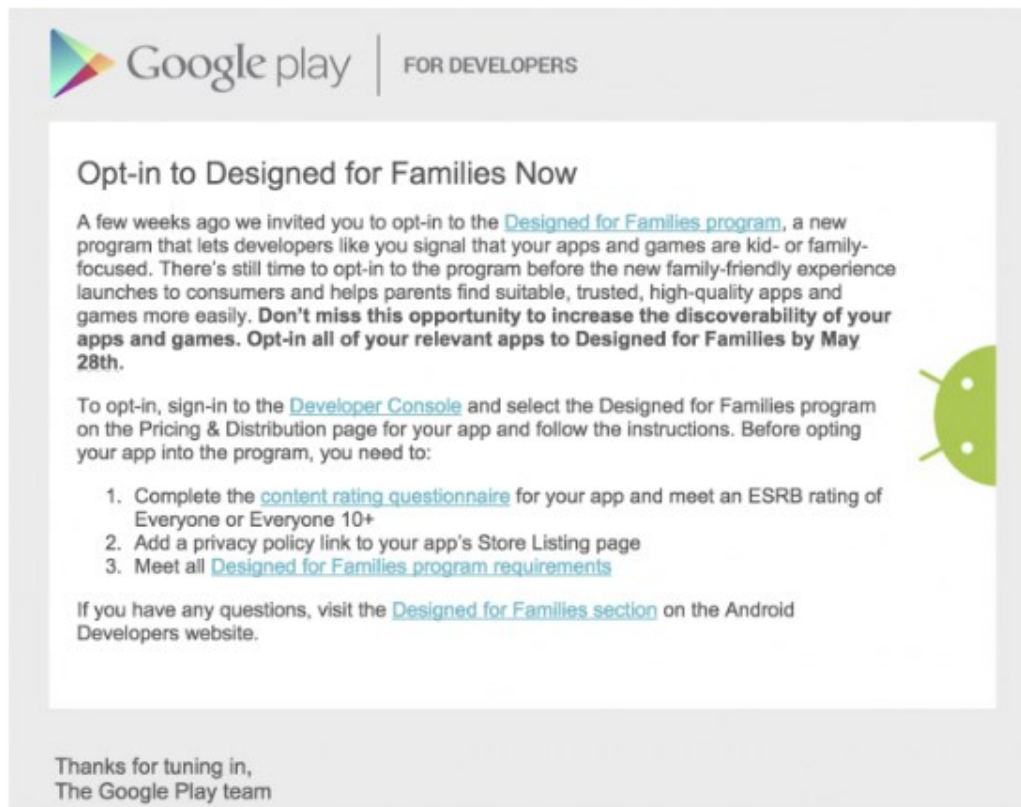
1 104. Google further stated that the DFF program was established in order to “help[]
2 developers connect with families on Google Play” and to “help parents discover great, age-appropriate
3 content and make more informed choices” regarding their children’s Android App use.
4

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

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

- 9 (1) by promising App developers greater visibility (and thus more downloads and users)
10 via the DFF program’s special perks; and
11 (2) providing a way for App developers to monetize those downloads and users.

12 106. For example, shortly after launching the DFF program, Google sent the following email
13 to App developers:
14



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

3 If you've built great apps designed for kids or families, the family discovery experience on
4 Google Play is a great way to surface them to parents.

5 Developers are invited to opt-in these apps and games to the new Designed for Families
6 program. Apps that meet the program requirements will be featured through Google Play's
7 family-friendly browse and search experiences so that parents can find suitable, trusted,
8 high-quality apps and games more easily.

9 Designed for Families expands the visibility of your family content on Google Play,
10 helping parents easily find your family-friendly apps and games throughout the store. Other
11 features create a trusted environment that empowers parents to make informed decisions
12 and engage with your content.³⁹

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

- 15 a. **Search:** Only apps and games opted-in to the Designed for Families program will show up in
16 searches initiated from the Family section in Apps Home. They'll also be more visible when
17 users search for family or kid related content from anywhere in the Play store.
- 18 b. **Browse:** The Family star button on Apps and Games Home points to an enhanced discovery
19 experience for parents looking for family appropriate content. The new Family section
20 includes uniquely merchandised content, new categories, and age-based browsing.
21 Participating apps will receive this additional visibility on top of their existing categories,
22 rankings, and reviews elsewhere on the Google Play store.
- 23 c. **Character pages:** Parents can now discover content for popular characters from around the
24 globe in one place, including apps, games, movies, tv shows, books, and even music. This
25 provides a powerful way for parents to discover content from familiar brands and beloved
26 characters, and allows you to reach a highly relevant and targeted audience.
- 27 d. **Merchandising:** The family sections include their own merchandised collections. The
28 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>

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

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

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

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

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

19 113. Fun Kid Racing was presented to individuals who accessed the Family section of Google
20 Play as follows:
21

22
23
24
25
26
27 _____
40

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Fun Kid Racing

Tiny Lab Racing Games Racing Action & Adventure ★★★★★ 79,707

Everyone

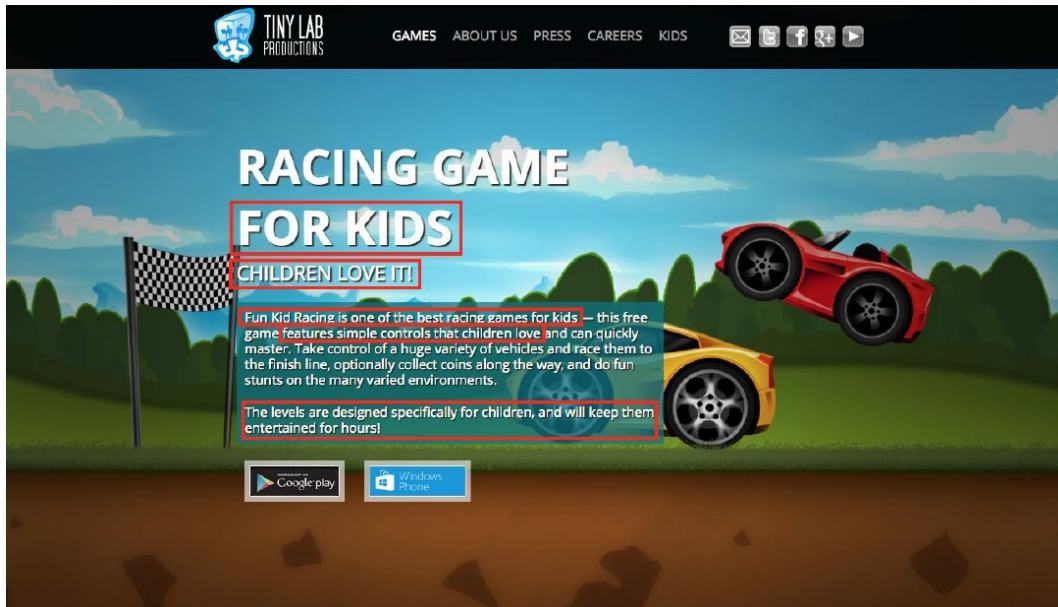
Contains Ads · Offers in-app purchases

Add to Wishlist

Install

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.

1 **B. GOOGLE’S “SPECIFIC BENEFIT” OR “RELEVANT” REQUIREMENTS**
2 **MEANT THAT ALMOST EVERY APP IN THE DFF PROGRAM WAS**
3 **“CHILD-DIRECTED” PURSUANT TO COPPA**

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

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

14 120. Google itself currently summarizes this determination as follows:

15 **What is “made for kids” content?**

16 According to the FTC’s guidance on the Children’s Online Privacy Protection Act (COPPA), [a](#)
17 [video is made for kids](#) [if](#):

- 18 • Children are the primary audience.
19 • Children are not the primary audience, but the video is still directed to children based on
20 factors such as the subject matter of the video, whether the video has an emphasis on kids
21 characters, themes, toys or games, [and more](#) [if](#).

22 Learn more about [determining if your content is “made for kids”](#) [if](#), and check out our
23 [frequently asked questions on the topic](#) [if](#).

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

1 122. According to FTC guidance, even if children are not the primary audience but the website
2 or online service targets children as one of its audiences, the service is “directed to children” under
3 COPPA and compliance is required for children under 13.⁴¹

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

6 123. Google successfully incentivized App developers to create child-directed content. As of
7 March 2018, approximately 5,855 child-directed apps had been voluntarily submitted to and accepted
8 into the DFF program and had achieved a cumulative install count of 4.5 billion installs, an average of
9 approximately 750,000 installs per DFF App.
10

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

14 125. For child-directed content, free-to-play Apps allowing behavioral advertising shown are
15 generally considered the more lucrative option for App developers it avoids the friction of requiring
16 children to ask for money to download and play the app and allows App developers to earn a continuous
17 stream of advertising revenue exceeding a one-time fee.
18

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

21 127. If an App developer categorized an App as “intended primarily for children,” Google
22 would not permit the App to exfiltrate the data of the App’s users and show behavioral advertising to
23 those users, the most lucrative type of advertising for both Defendants and App developers.
24
25
26
27

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

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

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

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

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

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

21 133. Defendants’ conduct is further belied by their dealings with security researchers from the
22 University of California in 2018. According to the Office of the Attorney General for the State of New
23 Mexico (the “NM AG”), in the Spring of 2018, security researchers at the University of California,
24 Berkeley (the “Berkeley Researchers”) informed Defendants of rampant and what the Berkeley
25
26
27
28

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

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

8 Using 84 of Tiny Lab Productions' ("Tiny Lab") apps, with a total of 75,000,000
9 downloads, as a case study: we illustrate how the listing of an app under the "mixed
10 audience" category, could be misleading to consumers and in potential violation of
11 COPPA, despite the representations app developers are making to Google as part of their
12 participation in the DFF program. We further explain how Tiny Lab (and potentially
13 others) employ defective "age gates" in potential violation of COPPA. Moreover, since
14 according to the FTC, "in most instances, a website or online service (such as an app)
15 directed to children must treat all visitors as children and provide COPPA's protections to
16 every such visitor," and given the "child-friendly" nature of DFF, we find it puzzling that
17 more than 50% of our corpus, amounting to thousands of apps, are categorized as so-
18 called "not primarily directed to children." More generally, we explain how Google's
19 DFF terms are contributing to this problem and might be incentivizing developers to
20 potentially abuse DFF and deceive consumers by potentially misrepresenting their apps'
21 true nature and stating they are not primarily directed to children (mixed-audience), when
22 they clearly are.

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

22 135. Again, Google's facile response was intended to evade liability for its unlawful conduct.
23 Further, it betrays Google's pattern of business methods which elevate profits over compliance with the
24 law and societal norms. This is evidenced in part by Google's history of settlements with regulators
25 (and myriad lawsuits) for these types of practices as outlined herein, including the FTC regarding
26 Google's practices in tracking children under 13 for behavioral advertising on Google's YouTube video
27
28

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

3 136. As part of the settlement agreement entered into by Google, AdMob, and the NM AG on
4 December 10, 2021, Google and AdMob agreed to implement the following changes to prevent mis-
5 categorization of DFF Apps as “mixed-audience” or “not primarily intended for children”:
6

7 **Google Play . . . 4.1.1. Policy Changes.** Google has revised its Google Play Families policies,
8 including its “Designing Apps for Children and Families” and “Ads and Monetization” policies .
9 . . . Google will maintain these resources, along with Google Play Academy courses and
10 additional Help Center articles (sample descriptions of which are attached hereto as Exhibit 4) to
11 help app developers create content for children in line with the revised policies.

12 **4.1.2. TAC Form.** Google will require all app developers with active apps on Google Play to
13 complete a Google Play Target Audience and Content (“TAC”) form [. . .] to indicate the
14 targeted age groups of apps submitted to Google Play.

15 **4.1.3. ATK Rubric.** Google will implement, and update as necessary, a rubric with which to
16 evaluate Google Play app submissions to help determine whether an app targets or appeals to
17 kids (“ATK”), independent from an app developer’s TAC submission(s).

18 **4.1.3.1.** This rubric will take into account child-directed popular characters, images, and terms.
19 The rubric will include, inter alia, criteria substantially similar to and consistent with the criteria
20 currently set forth in the “Families” page of the Google Play Academy
21 (<https://play.google.com/console/about/families/>), as well as the developer support page
22 “Manage Target Audience and App Content Settings”
23 (https://support.google.com/googleplay/androiddeveloper/answer/9867159?visit_id=637522057853722464-2168424342&rd=1#age-groups&zippy=%2Cage-and-under%2Cages--). In addition,
24 the State may provide a list of any child-directed characters, images, or terms to be considered
25 for inclusion in this rubric.

26 **4.1.3.2.** In the event that Google determines—via the ATK rubric—that an app may have been
27 misclassified in the TAC submission, Google will require the developer to correct its TAC
28 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.

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

4 138. Of course, had Google and AdMob not been knowingly violating COPPA and the
5 NMUPA by incentivizing App developers to mis-categorize their Apps to exploit children for profit,
6 these mandatory changes would have been unnecessary.
7

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

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

15 140. And worse, where AdMob was one of the SDKs integrated into a DFF App, Google
16 itself, via AdMob, was the one doing the exfiltrating of Personal Information of all users of DFF Apps in
17 which the AdMob SDK was installed, including from children under thirteen.
18

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

22 142. Because Google controlled the DFF program and required the DFF Apps to be child-
23 directed to be included in the DFF program, Google (and thus AdMob) had actual knowledge that the
24 Personal Information of DFF App users under thirteen was being collected.
25

26 143. Despite Defendants’ actual knowledge that the core audience and/or user base of DFF
27 Apps consisted of children under thirteen, Defendants exfiltrated the data of *every* DFF App user as long
28

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

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

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

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

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

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

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

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

- 23 a. **Android Advertising ID (“AAID”)**: An AAID is a unique identifier assigned to an
24 Android device by Google. The AAID is used to exfiltrate user data and deliver
25 behavioral advertising based on that data.
26
27
28

- 1 b. **International Mobile Equipment Identity (“IMEI”)**: is a unique identification
2 number assigned to every mobile device, including smartphones and tablets. The
3 IMEI is a 15-digit number that is used to identify the device and its capabilities on a
4 mobile network. IMEI serves as a device’s fingerprint and can be used to track and
5 identify it if it’s lost or stolen. It cannot be reset by a user.
- 6 c. **Device IP Address**: An IP address, or Internet Protocol address, is a unique
7 numerical identifier that is assigned to devices that are connected to a network that
8 uses the Internet Protocol for communication. This address is used to identify and
9 communicate with devices on the network, much like a telephone number is used to
10 identify and connect with a person on a telephone network. Thus, recording the IP
11 address of child’s device means that Google can identify and locate that child on the
12 internet and across multiple devices via the IP address.
- 13 d. **Device Manufacturer, make, and model**: The AdMob SDK exfiltrated the device
14 manufacturer, the type of device and model number and combined this with other
15 data points to track users across Apps and platforms and serve them with behavioral
16 advertising.
- 17 e. **Device Operating System**: AdMob exfiltrated the operating system running on a
18 device down to the version that was running on the user’s device. When paired with
19 other persistent identifiers, this information allows AdMob to track the user across
20 Apps.

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

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

27 152. Google, via AdMob, collected this information despite having actual knowledge that the
28 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>

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

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

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

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

19 158. As Google and AdMob's settlement with the NM AG makes clear, Google and AdMob's
20 practices with respect to the DFF program not only violate COPPA, but also independently violate the
21 state statutes prohibiting unfair and deceptive business practices modeled or patterned after, and/or
22 which take interpretive guidance from, the FTC Act (the "Little FTC Acts"), including those enacted by
23 California, Florida, and New York.
24
25
26
27
28

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

4 160. Defendants operate the first and second-most visited websites in the world and the most
5 popular mobile operating system in the world. As a result of their unlawful conduct, Defendants’
6 algorithms now incorporate ill-gotten data gleaned from billions of instances of children’s online
7 activity. The deep insights gleaned from these viewing sessions will enable the Defendants to keep
8 children using Apps and will solidify the Defendants’ dominance in the market for child-related content.
9

10
11 **V. DEFENDANTS’ TRACKING, PROFILING, TARGETING AND EXPLOITATION OF**
12 **CHILDREN WITHOUT PARENTAL CONSENT VIOLATED PLAINTIFFS’ AND**
13 **CLASS MEMBERS’ REASONABLE EXPECTATIONS OF PRIVACY AND IS HIGHLY**
14 **OFFENSIVE**

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

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

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

25 164. In fact, as discussed above, the FTC’s enhancements of COPPA in 2013 reflect the
26 specific concern with mobile app tracking and reflect the offensiveness with which society regards this
27 behavior.
28

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

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

6 167. Nearly all parents in the United States (94%) say their children under 13 use online apps,
7 with top apps used being video streaming (64%), video gaming (58%) and show/movie streaming
8 (58%).⁴⁵

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

11 169. Nearly 3 in 4 parents whose children under 13 use online apps (73%) say they are
12 concerned about their children's location being tracked by those apps; those residing in urban or rural
13 areas are more likely than those residing in suburban areas to share this sentiment (88% and 87% vs.
14 73%).⁴⁸

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

17
18
19
20
21
22
23 ⁴³ <https://www.common sense media.org/press-releases/new-research-by-common-sense-finds-major-spike-in-mobile-media-use-and-device-ownership-by-children-age>.

24 ⁴⁴ Dangers of YouTube for Kids, THE ATLANTIC (Nov. 2018), <https://www.theatlantic.com/magazine/archive/2018/11/raised-by-youtube/570838/>.

25 ⁴⁵ <https://www.pixalate.com/blog/childrens-online-privacy-harris-poll-recap>.

26 ⁴⁶ *Id.*

27 ⁴⁷ <https://www.cdpinstitute.org/news/childrens-privacy-data-tracking-is-a-big-concern-for-parents-and-trust-levels-in-companies-are-low/>.

28 ⁴⁸ <https://www.pixalate.com/blog/childrens-online-privacy-harris-poll-recap>.

⁴⁹ <https://trustedfuture.org/childrens-digital-privacy-and-safety>.

1 171. 73% of parents are concerned about personal data being collected by third parties,
2 without their consent.⁵⁰

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

5 173. Additionally, a survey conducted by the Center for Digital Democracy (“CDD”) and
6 Common Sense Media of more than 2,000 adults found overwhelming support for the basic principles of
7 privacy embedded in federal law and state common law.⁵² The parents who were polled responded as
8 follows when asked whether they agreed or disagreed with the following statements:
9

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

- 12 a. 5 percent strongly agree
- 13 b. 3 percent somewhat agree
- 14 c. 15 percent somewhat disagree
- 15 **d. 75 percent strongly disagree**
- 16 e. 3 percent do not know or refused to answer

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

- 19 a. 3 percent strongly agree.
- 20 b. 17 percent somewhat agree.
- 21 c. 10 percent somewhat disagree

22
23
24
25
26 _____
27 ⁵⁰ *Id.*

28 ⁵¹ *Id.*

⁵² *See, e.g.,*

<https://www.democraticmedia.org/sites/default/files/COPPA%20Executive%20Summary%20and%20Findings.pdf>.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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.

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

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

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

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

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

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

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

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

22 187. To enhance retention, AdMob uses the Personal Information of children under thirteen,
23 analyzes their behavior, and uses trigger events—both within the Apps and across the Internet—that will
24 encourage them to play the Apps more often and for longer periods.
25
26
27
28

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

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

5 190. By failing to (1) obtain parental consent, (2) disclose to parents the nature of their data
6 collection practices, and (3) take other steps to preclude the capture of children's Personal Information,
7 Defendants have breached the privacy rights and reasonable expectations of privacy of Plaintiffs and the
8 millions of other minors who used DFF Apps and were shown behavioral advertisements in
9 contravention of privacy norms that are reflected in consumer surveys, centuries of common law, state
10 and federal statutes, legislative commentaries, industry standards and guidelines, and scholarly
11 literature.
12
13

14 **V. VALUE OF PERSONAL INFORMATION**

15 191. Plaintiffs and the Classes and Subclasses have been deprived of, and thereby lost, the
16 economic value of their Personal Information. There is a market for this Personal Information. As the
17 advertising revenue figures outlined herein demonstrate, this information has tremendous value to
18 Google, AdMob and the App developers who share in the advertising revenue. On the open market, PII
19 is often mined, compiled, and resold by data brokers.⁵³ Further, there is a market for consumers to
20 monetize Personal Information and the behavioral preferences that Defendants have usurped. Multiple
21 published analyses and studies have placed a value in excess of \$200 on an individual's Personal
22 Information;⁵⁴ for example, one individual sold his data for \$2,733 on Kickstarter.⁵⁵ Surveys have
23
24
25

26 ⁵³ <https://www.visualcapitalist.com/much-personal-data-worth/>.

27 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>

28 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>.

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

3 192. A child's Personal Information has equivalent (or potentially greater) value than that of
4 an adult to companies like Google. As described above, a child is more susceptible to being influenced
5 by advertisements as they often cannot tell the difference between content and advertisements. In
6 addition, Google and AdMob may be able to utilize children's Personal Information to show them
7 behavioral advertising for the duration of their lives. Plaintiffs and the Classes and Subclasses can no
8 longer realize the full economic value of their Personal Information because their Personal Information
9 has already been collected, analyzed, acted upon, and monetized by Defendants.
10

11 VI. ALLEGATIONS RELATING TO PLAINTIFFS

12 A. PLAINTIFF A.B.

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

14 194. A.B. used monetized Android Apps included in the DFF program, including Fun Kid
15 Racing and Monster Truck Racing.
16

17 195. Defendants (and App developers) collected and enabled collection of A.B.'s Personal
18 Information for the purposes of tracking, profiling, and targeting A.B. with advertisements as he used
19 the Android Apps.
20

21 196. Neither the Defendants nor the App developers obtained verifiable parental consent prior
22 to the collection of A.B.'s Personal Information.
23

24 197. Neither Plaintiff A.B. nor his parent and guardian Jen Turner could have reasonably
25 discovered this conduct earlier through investigation. Plaintiff A.B. is a minor unable to consent to or
26

27
28

⁵⁶ <https://simpletexting.com/personal-data-value/>.

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

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

5
6 **B. PLAINTIFFS C.D.1, C.D.2, AND C.D.3**

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

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

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

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

16 203. Neither Plaintiffs C.D.1, C.D.2, and C.D.3 nor their parent and guardian Kirenda Johnson
17 could have reasonably discovered this conduct earlier through investigation. Plaintiffs C.D.1, C.D.2, and
18 C.D.3 are minors unable to consent to or understand Defendants' tracking of personal information, and
19 Defendants concealed their tracking, profiling, and targeting of C.D.1, C.D.2, and C.D.3.
20

21 204. The tracking, profiling, and targeting of C.D.1, C.D.2, and C.D.3 without parental
22 consent by the Defendants and these App developers is highly offensive and constitutes an invasion of
23 C.D.1's, C.D.2's, and C.D.3's privacy.
24

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

26 205. At all relevant times, Plaintiffs E.F.1 and E.F.2 used Android Apps included in the DFF
27 program.
28

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

3 207. Defendants (and App developers) collected and enabled collection of E.F.1's and E.F.2's
4 Personal Information for the purposes of tracking, profiling, and targeting E.F.1 and E.F.2 with
5 advertisements as he used the Android Apps.
6

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

9 209. Neither Plaintiffs E.F.1 and E.F.2 nor their parent and guardian Barbara Hayden-Seaman
10 could have reasonably discovered this conduct earlier through investigation. Plaintiffs E.F.1 and E.F.2
11 are minors unable to consent to or understand Defendants' tracking of personal information, and
12 Defendants concealed their tracking, profiling, and targeting of E.F.1 and E.F.2.
13

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

TOLLING AND ESTOPPEL

I. DISCOVERY RULE TOLLING

17
18
19 211. Plaintiffs, the Classes, and the Subclasses had no way of knowing about Defendants'
20 conduct with respect to the collection and impermissible and unauthorized use of, and profit from, the
21 Personal Information of Plaintiffs and the members of the Classes and Subclasses.
22

23 212. Neither Plaintiffs nor any other members of the Classes and Subclasses, through the
24 exercise of reasonable diligence, could have discovered the conduct alleged herein. Further, Plaintiffs
25 and the members of the Classes and Subclasses did not discover, and did not know of, facts that would
26 have caused a reasonable person to suspect, that Defendants were engaged in the conduct alleged herein.
27
28

1 **II. FRAUDULENT CONCEALMENT TOLLING**

2 213. By failing to provide notice of the collection and use of the Personal Information and
3 obtain verifiable consent, in violation of COPPA and societal norms and conventions, Defendants
4 concealed their conduct and the existence of the claims asserted herein from Plaintiff and the members
5 of the Classes and Subclasses.
6

7 214. Upon information and belief, Defendants intended by their acts to conceal the facts and
8 claims from Plaintiffs and members of the Classes and Subclasses. Plaintiffs and the members of the
9 Classes and Subclasses were unaware of the facts alleged herein without any fault or lack of diligence
10 on their part and could not have reasonably discovered Defendants' conduct. For this reason, any statute
11 of limitations that otherwise may apply to the claims of Plaintiff or members of the Classes and
12 Subclasses should be tolled.
13

14 **III. ESTOPPEL**

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

18 216. Defendants are therefore estopped from relying on any statutes of limitations in defense
19 of this action.
20

21 **CLASS ACTION ALLEGATIONS**

22 217. Plaintiffs bring this action as a class action pursuant to Federal Rules of Civil Procedure
23 23(a), 23(b)(2), and 23(b)(3).
24

25 218. 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
26 and guardians, seek certification of a claim for violation of the California Unfair Competition Law, Cal.
27 Bus. & Prof. Code § 17200, *et seq.*, on behalf of a class defined as follows:
28

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

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

7 **The Intrusion Upon Seclusion Class:** all persons residing in the States of Alabama,
8 Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia,
9 Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota,
10 Missouri, Nevada, New Hampshire, New Jersey, North Carolina, Ohio, Oklahoma,
11 Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West
12 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.

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

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

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

24 **The Florida Subclass:** all persons residing in the State of Florida who were younger than
25 the age of 13 when they used the Android Apps, and from whom Defendants collected,
26 used, or disclosed Personal Information without first obtaining verified parental consent
27 during the applicable statute of limitations period.
28

1 222. Plaintiffs E.F.1 and E.F.2, by and through their parent and legal guardian, seek
2 certification of a claim for violations of NY Gen. Bus. Law § 349, as well as Unjust Enrichment, on
3 behalf of a New York Subclass defined as follows:
4

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

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

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

21 225. **Numerosity (Rule 23(a)(1)).** The Classes and Subclasses are so numerous that joinder of
22 individual members herein is impracticable. The exact number of Classes or Subclass members, as herein
23 identified and described, is not known, but App download and usage figures indicate that Defendants
24 have collected information on millions of children (if not more).
25

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- 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;

- 1 o. Whether Defendants were unjustly enriched by their conduct;
- 2 p. Whether Defendants' fraudulently concealed their conduct; and
- 3 q. Whether Plaintiffs and the Classes and Subclasses are entitled to injunctive or other
- 4 equitable relief.

5
6 227. **Typicality (Rule 23(a)(3)).** Plaintiffs' claims are typical of the claims of the other
7 members of the proposed Classes and Subclasses. Plaintiffs and members of the Classes and Subclasses
8 suffered an invasion of privacy as a result of Defendants' wrongful conduct that is uniform across the
9 Classes and Subclasses.

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

17
18 229. **Substantial Benefits.** This class action is appropriate for certification because class
19 proceedings are superior to other available methods for the fair and efficient adjudication of this
20 controversy and joinder of all members of the Classes and Subclasses is impracticable. The prosecution
21 of separate actions by individual members of the Classes and Subclasses would impose heavy burdens
22 upon the Courts and defendants, would create a risk of inconsistent or varying adjudications of the
23 questions of law and fact common to members of the Classes and Subclasses, and would be dispositive
24 of the interests of the other members not parties to the individual adjudications or would substantially
25 impair or impede their ability to protect their interests. This proposed class action presents fewer
26 management difficulties than individual litigation and provides the benefits of single adjudication,
27
28

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

3 230. Plaintiffs reserve the right to revise the foregoing class allegations and definitions of the
4 Classes and Subclasses based on new information learned and legal developments following additional
5 investigation, discovery, or otherwise, and/or in order to accommodate any of the Court’s manageability
6 concerns.
7

8 **CLAIMS FOR RELIEF**

9 **FIRST CLAIM FOR RELIEF**

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

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

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

22 233. As outlined herein, Defendants at all times had actual knowledge that the Android Apps
23 were not compliant with the guidelines and requirements in Google’s DFF program, which mandated
24 adherence to COPPA and other applicable privacy-related laws. Further, Defendants at all times had
25 actual knowledge and specifically intended that the AdMob SDKs embedded in the Android Apps
26 enabled and effectuated the exfiltration of Personal Information from Plaintiffs and children under 13
27
28

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

3 234. In addition, as outlined herein, Google broadly promoted, marketed, and represented in
4 numerous ways that the DFF program and the Apps included in the program were suitable and safe and
5 designed for children and legally compliant, including in public-facing websites, privacy policies and
6 program requirements, marketing materials, App interfaces, and other public statements and materials,
7 and internally acknowledged and advised its App developer partners the same. For example:
8

9 The DFF program had a “strict legal and policy bar,” requiring that Apps displaying ads “comply
10 with all legal obligations relating to advertising to children,” “Ads displayed to child audiences
11 do not involve interest-based advertising,” Apps submitted to the DFF program were “compliant
12 with COPPA and other relevant statutes,” and that “Ads displayed to child audiences must
13 comply with laws relating to advertising to kids,” and the App “must disable interest-based
14 advertising;”

15 Google warned that non-compliance with DFF guidelines and requirements could result in
16 expulsion of the App from the DFF program;

17 Google stated that DFF was designed to be “inclusive of apps that are made for kids,” and that
18 “apps that have no specific benefit or relevance for audiences under the age of thirteen will not
19 be accepted into the program;”

20 Google stated that “Apps that meet the [DFF] program requirements will be featured through
21 Google Play's family-friendly browse and search experiences so that parents can find suitable,
22 trusted, high-quality apps and games more easily.”

23 Google stated that the DFF program “helps parents easily find your family-friendly apps and
24 games” and “create[s] a trusted environment that empowers parents to make informed decisions
25 and engage with [App developer] content.”

26 The DFF program provided privileges to DFF Apps/games that opted in to DFF, touting that
27 only those Apps/games “[would] show up in searches initiated from the family section in Apps
28 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.”

1 235. In addition, the Android Apps were child-directed as defined under COPPA. Given the
2 inherent characteristics, content, and features of the Android Apps offered and available in the DFF
3 program in the Google Play Store, including the names, designs, cartoon elements, and children’s
4 themes and songs, were plainly intended for and meant to attract children and, in particular, children
5 under 13, through which Defendants intended to and did collect Personal Information to serve these
6 children behavioral advertising for substantial commercial gain. And, in fact, Defendants, “operators”
7 as defined under COPPA and FTC regulations, collected Personal Information from children under 13
8 through the Android Apps, which were directed to children.
9

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

14 a. Failing to provide sufficient notice of the information Defendants collected, or the information
15 that was collected on Defendants’ behalf, online from children under 13, how Defendants used
16 such information, their disclosure practices, and all other required content, in violation of Section
17 312.4(d) of COPPA, 16 C.F.R. § 312.4(d);

18 b. Failing to provide direct notice to parents of the information Defendants collected, or the
19 information that was collected on Defendants’ behalf, online from children under 13, how
20 Defendants used such information, their disclosure practices, and all other required content, in
21 violation of Section 312.4(b) and (c) of COPPA, 16 C.F.R. § 312.4(b)-(c);

22 c. Failing to obtain verifiable parental consent before any collection or use of Personal
23 Information from children under 13, in violation of Section 312.5 of COPPA, 16 C.F.R. § 312.5;
24 and

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

28 237. 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

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

3 238. Accordingly, Defendants engaged in business acts and practices deemed “unlawful”
4 under the UCL predicated on their violations of COPPA and the FTC regulations. For the same reasons
5 and based on Defendants’ unlawful tracking, targeting, and profiling of Plaintiffs and UCL Class and
6 California Subclass Members without obtaining parental consent, defendants engaged in business acts
7 and practices deemed “unlawful” in violation of state common laws protecting invasion of privacy and
8 prohibiting intrusion upon seclusion and the California Constitutional Right to Privacy, Cal. Const. Art.
9 1, § 1.
10

11 239. Defendants also engaged in business acts or practices deemed “unfair” under the UCL,
12 because, as outlined herein, Defendants failed to disclose that they were tracking, profiling, and
13 targeting children, including Plaintiffs and UCL Class and California Subclass Members, through the
14 collection of Personal Information, and that they were profiting from this conduct through behavioral
15 (interest-based) advertising. Unfair acts under the UCL have been interpreted using three different tests:
16 (1) whether the public policy which is a predicate to a consumer unfair competition action under the
17 unfair prong of the UCL is tethered to specific constitutional, statutory, or regulatory provisions;
18 (2) whether the gravity of the harm to the consumer caused by the challenged business practice
19 outweighs the utility of the defendant’s conduct; and (3) whether the consumer injury is substantial, not
20 outweighed by any countervailing benefits to consumers or competition, and is an injury that consumers
21 themselves could not reasonably have avoided.
22
23

24 240. Defendants’ conduct is unfair under each of these tests. As outlined herein, Defendants’
25 conduct violates COPPA and FTC regulations and the policies underlying privacy laws. The gravity of
26

27
28 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.”).

1 the harm of Defendants’ secret tracking, profiling, and targeting of children is significant and there is
2 no corresponding benefit to consumers or competition from Defendants’ conduct. Finally, because
3 Plaintiffs and UCL Class and California Subclass Members were minors unable to consent to or
4 understand Defendants’ conduct—and because their parents and guardians did not consent to this
5 conduct and were misled by their belief that Defendants would follow applicable laws and societal
6 expectations about children’s privacy as well as Defendants’ statements, policies, and promotion—they
7 could not have avoided the harm.
8

9 241. The parents and guardians of Plaintiffs and the members of the UCL Class and California
10 Subclass reasonably expected that Defendants would respect children’s privacy online, in accordance
11 with their own policies and guidelines, statements, and representations, societal expectations and public
12 policy, as well as state and federal statutes and regulations including COPPA and Federal Trade
13 Commission regulations. As outlined herein, the Android App games are marketed, promoted, and
14 represented as safe and suitable for children, predicated on, *inter alia*, (i) their offering and availability
15 and promotion and marketing in the DFF program in the Family section of the Google Play Store and
16 the representations and statements concerning the DFF program and the Family section of the Google
17 Play Store, (ii) the public statements marketing and promoting the games as suitable and appropriate for
18 children by the Android App developers, and (iii) the inherent characteristics, content, and features of
19 Android App games, which were designed for children.
20
21

22 242. At the same time, Defendants have (i) at all relevant times known that children under the
23 age of 13 use the Android Apps, (ii) actively sought to increase use of the Apps by these children, and
24 (iii) sought to exploit, for commercial purposes and gain, the millions of children under the age of 13
25 using the Android Apps. Defendants’ knowledge of the widespread use of the Apps by children (which
26 Defendants have expressly touted in their advertising sales efforts) and their concealment and failure to
27 disclose the exfiltration of Personal Information from such children and that they were tracking,
28

1 profiling, and targeting these children and/or profiting from this conduct through lucrative behavioral
2 advertising, while promoting, representing, and purporting to ensure that the Android Apps comply with
3 law and societal expectation, are likely to and, in fact, did deceive Plaintiffs and members of the UCL
4 Class and California Subclass and their parents or guardians. Defendants' conduct therefore constitutes
5 deceptive business practices in violation of the UCL.
6

7 243. Defendants' misrepresentations and omissions were explicit and implicit. Defendants'
8 representations and omissions were material because they were likely to deceive reasonable consumers
9 such as the parents or guardians of Plaintiffs and UCL Class and California Subclass Members about the
10 terms under which their children were using the Apps as well as the fact that Defendants were collecting
11 and profiting from the Personal Information of children under the age of thirteen without their parents
12 and guardians' knowledge or consent.
13

14 244. Defendants had a duty to disclose the above-described facts due to the important public
15 interest in securing the privacy of young children's Personal Information and the fact that young
16 children are unable to fully protect their own interests. Parents and guardians of Plaintiffs and UCL
17 Class and California Subclass Members placed trust in Defendants as reputable companies which
18 represent that they comply with applicable laws and societal interests in safeguarding children's
19 Personal Information. Additionally, Defendants exclusively knew and understood the extent of their
20 collection of Personal Information, and the parents or guardians of Plaintiffs and UCL Class and
21 Subclass Members could not reasonably have discovered—and were unaware of—Defendants' secret
22 tracking, profiling, and targeting.
23

24 245. Defendants invaded Plaintiff's and UCL Class and California Subclass Members' privacy
25 without their or their parents and guardians' consent.
26
27
28

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

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

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

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

22 250. Defendants’ monetization of the Plaintiffs’ and UCL Class and California Subclass
23 Members’ Personal Information demonstrates that there is a market for their Personal Information.
24
25
26
27
28

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

3 252. Plaintiffs’ and the UCL Class and California Subclass Members’ injury was the direct
4 and proximate result of Defendants’ conduct described herein. The Defendants’ retention of UCL Class
5 and California Subclass Members’ Personal Information presents a continuing risk to them as well as the
6 general public.
7

8 253. Plaintiffs, individually and on behalf of the UCL Class and California Subclass, seek: (1)
9 an injunction requiring Defendants to permanently delete, destroy or otherwise sequester the Personal
10 Information collected without parental consent, requiring Defendants to provide a complete audit and
11 accounting of the uses of the Personal Information by Defendants, App developers and any other third
12 parties, and other appropriate injunctive relief; (2) compensatory restitution of Plaintiffs’ and the UCL
13 Class and California Subclass Members’ money and property lost as a result of Defendants’ acts of
14 unfair competition; (3) disgorgement of Defendants’ profits and unjust gains; and (4) reasonable
15 attorney’s fees (pursuant to Cal. Code of Civ. Proc. § 1021.5).
16

17 **SECOND CLAIM FOR RELIEF**

18 **INTRUSION UPON SECLUSION**

19 **(Brought on Behalf of Plaintiff A.B. and the Intrusion Upon Seclusion Class Against All**
20 **Defendants)**

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

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

25 256. The parents and guardians of Plaintiff A.B. and members of the Intrusion Upon
26 Seclusion Class have reasonable expectations of privacy in their mobile devices and their online
27 behavior, generally. As outlined herein, these expectations stemmed from Google’s policies and
28

1 guidelines, statements, and representations, societal expectations, and public policy, as well as state and
2 federal statutes and regulations including COPPA and Federal Trade Commission regulations. Further,
3 these expectations stemmed from the fact that the Android App games are marketed, promoted, and
4 represented as safe and suitable for children, predicated on, *inter alia*, (i) their offering and availability
5 and promotion and marketing in the DFF program in the Family section of the Google Play Store and
6 the representations and statements concerning the DFF program and the Family section of the Google
7 Play Store, (ii) the public statements marketing and promoting the games as suitable and appropriate for
8 children by the Android App developers, and (iii) the inherent characteristics, content, and features of
9 Android App games, which were designed for children. The expectations of the parents and guardians
10 of Plaintiff A.B. and members of the Intrusion Upon Seclusion Class includes that the Defendants
11 would not track their children's activity across the Internet and exfiltrate their Personal Information,
12 without consent, in order for the Defendants to earn substantial profits through targeted behavioral
13 advertising.
14

15
16 257. As children under the age of 13, Plaintiff A.B. and the members of the Intrusion Upon
17 Seclusion Class lacked the ability to form expectations about reasonable privacy or to consent to
18 Defendants' actions.

19
20 258. Defendants intentionally intruded on and into Plaintiff A.B.'s and the Intrusion Upon
21 Seclusion Class members' solitude, seclusion, or private affairs by intentionally and surreptitiously
22 obtaining, improperly gaining knowledge of, reviewing, and/or retaining Plaintiff A.B.'s and the
23 Intrusion Upon Seclusion Class members' activities (and Personal Information) through the collection,
24 monitoring, and tracking activities described herein.

25
26 259. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter*
27 *alia*, countless consumer surveys, studies, and op-eds decrying the online tracking of children, centuries
28 of common law, state and federal statutes and regulations including COPPA and FTC regulations,

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

3 260. These societal expectations and laws created a duty that Defendants owed to Plaintiff
4 A.B. and the members of the Intrusion Upon Seclusion Class. Defendants breached that duty by
5 tracking and monitoring children and profiting from the behavioral advertising served to them.
6

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

10 262. Plaintiff A.B. and the members of the Intrusion Upon Seclusion Class were harmed by the
11 intrusion into their private affairs as outlined in detail in this Complaint. Defendants' actions and conduct
12 complained of herein were a substantial factor in causing the harm suffered by Plaintiff A.B. and
13 members of the Intrusion Upon Seclusion Class.
14

15 263. Plaintiff A.B. and members of the Intrusion Upon Seclusion Class therefore seek (1) an
16 injunction requiring Defendants to permanently delete, destroy or otherwise sequester the Personal
17 Information collected without parental consent, requiring Defendants to provide a complete audit and
18 accounting of the uses of the Personal Information by Defendants, App developers and any other third
19 parties, and other appropriate injunctive relief; and (2) compensatory and punitive damages in an amount
20 to be determined at trial. Plaintiff A.B. and Intrusion Upon Seclusion Class members seek punitive
21 damages because Defendants' actions—which were malicious, oppressive, willful—were calculated to
22 injure Plaintiff A.B. and Intrusion Upon Seclusion Class members and made in conscious disregard of
23 Plaintiff A.B.'s and Intrusion Upon Seclusion Class members' rights. Punitive damages are warranted to
24 deter Defendants from engaging in future misconduct.
25
26
27
28

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.

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

2 272. Plaintiff A.B. and the California Subclass members are entitled to restitution,
3 disgorgement, and/or the imposition of a constructive trust to recover the amount of Defendants' ill-
4 gotten gains, and/or other sums as may be just and equitable.
5

6 **FOURTH CLAIM FOR RELIEF**

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

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

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

10 274. Plaintiff A.B.'s and the California Subclass Members' private affairs include their
11 behavior on their mobile devices and computers, as well as any other online behavior that may be
12 monitored by the surreptitious tracking employed or otherwise enabled by Defendants.
13

14 275. The parents and guardians of Plaintiff A.B. and the California Subclass Members have
15 reasonable expectations of privacy in their children's mobile devices and their online behavior and
16 activities, generally. As outlined herein, these expectations stemmed from Google's policies and
17 guidelines, statements, and representations, societal expectations, and public policy, as well as state and
18 federal statutes and regulations including COPPA and Federal Trade Commission regulations. Further,
19 these expectations stemmed from the fact that the Android App games are marketed, promoted, and
20 represented as safe and suitable for children, predicated on, *inter alia*, (i) their offering and availability
21 and promotion and marketing in the DFF program in the Family section of the Google Play Store and
22 the representations and statements concerning the DFF program and the Family section of the Google
23 Play Store, (ii) the public statements marketing and promoting the games as suitable and appropriate for
24 children by the Android App developers, and (iii) the inherent characteristics, content, and features of
25 Android App games, which were designed for children. The expectations of the parents and guardians
26 of Plaintiff A.B. and members of the Intrusion Upon Seclusion Class includes that the Defendants would
27
28

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

3 276. As minor children, Plaintiff A.B. and California Subclass Members lack the ability to
4 form expectations about reasonable privacy or to consent to Defendants’ actions. Plaintiff A.B. and
5 California Subclass Members rely on their parents for such determinations.
6

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

11 278. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter*
12 *alia*, countless consumer surveys, studies, and op-eds decrying the online tracking of children, centuries
13 of common law, state and federal statutes and regulations, legislative commentaries, enforcement
14 actions undertaken by the FTC, industry standards and guidelines, and scholarly literature on
15 consumers’ reasonable expectations.
16

17 279. These societal expectations and laws created a duty that Defendants owed to Plaintiff
18 A.B. and California Subclass Members. Defendants breached that duty by tracking and monitoring
19 children, and Defendants breached that duty by profiting from the behavioral advertising served to them.
20

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

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

26 282. Plaintiff A.B. and the California Subclass Members were harmed by the intrusion into
27 their private affairs as outlined in detail in this Complaint. Defendants’ actions and conduct complained
28

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

3 283. Plaintiff A.B. and members of the California Subclass therefore seek (1) an injunction
4 requiring Defendants to permanently delete, destroy or otherwise sequester the Personal Information
5 collected without parental consent, requiring Defendants to provide a complete audit and accounting of
6 the uses of the Personal Information by Defendants, App developers and any other third parties, and
7 other appropriate injunctive relief; and (2) compensatory and punitive damages in an amount to be
8 determined at trial. Plaintiff A.B. and the California Subclass members seek punitive damages because
9 Defendants' actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff
10 A.B. and California Subclass members and made in conscious disregard of the rights of Plaintiff A.B.
11 and California Subclass members. Punitive damages are warranted to deter Defendants from engaging in
12 future misconduct.
13

14 **FIFTH CLAIM FOR RELIEF**

15 **FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT**

16 **Fla. Stat. § 501.201, *et seq.***

17 **(Brought on behalf of Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass against all**
18 **Defendants)**

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

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

23 286. Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass Members are “consumers,”
24 as defined by Fla. Stat. § 501.203(7) and the conduct at issue was within “trade or commerce” as
25 defined by Fla. Stat. § 501.203(8), in that Defendants advertised, offered for sale, sold or distributed
26 goods or services, or any property whether tangible or intangible, or any other article, commodity or
27
28

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

3 287. FDUTPA, Fla. Stat. § 501.204 provides that “[u]nfair methods of competition,
4 unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or
5 commerce are hereby declared unlawful.”
6

7 288. Defendants at all relevant times knowingly violated legal duties and public policy by
8 collecting the Personal Information of children under 13 and tracking, profiling, and targeting those
9 children with behavioral advertising for Defendants’ financial gain. As outlined herein, Defendants at
10 all times had actual knowledge that the Android Apps were not compliant with the guidelines and
11 requirements in Google’s DFF program, which mandated adherence to COPPA and other applicable
12 privacy-related laws. Further, Defendants at all times had actual knowledge and specifically intended
13 that the AdMob SDKs embedded in the Android Apps enabled and effectuated the exfiltration of
14 Personal Information from Plaintiffs and children under 13 using the Android Apps and the tracking,
15 profiling, and targeting of those children for lucrative behavioral advertising.
16

17 289. As outlined herein, Google broadly promoted, marketed, and represented in numerous
18 ways that the DFF program and the Apps included in the program as suitable and safe and designed for
19 children and legally compliant, including in public-facing websites, privacy policies and program
20 requirements, marketing materials, App interfaces, and other public statements and materials, and
21 internally acknowledged and advised its App developer partners the same. For example:
22

23 The DFF program had a “strict legal and policy bar,” requiring that Apps displaying ads “comply
24 with all legal obligations relating to advertising to children,” “Ads displayed to child audiences
25 do not involve interest-based advertising,” Apps submitted to the DFF program were “compliant
26 with COPPA and other relevant statutes,” and that “Ads displayed to child audiences must
27 comply with laws relating to advertising to kids,” and the App “must disable interest-based
28 advertising;”

Google warned that non-compliance with DFF guidelines and requirements could result in
expulsion of the App from the DFF program;

1 Google stated that DFF was designed to be “inclusive of apps that are made for kids,” and that
2 “apps that have no specific benefit or relevance for audiences under the age of thirteen will not
3 be accepted into the program;”

4 Google stated that “Apps that meet the [DFF] program requirements will be featured through
5 Google Play's family-friendly browse and search experiences so that parents can find suitable,
6 trusted, high-quality apps and games more easily.”

7 Google stated that the DFF program “helps parents easily find your family-friendly apps and
8 games” and “create[s] a trusted environment that empowers parents to make informed decisions
9 and engage with [App developer] content.”

10 The DFF program provided privileges to DFF Apps/games that opted in to DFF, touting that
11 only those Apps/games “[would] show up in searches initiated from the family section in Apps
12 Home,” and be “more visible” when “users search for family or kids related content from
13 anywhere in the [Google] Play store.”

14 The DFF program implemented a “Family star button on Apps and Games Home point[ed] to an
15 enhanced discovery experience for parents looking for family appropriate content,” and “Apps
16 participating in [DFF] are marked with the family star badge, which reflects the target age you
17 select for your apps and serves as a signal of quality for parents.”

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

23 291. In addition, the Android Apps were child-directed as defined under COPPA. Given the
24 inherent characteristics, content, and features of the Android Apps offered and available in the DFF
25 program in the Google Play Store, including the names, designs, cartoon elements, and children’s
26 themes and songs, were plainly intended for and meant to attract children and, in particular, children
27 under 13, through which Defendants intended to and did collect Personal Information to serve these
28 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.

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

4 a. Failing to provide sufficient notice of the information Defendants collected, or the information
5 that was collected on Defendants' behalf, online from children under 13, how Defendants used
6 such information, their disclosure practices, and all other required content, in violation of Section
7 312.4(d) of COPPA, 16 C.F.R. § 312.4(d);

8 b. Failing to provide direct notice to parents of the information Defendants collected, or the
9 information that was collected on Defendants' behalf, online from children under 13, how
10 Defendants used such information, their disclosure practices, and all other required content, in
11 violation of Section 312.4(b) and (c) of COPPA, 16 C.F.R. § 312.4(b)-(c);

12 c. Failing to obtain verifiable parental consent before any collection or use of Personal
13 Information from children under 13, in violation of Section 312.5 of COPPA, 16 C.F.R. § 312.5;
14 and

15 d. Failing to establish and maintain reasonable procedures to protect the confidentiality, security,
16 and integrity of Personal Information collected from children under 13, in violation of Section
17 312.8 of COPPA, 16 C.F.R. § 312.8.

18 293. Violations of COPPA and the accompanying FTC regulations “shall be treated as a
19 violation of a rule defining an unfair or deceptive act or practice prescribed under 15 U.S.C. §
20 57a(a)(1)(B).” 15 U.S.C. § 6502(c). These rules define unfair or deceptive acts or practices in or
21 affecting commerce within the meaning of 15 U.S.C. § 45(a)(1), which is the model for the various
22 consumer protection statutes in the several states, including the FDUTPA.⁵⁸

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

27 _____
28 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.”).

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

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

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

17 298. At the same time, Defendants have (i) at all relevant times known that children under the
18 age of 13 use the Android Apps, (ii) actively sought to increase use of the Apps by these children, and
19 (iii) sought to exploit, for commercial purposes and gain, the millions of children under the age of 13
20 using the Android Apps. Defendants' knowledge of the widespread use of the Apps by children (which
21 Defendants have expressly touted in their advertising sales efforts) and their concealment and failure to
22 disclose the exfiltration of Personal Information from such children and they were tracking, profiling,
23 and targeting these children and/or profiting from this conduct through lucrative behavioral advertising,
24 while at the same time promoting, representing, and purporting to ensure that the Android Apps comply
25
26
27
28

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

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

9
10 300. Defendants had a duty to disclose the above-described facts due to the important public
11 interest in securing the privacy of young children's Personal Information and the fact that young
12 children are unable to fully protect their own interests. Parents and guardians of Plaintiffs C.D.1, C.D.2,
13 and C.D.3 and the Florida Subclass Members placed trust in Defendants as reputable companies, which
14 represent that they comply with applicable laws and societal interests in safeguarding children's
15 Personal Information. Additionally, Defendants exclusively knew and understood the extent of their
16 collection of Personal Information, and the parents or guardians of Plaintiffs C.D.1, C.D.2, and C.D.3
17 and Florida Subclass Members could not reasonably have discovered—and were unaware of—
18 Defendants' secret tracking, profiling, and targeting.

19
20 301. Defendants' conduct is immoral, unethical, oppressive, unscrupulous and substantially
21 injurious to consumers, and there are no greater countervailing benefits to consumers or competition.
22 Further, Plaintiffs and Florida Subclass Members could not have reasonably avoided injury because
23 Defendants took advantage of the lack of knowledge, ability, experience, and/or capacity of consumers
24 to their detriment.

25
26 302. Defendants willfully engaged in the deceptive, misleading, and unlawful acts described
27 herein and knew or recklessly disregarded the fact that they violated Fla. Stat. § 501.201, *et seq.*
28

1 303. Plaintiffs C.D.1, C.D.2, and C.D.3 and Florida Subclass Members were harmed by
2 Defendants' practices, which were a substantial factor and caused injury in fact and actual damages to
3 Plaintiffs C.D.1, C.D.2, and C.D.3 and Florida Subclass Members. As a direct and proximate result of
4 Defendants' unlawful, unfair, and deceptive acts and practices in violation of Fla. Stat. § 501.201, *et*
5 *seq.*, Plaintiffs and Florida Subclass Members have suffered and will continue to suffer an ascertainable
6 loss of money or property, real or personal, and monetary and non-monetary damages, as described
7 herein, including the loss of the value or diminishment in value of their Personal Information and the
8 loss of the ability to control the use of their Personal Information, which allowed Defendants to profit at
9 the expense of Plaintiffs C.D.1, C.D.2, and C.D.3 and Florida Subclass Members.
10

11 304. As outlined herein, there is tangible value in Plaintiffs C.D.1, C.D.2, and C.D.3's and
12 Florida Subclass Members' Personal Information has tangible value. Plaintiffs C.D.1, C.D.2, and C.D.3
13 and Florida Subclass Members have lost the opportunity to receive value in exchange for their Personal
14 Information.
15

16 305. Defendants' monetization of Plaintiffs C.D.1, C.D.2, and C.D.3's and Florida Subclass
17 Members' Personal Information demonstrates that there is a market for their Personal Information.
18

19 306. Plaintiffs C.D.1, C.D.2, and C.D.3's and Florida Subclass Members' Personal
20 Information is now in the possession of Defendants, who have used and will use it for their financial
21 gain.
22

23 307. Defendants' retention of Plaintiffs C.D.1, C.D.2, and C.D.3's and Florida Subclass
24 Members' Personal Information presents a continuing risk to them as well as the general public.
25

26 308. Florida Plaintiffs and Florida Subclass Members seek relief for the injuries they have
27 suffered as a result of Defendants' unconscionable, unfair, and deceptive acts and practices, as provided
28 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

1 Information collected without parental consent, requiring Defendants to provide a complete audit and
2 accounting of the uses of the Personal Information by Defendants, App developers and any other third
3 parties, and other appropriate injunctive and/or declaratory relief.
4

5 **SIXTH CLAIM FOR RELIEF**

6 **FLORIDA UNJUST ENRICHMENT**

7 **(On Behalf of the Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclasses)**

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

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

14 311. This Personal Information, the value of the Personal Information, and/or the attendant
15 revenue from the use and profit by Defendants, were monetary benefits conferred upon Defendants by
16 Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass members.
17

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

21 313. It would be inequitable and unjust to permit Defendants to retain the substantial economic
22 benefits (financial and otherwise) they obtained from and/or at the expense of Plaintiffs C.D.1, C.D.2,
23 and C.D.3 and the Florida Subclass.
24

25 314. Defendants will be unjustly enriched if they are permitted to retain the economic benefits
26 conferred upon them by Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass members through
27 Defendants obtaining Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass members' Personal
28

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

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

5 316. Plaintiffs C.D.1, C.D.2, and C.D.3 and the Florida Subclass members are entitled to
6 restitution, disgorgement, and/or the imposition of a constructive trust to recover the amount of
7 Defendants' ill-gotten gains, and/or other sums as may be just and equitable.
8

9 **SEVENTH CLAIM FOR RELIEF**

10 **NEW YORK CONSUMER PROTECTION LAW**

11 **N.Y. Gen. Bus. Law § 349 *et seq.***

12 **(Brought on behalf of Plaintiffs E.F.1 and E.F.2 and the New York Subclass against All
13 Defendants)**

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

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

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

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

24 321. N.Y. Gen. Bus. Law § 349(a) provides “[d]eceptive acts or practices in the conduct of
25 any business, trade or commerce or in the furnishing of any service in this state are hereby declared
26 unlawful.”
27
28

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

3 323. Defendants at all relevant times knowingly violated legal duties and public policy by
4 collecting the Personal Information of children under 13 and tracking, profiling, and targeting those
5 children with behavioral advertising for Defendants’ financial gain. As outlined herein, Defendants at
6 all times had actual knowledge that the Android Apps were not compliant with the guidelines and
7 requirements in Google’s DFF program, which mandated adherence to COPPA and other applicable
8 privacy-related laws. Further, Defendants at all times had actual knowledge and specifically intended
9 that the AdMob SDKs embedded in the Android Apps enabled and effectuated the exfiltration of
10 Personal Information from Plaintiffs and children under 13 using the Android Apps and the tracking,
11 profiling, and targeting of those children for lucrative behavioral advertising.
12

13 324. As outlined herein, Google broadly promoted, marketed, and represented in numerous
14 ways that the DFF program and the Apps included in the program as suitable and safe and designed for
15 children and legally compliant, including in public-facing websites, privacy policies and program
16 requirements, marketing materials, App interfaces, and other public statements and materials, and
17 internally acknowledged and advised its App developer partners the same. For example:
18

19 The DFF program had a “strict legal and policy bar,” requiring that Apps displaying ads “comply
20 with all legal obligations relating to advertising to children,” “Ads displayed to child audiences
21 do not involve interest-based advertising,” Apps submitted to the DFF program were “compliant
22 with COPPA and other relevant statutes,” and that “Ads displayed to child audiences must
23 comply with laws relating to advertising to kids,” and the App “must disable interest-based
24 advertising;”

25 Google warned that non-compliance with DFF guidelines and requirements could result in
26 expulsion of the App from the DFF program;

27 Google stated that DFF was designed to be “inclusive of apps that are made for kids,” and that
28 “apps that have no specific benefit or relevance for audiences under the age of thirteen will not
be accepted into the program;”

1 Google stated that “Apps that meet the [DFF] program requirements will be featured through
2 Google Play's family-friendly browse and search experiences so that parents can find suitable,
3 trusted, high-quality apps and games more easily.”

4 Google stated that the DFF program “helps parents easily find your family-friendly apps and
5 games” and “create[s] a trusted environment that empowers parents to make informed decisions
6 and engage with [App developer] content.”

7 The DFF program provided privileges to DFF Apps/games that opted in to DFF, touting that
8 only those Apps/games “[would] show up in searches initiated from the family section in Apps
9 Home,” and be “more visible” when “users search for family or kids related content from
10 anywhere in the [Google] Play store.”

11 The DFF program implemented a “Family star button on Apps and Games Home point[ed] to an
12 enhanced discovery experience for parents looking for family appropriate content,” and “Apps
13 participating in [DFF] are marked with the family star badge, which reflects the target age you
14 select for your apps and serves as a signal of quality for parents.”

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

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

25 a. Failing to provide sufficient notice of the information Defendants collected, or the information
26 that was collected on Defendants’ behalf, online from children under 13, how Defendants used
27 such information, their disclosure practices, and all other required content, in violation of Section
28 312.4(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);

1 c. Failing to obtain verifiable parental consent before any collection or use of Personal
2 Information from children under 13, in violation of Section 312.5 of COPPA, 16 C.F.R. § 312.5;
and

3 d. Failing to establish and maintain reasonable procedures to protect the confidentiality, security,
4 and integrity of Personal Information collected from children under 13, in violation of Section
5 312.8 of COPPA, 16 C.F.R. § 312.8.

6 327. Violations of COPPA and the accompanying FTC regulations “shall be treated as a
7 violation of a rule defining an unfair or deceptive act or practice prescribed under 15 U.S.C. §
8 57a(a)(1)(B).” 15 U.S.C. § 6502(c). These rules define unfair or deceptive acts or practices in or
9 affecting commerce within the meaning of 15 U.S.C. § 45(a)(1), which is the model for the various
10 consumer protection statutes in the several states, including the GBL.⁵⁹

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

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

16 330. Parents and guardians of Plaintiffs E.F.1 and E.F.2 and the members of the New York
17 Subclass reasonably expected that Defendants would respect children’s privacy online, in accordance
18 with their own policies and guidelines, statements, and representations, societal expectations and public
19 policy, as well as state and federal statutes and regulations including COPPA and Federal Trade
20 Commission regulations. As outlined herein, the Android App games are marketed, promoted, and
21 represented as safe and suitable for children, predicated on, *inter alia*, (i) their offering and availability
22 and promotion and marketing in the DFF program in the Family section of the Google Play Store and
23 the representations and statements concerning the DFF program and the Family section of the Google
24

25
26
27 _____
28 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.”).

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

4
5 331. At the same time, Defendants have (i) at all relevant times known that children under the
6 age of 13 use the Android Apps, (ii) actively sought to increase use of the Apps by these children, and
7 (iii) sought to exploit, for commercial purposes and gain, the millions of children under the age of 13
8 using the Android Apps. Defendants' knowledge of the widespread use of the Apps by children (which
9 Defendants have expressly touted in their advertising sales efforts) and their concealment and failure to
10 disclose the exfiltration of Personal Information from such children and they were tracking, profiling,
11 and targeting these children and/or profiting from this conduct through lucrative behavioral advertising,
12 while at the same time promoting, representing, and purporting to ensure that the Android Apps comply
13 with law and societal expectation, are likely to and, in fact, did deceive Plaintiffs E.F.1 and E.F.2 and
14 members of the New York Subclass and their parents or guardians.

15
16 332. Defendants' misrepresentations and omissions were explicit and implicit. Defendants'
17 representations and omissions were material because they were likely to deceive reasonable consumers
18 such as the parents or guardians of Plaintiffs E.F.1 and E.F.2 and the New York Subclass Members
19 about the terms under which their children were using the Apps as well as the fact that Defendants were
20 collecting and profiting from the Personal Information of children under the age of thirteen without their
21 parents and guardians' knowledge or consent.

22
23 333. Defendants had a duty to disclose the above-described facts due to the important public
24 interest in securing the privacy of young children's Personal Information and the fact that young
25 children are unable to fully protect their own interests. Parents and guardians of Plaintiffs E.F.1 and
26 E.F.2 and the New York Subclass Members placed trust in Defendants as reputable companies which
27 represent that they comply with applicable laws and societal interests in safeguarding childrens'
28

1 Personal Information. Additionally, Defendants exclusively knew and understood the extent of their
2 collection of Personal Information, and the parents or guardians of Plaintiffs E.F.1 and E.F.2 and New
3 York Subclass Members could not reasonably have discovered—and were unaware of—Defendants’
4 secret tracking, profiling, and targeting.
5

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

11 335. Defendants willfully engaged in the deceptive, misleading, and unlawful acts described
12 herein and knew or recklessly disregarded the fact that they violated NY GBL § 349.
13

14 336. Plaintiffs E.F.1 and E.F.2 and New York Subclass Members were harmed by Defendants’
15 practices, which were a substantial factor and caused injury in fact and actual damages to Plaintiffs
16 E.F.1 and E.F.2 and New York Subclass Members. As a direct and proximate result of Defendants’
17 unlawful, unfair, and deceptive acts and practices in violation of NY GBL § 349, Plaintiffs and New
18 York Subclass Members have suffered and will continue to suffer an ascertainable loss of money or
19 property, real or personal, and monetary and non-monetary damages, as described herein, including the
20 loss of the value or diminishment in value of their Personal Information and the loss of the ability to
21 control the use of their Personal Information, which allowed Defendants to profit at the expense of
22 Plaintiffs E.F.1 and E.F.2 and New York Subclass Members.
23

24 337. As outlined herein, there is tangible value in Plaintiffs E.F.1 and E.F.2’s and New York
25 Subclass Members’ Personal Information has tangible value. Plaintiffs E.F.1 and E.F.2 and New York
26 Subclass Members have lost the opportunity to receive value in exchange for their Personal Information.
27
28

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

3 339. Plaintiffs E.F.1 and E.F.2's and New York Subclass Members' Personal Information is
4 now in the possession of Defendants, who have used and will use it for their financial gain.
5

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

8 341. Plaintiffs E.F.1 and E.F.2 and New York Subclass Members seek relief for the injuries
9 they have suffered as a result of Defendants' unlawful, unfair, and deceptive acts and practices, as
10 provided by NY GBL § 349 and applicable law, including all actual damages and attorneys' fees and
11 costs, treble damages, statutory damages, and restitution, as well as an injunction requiring Defendants
12 to permanently delete, destroy or otherwise sequester the Personal Information collected without
13 parental consent, requiring Defendants to provide a complete audit and accounting of the uses of the
14 Personal Information by Defendants, App developers and any other third parties, and other appropriate
15 injunctive and/or declaratory relief.
16

17 **EIGHTH CLAIM FOR RELIEF**

18 **NEW YORK UNJUST ENRICHMENT**

19 **(On Behalf of Plaintiffs E.F.1 and E.F.2 and the New York Subclass)**

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

21 343. By virtue of the unlawful, unfair, and deceptive conduct alleged herein, Defendants
22 knowingly realized hundreds of millions of dollars in revenue from the use and/or sale of Personal
23 Information of Plaintiffs E.F.1 and E.F.2 and the New York Subclass members for advertising and
24 commercialization purposes.
25

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

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

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

7 347. Defendants will be unjustly enriched if they are permitted to retain the economic benefits
8 conferred upon them by Plaintiffs E.F.1 and E.F.2 and the New York Subclass members through
9 Defendants obtaining Plaintiffs E.F.1 and E.F.2 and the New York Subclass members' Personal
10 Information and the value thereof, and profiting from the unlawful, unauthorized, and impermissible use
11 of the Personal Information of Plaintiffs E.F.1 and E.F.2 and the New York Subclass members.
12

13 348. Plaintiffs E.F.1 and E.F.2 and the New York Subclass members are therefore entitled to
14 recover the amounts realized by Defendants at their expense.
15

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

18 350. Plaintiffs E.F.1 and E.F.2 and the New York Subclass members are entitled to restitution,
19 disgorgement, and/or the imposition of a constructive trust to recover the amount of Defendants' ill-
20 gotten gains, and/or other sums as may be just and equitable.
21

22 **PRAYER FOR RELIEF**

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

25 A An order certifying this action as a class action, and certifying the Classes and Subclasses
26 defined herein, designating Plaintiffs, as described above, as the representatives of the respective Classes
27
28

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

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

9
10 C. A judgment awarding Plaintiffs and the members of the Classes and Subclasses
11 appropriate relief, including actual, compensatory, and/or statutory damages, and punitive damages (as
12 permitted by law), in an amount to be determined at trial;

13
14 D. A judgment awarding any and all equitable, injunctive, and declaratory relief as may be
15 appropriate, including orders of disgorgement of Defendants' unlawful gains, and restitution.

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

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

19 G. Grant such other legal and equitable relief as the Court may deem appropriate.
20

21 **DEMAND FOR JURY TRIAL**

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

23 Respectfully submitted,

24 DATED: June 22, 2023

/s/ Patrick Carey

25 Mark Todzo, (Bar No. 168389)

26 Patrick Carey, (Bar No. 308623)

LEXINGTON LAW GROUP

27 503 Divisadero Street

San Francisco, CA 94117

28 Telephone: 415-913-7800

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

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

(b) County of Residence of First Listed Plaintiff Tulare County (EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Patrick Carey, LEXINGTON LAW GROUP, 503 Divisadero Street, San Francisco, CA 94117, Telephone: 415-913-7800

DEFENDANTS

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

County of Residence of First Listed Defendant Santa Clara County (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff 3 Federal Question (U.S. Government Not a Party) 2 U.S. Government Defendant 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship: Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, Incorporated or Principal Place of Business In This State, Incorporated and Principal Place of Business In Another State, Foreign Nation.

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding 2 Removed from State Court 3 Remanded from Appellate Court 4 Reinstated or Reopened 5 Transferred from Another District (specify) 6 Multidistrict Litigation-Transfer 8 Multidistrict Litigation-Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U.S.C. 1332(d)(2)(A) Class Action Fairness Act, member of a class of plaintiffs is a citizen of a State different from Defendants

Brief description of cause: Violation of Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P. DEMAND \$ JURY DEMAND: X Yes No

VIII. RELATED CASE(S), IF ANY (See instructions):

JUDGE DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) SAN FRANCISCO/OAKLAND X SAN JOSE EUREKA-MCKINLEYVILLE

DATE 06/22/2023

SIGNATURE OF ATTORNEY OF RECORD

/s/ Patrick Carey

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I. a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the “defendant” is the location of the tract of land involved.)
- c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section “(see attachment).”
- II. Jurisdiction.** The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an “X” in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- (1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.
 - (2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an “X” in this box.
 - (3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 - (4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an “X” in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.
- V. Origin.** Place an “X” in one of the six boxes.
- (1) Original Proceedings. Cases originating in the United States district courts.
 - (2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.
 - (3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 - (4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 - (5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 - (6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.
 - (8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket. Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an “X” in this box if you are filing a class action under Federal Rule of Civil Procedure 23.
- Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
- Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.
- IX. Divisional Assignment.** If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: “the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated.”
- Date and Attorney Signature.** Date and sign the civil cover sheet.