

**LIEFF CABRASER HEIMANN & BERNSTEIN, LLP**

Michael W. Sobol (SBN 194857)  
msobol@lchb.com  
275 Battery Street, 29th Floor  
San Francisco, CA 94111-3339  
Telephone: 415.956.1000  
Facsimile: 415.956.1008

**LIEFF CABRASER HEIMANN & BERNSTEIN, LLP**

Nicholas Diamand  
ndiamand@lchb.com  
Douglas I. Cuthbertson  
dcuthbertson@lchb.com  
Abbye R. Klamann (SBN 311112)  
aklamann@lchb.com  
250 Hudson Street, 8th Floor  
New York, NY 10013-1413  
Telephone: 212.355.9500  
Facsimile: 212.355.9592

**CARNEY BATES & PULLIAM, PLLC**

Hank Bates (SBN 167688)  
hbates@cbplaw.com  
Allen Carney  
acarney@cbplaw.com  
David Slade  
dslade@cbplaw.com  
519 West 7<sup>th</sup> St.  
Little Rock, AR 72201  
Telephone: 501.312.8500  
Facsimile: 501.312.8505

*Attorneys for Plaintiffs individually and on behalf of all others similar situated*

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO/OAKLAND DIVISION

MICHAEL MCDONALD, TAMARA DRAUT, and their children, P.G.M., P.S.M., P.R.M., and H.D.-F., on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

KILOO APS; SYBO GAMES APS; ADCOLONY, INC.; ALTABA INC.; CHARTBOOST, INC.; FLURRY, INC.; INMOBI PTE LTD.; INMOBI INC.; IRONSOURCE LTD.; IRONSOURCE USA INC.; TAPJOY, INC.; and VUNGLE, INC.

Defendants.

Case No. 3:17-cv-4344

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

1 **I. INTRODUCTION**

2 1. This is an action brought by the parents of children<sup>1</sup> who, while playing online  
3 games via smart phone apps, have had their personally identifying information exfiltrated by the  
4 defendant game developers and their partners, for future commercial exploitation, in direct  
5 violation of the federal Children’s Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–  
6 6506. Plaintiffs bring claims under state laws to obtain an injunction to cease these practices,  
7 sequester illegally obtained information, and damages.

8 **II. PARTIES**

9 **Plaintiffs**

10 2. Plaintiffs are the parents and their children who used online gaming apps via  
11 websites or online services operated by the Defendants.

12 3. Plaintiff Michael McDonald, and his children, “P.G.M.,” “P.S.M.,” and “P.R.M.,”  
13 reside in Blue Lake, California. Mr. McDonald brings this action on behalf of himself, P.G.M.,  
14 P.S.M., and P.R.M., and all others similarly situated. P.G.M., P.S.M., and P.R.M. were under the  
15 age of 13 while using the gaming app Subway Surfers.

16 4. Plaintiff Tamara Draut and her child, “H.D.-F.,” reside in Brooklyn, New York.  
17 Ms. Draut brings this action on behalf of herself, H.D.-F, and all others similarly situated. H.D.-F  
18 was under the age of 13 while using the gaming app Subway Surfers.

19 **The Developer Defendants**

20 5. The Defendants Kiloo and Sybo (collectively, the “Developer Defendants”)  
21 developed and marketed the online gaming apps used by Plaintiffs, and many others in the United  
22 States.<sup>2</sup>

23 6. Defendant Kiloo ApS (“Kiloo”) is a commercial mobile game development  
24 company headquartered at Klostergade 28, First Floor, 8000 Aarhus C in Copenhagen, Denmark.

25  
26 

---

<sup>1</sup> All references to “children” contained herein refer to persons under the age of 13 pursuant to  
27 COPPA’s definition of children. See 16 C.F.R. § 312.2.

28 <sup>2</sup> See <https://sensortower.com/ios/us/kiloo/app/subway-surfers/512939461/> (last visited July 13,  
2017) (approximately 32% of Subway Surfers users are based in the United States).

1           7. Defendant Sybo Games ApS (“Sybo”) is a commercial mobile game development  
2 company headquartered at Jorcks Passage 1A, 4, 1162 Copenhagen K in Denmark.

3           8. Kiloo and Sybo co-developed the gaming app Subway Surfers.

4           **The SDK Defendants**

5           9. The “SDK Defendants” – identified in paragraphs 10 through 16 below – are  
6 entities which provided their own proprietary computer code to the Developer Defendants Kiloo  
7 and Sybo, known as software development kits (“SDK”), for installation and use in the Developer  
8 Defendants’ gaming apps, including Subway Surfers. Each of the SDK Defendants named herein  
9 embedded their respective SDKs in the Developer Defendants’ gaming apps, causing the  
10 transmittal of app users’ personally identifying information to the SDK Defendants to facilitate  
11 subsequent behavioral advertising.

12           10. SDK Defendant AdColony, Inc. (“AdColony”) is an American technology  
13 company with offices throughout the world, headquartered at 11400 W. Olympic Blvd., 12<sup>th</sup>  
14 Floor, Los Angeles, CA 90064.

15           11. SDK Defendant Chartboost, Inc. (“Chartboost”) is an American technology  
16 headquartered at 85 2<sup>nd</sup> Street, Suite 100, San Francisco, CA 94105.

17           12. SDK Defendant Flurry, Inc. is an American technology company headquartered at  
18 360 3<sup>rd</sup> Street, Suite 750, San Francisco, CA 94107. Flurry Inc. is a subsidiary of Defendant  
19 Altaba Inc., which is headquartered at 140 East 45th Street, 15th Floor, New York, NY 10017  
20 (Flurry, Inc. and Altaba Inc. together, “Flurry”).

21           13. SDK Defendant InMobi Pte Ltd. is a technology company with offices throughout  
22 the world. Its headquarters are located at 30 Cecil Street # 19-08, Prudential Tower, Singapore  
23 049712. SDK Defendant InMobi Inc. is a U.S. subsidiary wholly owned by InMobi Pte Ltd. Its  
24 headquarters are located at 475 Brannan Street, Suite 420, San Francisco, CA 94107. On  
25 information and belief, InMobi Inc. functions as the marketing arm and acts as a general manager  
26 of its parent company, InMobi Pte. Ltd. (InMobi Inc. and InMobi Pte. Ltd. together, “InMobi”).

27           14. SDK Defendant ironSource Ltd. is a global technology company with offices  
28 throughout the world and headquarters at 121 Menachem Begin Road, Azrieli Sarona Tower, Tel

1 Aviv. Upon information and belief, SDK Defendant ironSource USA Inc. is the U.S. subsidiary  
2 of ironSource Ltd., headquartered at 17 Bluxome Street, San Francisco, CA 94107, which acts as  
3 a general manager of its parent company, ironSource Ltd. (ironSource Ltd. and ironSource USA  
4 Inc. together, “ironSource”). SDK Defendant ironSource owns and operates the advertising SDK  
5 “Supersonic.”

6 15. SDK Defendant Tapjoy, Inc. (“Tapjoy”) is an American technology company with  
7 offices throughout the world, headquartered at 111 Sutter Street, 12th Floor, San Francisco, CA  
8 94104.

9 16. SDK Defendant Vungle, Inc. (“Vungle”) is an American technology company  
10 with offices throughout the world and headquarters at 185 Clara Street, San Francisco, CA 94107.

### 11 **III. JURISDICTION AND VENUE**

12 17. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C.  
13 §§ 1332 and 1367 because this is a class action in which the matter or controversy exceeds the  
14 sum of \$5,000,000, exclusive of interest and costs, and in which some members of the proposed  
15 Classes are citizens of a state different from some defendants.

16 18. This Court has personal jurisdiction over Defendants because they transact  
17 business in the United States, including in this District, have substantial aggregate contacts with  
18 the United States, including in this District, engaged and are engaging in conduct that has and had  
19 a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons  
20 throughout the United States, and purposely availed themselves of the laws of the United States.

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

### 25 **IV. INTRADISTRICT ASSIGNMENT**

26 20. Pursuant to Civil L.R. 3-2(c), assignment to this Division is proper because a  
27 substantial part of the conduct which give rise to Plaintiffs’ claims occurred in this District.  
28 Defendants market their products throughout the United States, including in San Francisco and

1 Alameda counties. In addition, most SDK Defendants are headquartered in or have offices in San  
2 Francisco.

3 **V. ALLEGATIONS APPLICABLE TO ALL COUNTS**

4 **A. The Programming of Mobile Online Gaming Apps Enables the Collection of**  
5 **Personal Data.**

6 21. The number of Americans using and relying on mobile devices connected to the  
7 internet (“smart” phones, tablets, and other devices) had increased to 77% of Americans by  
8 November 2016. Consumers increasingly use smart devices to play their favorite online games,  
9 or “apps.” Many apps are aimed at children, who increasingly use smart devices to play their  
10 favorite games.

11 22. Most consumers, including parents of children consumers, do not know that apps  
12 created for children are engineered to surreptitiously and unlawfully collect the child-users’  
13 personal information, and then exfiltrate that information off the smart device for advertising and  
14 other commercial purposes.

15 23. App developers contract with third-parties for the right to embed third-party  
16 computer code into the developers’ apps, for various purposes. For example, a developer may  
17 incorporate Google’s “In-App Billing SDK,” so that app users may make purchases and payments  
18 directly to the developer. In this way, app developers are like vehicle manufacturers, which also  
19 incorporate third-party components, such as airbags or brake pads, into their vehicles, rather than  
20 developing their own component parts from scratch.

21 24. Advertising-specific SDKs are blocks of computer code which operate to secretly  
22 collect an app user’s personal information and track online behavior to facilitate behavioral  
23 advertising or marketing analysis. In the case of an advertising SDK, the creator of the SDK will  
24 embed its SDK code into the underlying code of the app itself, collect personal information to  
25 serve behavioral advertisements, and then pay the app developer based on the number of ads  
26 shown. This practice is a substantial source of many app developers’ revenue, enabling app  
27 developers to allow users to download the apps without charging a purchase price.<sup>3</sup>

28 <sup>3</sup> “Only 33% of US Mobile Users Will Pay for Apps This Year,” eMarketer (Feb. 5, 2015),

1           25.     App developers and their SDK-providing partners can track children’s behavior  
2 while they play online games with their mobile devices by obtaining critical pieces of data from  
3 the mobile devices, including “persistent identifiers,” typically a unique number linked to a  
4 specific mobile device (*e.g.*, an individual’s smart phone may be identified as “45 125792 45513  
5 7”). SDK providers, such as the SDK Defendants, use their advertising SDKs, embedded into an  
6 app in conjunction with the app developers, such as the Developer Defendants, to capture and  
7 collect persistent identifiers associated with a particular child user from her mobile device. These  
8 persistent identifiers allow SDK providers to detect a child’s activity across multiple apps and  
9 platforms on the internet, and across different devices, effectively providing a full chronology of  
10 the child’s actions across devices and apps. This information is then sold to various third-parties  
11 who sell targeted online advertising.

12           26.     Key digital privacy and consumer groups described why and how a persistent  
13 identifier alone facilitates behavioral advertising:

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

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

21           27.     In other words, the ability to serve behavioral advertisements to a specific user no  
22 longer turns upon obtaining the kinds of data with which most consumers are familiar (email  
23 addresses, etc.), but instead on the surreptitious collection of persistent identifiers, which are used  
24 in conjunction with other data points to build robust online profiles. Permitting technology

25  
26 *available at* <https://www.emarketer.com/Article/Only-33-of-US-Mobile-Users-Will-Pay-Apps-This-Year/1011965> (last visited July 31, 2017) (“Put a dollar sign in front of an app, and the  
27 number of people who are willing to download and install it drops dramatically. According to a  
28 new forecast from eMarketer, 80.1 million US consumers will pay for mobile apps at least once  
this year, representing only 33.3% of all mobile users.”).

1 companies to obtain persistent identifiers associated with children exposes them to the behavioral  
2 advertising (as well as other privacy violations) that COPPA was designed to prevent.

3 28. When children are tracked over time and across the internet, various activities are  
4 linked to a unique and persistent identifier to construct a profile of the user of a given smart  
5 device. Viewed in isolation, a persistent identifier is merely a string of numbers uniquely  
6 identifying a user, but when linked to other data points about the same user, such as app usage,  
7 geographic location (including likely domicile), and internet navigation, it discloses a personal  
8 profile that can be exploited in a commercial context. The chain of events typically works as  
9 follows: an app developer installs an SDK in an app, which collects persistent identifiers,  
10 permitting the SDK entity to sell the child's persistent identifier to an advertising network or  
11 third-party data aggregator (who then further resells the data to additional partners). An "Ad  
12 Network" will store the persistent identifiers on its servers. Later, other app or SDK developers  
13 sell that same child's persistent identifier to the Ad Network, bolstering the Ad Network's profile  
14 of the child, increasing the value of the child's data and, relatedly, the ability to serve a more  
15 highly-targeted ad to a specific device. Multiple Ad Networks or other third-parties can then buy  
16 and sell data, exchanging databases amongst themselves, creating an increasingly sophisticated  
17 and merchantable profile of how, when, and why a child uses her mobile device, along with all of  
18 the demographic and psychographic inferences that can be drawn therefrom.

19 29. The Ad Networks, informed by the surreptitious collection of data from children,  
20 will assist in the sale of advertising placed within the gaming apps and targeted specifically to  
21 children.

22 30. In sum, children's personal information is captured from them, as is information of  
23 their online behavior, which is then sold to third-parties who track multiple data points associated  
24 with a personal identifier, analyzed with the sophisticated algorithms of Big Data to create a user  
25 profile, and then used to serve behavioral advertising to children whose profile fits a set of  
26 demographic and behavioral traits.

27  
28

1           **COPPA Outlaws the Collection of Children’s Personal Information Without**  
2           **Verifiable Parental Consent.**

3           31. Children are especially vulnerable to online tracking and the resulting behavioral  
4 advertising. As children’s cognitive abilities still are developing, they have limited understanding  
5 or awareness of sophisticated advertising and therefore are less likely than adults to distinguish  
6 between the actual content of online gaming apps and the advertising content that is targeted to  
7 them alongside it. Thus, children may engage with advertising content without realizing they are  
8 doing so. *See* Comments of The Center for Digital Democracy, et al., FTC, *In the Matter of*  
9 *Children’s Online Privacy Protection Rule* at 13-14 (Dec. 23, 2011).

10           32. Recognizing the vulnerability of children in the Internet age, in 1999 Congress  
11 enacted the Children’s Online Privacy Protection Act (COPPA). *See* 15 U.S.C. §§ 6501–6506.  
12 COPPA’s express goal is to protect children’s privacy while they are connected to the internet.<sup>4</sup>  
13 Under COPPA, developers of child-focused apps, and any third-parties working with these app  
14 developers, cannot lawfully obtain the personal information of children under 13 years of age  
15 without first obtaining verifiable consent from their parents.

16           33. COPPA applies to any operator of a commercial website or online service  
17 (including an app) that is directed to children and that: (a) collects, uses, and/or discloses personal  
18 information from children, or (b) on whose behalf such information is collected or maintained.  
19 Under COPPA, personal information is “collected or maintained on behalf of an operator when .  
20 . . [t]he operator benefits by allowing another person to collect personal information directly  
21 from users of” an online service. 16C.F.R. § 312.2. In addition, COPPA applies to any  
22 operator of a commercial website or online service that has actual knowledge that it collects, uses,  
23 and/or discloses personal information from children.

24           34. Under COPPA, “personal information” includes more commonly understood  
25 information like names, email addresses, and social security numbers, but it also includes  
26 “persistent identifier[s] that can be used to recognize a user over time and across different Web

---

27 <sup>4</sup> *See* Federal Trade Commission, “New Rule Will Protect Privacy of Children Online,” Oct. 20,  
28 1999, *available at* <https://www.ftc.gov/news-events/press-releases/1999/10/new-rule-will-protect-privacy-children-online> (last visited July 31, 2017).



1 sites or online services.” 16 C.F.R. § 312.2. COPPA’s broad definition of “personal  
2 information” is as follows:

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

19 35. The FTC regards “persistent identifiers” as “personally identifiable” information  
20 that can be reasonably linked to a particular child. The FTC amended COPPA’s definition of  
21 “personal information” to clarify the inclusion of persistent identifiers. *See*  
22 <https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising->  
23 [industry](https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-) (2016 FTC Blog post from Director of the FTC Bureau of Consumer Protection) (last  
24 visited July 19, 2017).

25 36. In order to lawfully collect, use, or disclose personal information, COPPA requires  
26 that an operator meet specific requirements, including *each* of the following:

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

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

6           38. The FTC recently clarified acceptable methods for obtaining verifiable parental  
7 consent, which include: (i) providing a consent form for parents to sign and return; (ii) requiring  
8 the use of a credit card/online payment that provides notification of each transaction; (iii)  
9 connecting to trained personnel via video conference; (iv) calling a staffed toll-free number; (v)  
10 emailing the parent soliciting a response email plus requesting follow-up information from the  
11 parent; (vi) asking knowledge-based questions; or (vii) verifying a photo ID from the parent  
12 compared to a second photo using facial recognition technology. *See* [https://www.ftc.gov/tips-](https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance)  
13 [advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance](https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance)  
14 (last visited July 20, 2017).

15           **C. Defendants Collect and Use Children’s Personal Information Through Their**  
16           **Game Tracking Apps.**

17           39. Kiloo and Sybo co-developed the mobile online gaming app Subway Surfers  
18 which they have marketed since 2012. By 2015, it had been downloaded more than 1 billion  
19 times.<sup>5</sup> By 2016, it became the top Google Play game of all time, calculated by both revenue and  
20 number of downloads.<sup>6</sup>

21           40. In addition to Subway Surfers, the Developer Defendants have developed and  
22 marketed other gaming apps that, like Subway Surfers, track their users. Sybo has developed an  
23 app called Blades of Brim, and Kiloo has developed these other apps: Frisbee Forever, Frisbee  
24 Forever 2, Spellbinders, Smash Champs, Tesla Tubes, and Storm Blades (with Subway Surfers,  
25 these apps are collectively referred to as the “Game Tracking Apps”). Since at least 2012, the

26 <sup>5</sup>[http://www.gamasutra.com/view/pressreleases/254458/Subway\\_Surfers\\_Reaches\\_One\\_Billion\\_](http://www.gamasutra.com/view/pressreleases/254458/Subway_Surfers_Reaches_One_Billion_Downloads_Worldwide.php)  
27 [Downloads\\_Worldwide.php](http://www.gamasutra.com/view/pressreleases/254458/Subway_Surfers_Reaches_One_Billion_Downloads_Worldwide.php) (last visited July 19, 2017).

28 <sup>6</sup>[http://www.adweek.com/digital/report-subway-surfers-most-downloaded-google-play-game-](http://www.adweek.com/digital/report-subway-surfers-most-downloaded-google-play-game-ever/)  
ever/ (last visited July 25, 2017).

1 Developer Defendants, individually and together, have offered one or more of the Games  
2 Tracking Apps for download from Apple’s App Store, Google Play, and Amazon.

3 41. The Developer Defendants collect and maintain personal information about the  
4 users of the Game Tracking Apps, including users under the age of 13, and permit the SDK  
5 Defendants to embed their advertising SDKS to collect those users’ personal information and use  
6 that information to track those users over time and across different websites and online services.

7 42. The Developer Defendants have control over and responsibility for any advertising  
8 and data mining permitted by the Game Tracking Apps. The Developer Defendants have failed  
9 to safeguard children’s personal information and ensure that third-parties’ collection of data from  
10 children is lawful, in part, by allowing the SDK Defendants to embed advertising SDKs in the  
11 Game Tracking Apps directed at children.

12 43. Each SDK Defendant has an SDK placed in Subway Surfers which collects  
13 persistent identifiers to track children app users over time and across the internet. In addition to  
14 Subway Surfers, the other Game Tracking Apps contain SDKs that surreptitiously track child  
15 users for behavioral advertising, analytics, or both. Subway Surfers and the other Game Tracking  
16 Apps contain multiple SDKs, each operating independently from and in concert with one another.

17 44. Each SDK Defendant facilitates behavioral advertising in the mobile app space by  
18 collecting personal information about app users that enables advertisers and other third-parties to  
19 reach those users over time and across different websites and online services. Each SDK  
20 Defendant does so through its proprietary SDK embedded in the Developer Defendants’ Apps –  
21 including Subway Surfers – which collect personal information about children under the age of  
22 13 so that advertisers and other third-parties can target those children over time and across  
23 different websites and online services.

24 45. Analytics and network analysis tools have detected the persistent identifiers that  
25 each Game Tracking App accessed in real time, determined which SDKs reside in the Game  
26 Tracking Apps’ code, and recorded all network traffic, including encrypted data. That  
27 documentation contains raw network data, which shows the presence of persistent identifiers and  
28 documents (i) when the Game Tracking Apps first attempted to access persistent identifiers, (ii)

1 which persistent identifiers were sent from a users' device, and (iii) the SDK Defendant to which  
2 they were sent.

3 46. Extensive analysis conducted as to each of the Developer Defendants' Game  
4 Tracking Apps and as to each SDK Defendant, found substantial evidence that each of these  
5 child-directed apps collect and use children's persistent identifiers.

6 **2. The Developer Defendants' Tracking Game Apps Are Directed to**  
7 **Children.**

8 47. COPPA defines "children" as individuals under the age of 13. *See* 16 C.F.R.  
9 § 312.2. An app is directed to children if the "subject matter, visual content, use of animated  
10 characters or child-oriented activities and incentives, music or other audio content, age of models,  
11 presence of child celebrities or celebrities who appeal to children, language or other  
12 characteristics of the Web site or online service, as well as whether advertising promoting or  
13 appearing on the Web site or online service is directed to children." *See* 16 C.F.R. § 312.2.

14 48. Subway Surfers and the other Game Tracking Apps are directed to children under  
15 age 13.<sup>7</sup> For example, Subway Surfers is a game in which users pretend to be a graffiti artist,  
16 described by the Developer Defendants as a "youthful hooligan," who runs down subway tracks  
17 to avoid capture by the police. The description of Subway Surfers in both Apple's App Store and  
18 Google Play states, "DASH as fast as you can! DODGE the oncoming trains! Help Jake, Tricky  
19 & Fresh escape from the grumpy Inspector and his dog. Grind trains with your cool crew!  
20 Colorful and vivid HD graphics! Hoverboard Surfing! Paint powered jetpack! Lightning fast  
21 swipe acrobatics! Challenge and help your friends! Join the most daring chase!" Below is a  
22 screenshot from the game:

23  
24  
25  
26  
27 \_\_\_\_\_  
28 <sup>7</sup> A description of the additional Game Tracking Apps, including screenshots of the games from  
the Apple Store and from Google Play, is appended hereto as Exhibit A.



49. In the Apple Store, Google Play, and Amazon, Subway Surfers is rated as a game for users younger than 13 or as appropriate for most users.

50. In 2015, the Children’s Advertising Review Unit (“CARU”), the advertising industry’s self-regulating body that is a branch of the Better Business Bureau, found that children under the age of 13 played Subway Surfers, that the game was directed to children, and that Defendant Kiloo may have violated COPPA. CARU based its conclusion on the following:

The protagonist is a brightly colored cartoon character and is himself a “kid” and the game is basic in its play pattern. The game is featured as one of the “Games for Children” in the Android Store. It is rated for players age nine years and up in the Apple Store, players 10 years and up in the Google Play Store and for “All Ages” by Amazon. Parents posting to the website of Common Sense Media rated the game as appropriate for children age nine and older, while children rated it appropriate for children age six or older. The Australian Council on Children and the Media reviewed Subway Surfer and provided special advice for parents relating to the game.

See <http://www.asrcreviews.org/following-caru-inquiry-app-maker-kiloo-agrees-to-modify-subway-surfers-privacy-policy-to-better-protect-child-players/> (last visited July 5, 2017).

1           51. In response, Kiloo stated that – at that time – it did not “collect personal  
2 information that would require Kiloo to obtain verifiable parental consent under COPPA.” *See*  
3 *id.* This statement was and remains false, because the Developer Defendants contracted then and  
4 contract now with the SDK Defendants to permit collection of personal information regarding  
5 children playing the Game Tracking Apps in violation of COPPA.

6           52. Even if the Game Tracking Apps were not directed at children, on information and  
7 belief, Defendants have actual knowledge that they collected personal information from children.  
8 The Game Tracking Apps contain child-oriented “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  
11 characteristics of the Web site or online service, as well as whether advertising promoting or  
12 appearing on the Web site or online service is directed to children.” 16 C.F.R. § 312.2.

13                           **3. The Defendants Are Operators under COPPA.**

14           53. Each Defendant is an “operator” pursuant to COPPA. Specifically, COPPA  
15 defines an “operator,” in pertinent part, as:

16                           any person who operates a Web site located on the Internet or an  
17                           online service and who collects or maintains personal information  
18                           from or about the users of or visitors to such Web site or online  
19                           service, or on whose behalf such information is collected or  
20                           maintained, or offers products or services for sale through that Web  
21                           site or online service, where such Web site or online service is  
22                           operated for commercial purposes involving commerce among the  
23                           several States or with 1 or more foreign nations; in any territory of  
24                           the United States or in the District of Columbia, or between any  
25                           such territory and another such territory or any State or foreign  
26                           nation; or between the District of Columbia and any State, territory,  
27                           or foreign nation.

28                           16 C.F.R. § 312.2.

          54. Both the Developer Defendants and the SDK Defendants operate the Game  
Tracking Apps entirely online. Indeed, without a connection to the internet, Plaintiffs could not  
have downloaded and played Subway Surfers.

1                   **4. Defendants Engaged in the Foregoing Acts Without Obtaining**  
2                   **Verifiable Parental Consent.**

3           55. Defendants collected, used, or disclosed the personal information of Plaintiffs'  
4 children without notifying their parents. The Developer Defendants never obtained Plaintiffs'  
5 verifiable parental consent to collect, use, or disclose their children's personal information. The  
6 SDK Defendants failed to adequately ensure that when they embedded their advertising SDKS on  
7 the Game Tracking Apps or when they collected, used, or disclosed personal information from  
8 children via their advertising SDKs on the Game Tracking Apps, that the Developer Defendants  
9 had obtained verifiable parental consent for those children's use of the Game Tracking Apps.

10           56. Plaintiffs never knew that Defendants collected, disclosed, or used their children's  
11 personal information because Defendants at all times failed to provide Plaintiffs any of the  
12 required disclosures, never sought verifiable parental consent, and never provided a mechanism  
13 by which the Plaintiffs could provide verifiable consent.

14                   **5. Each SDK Defendant, in Coordination with the Developer Defendants,**  
15                   **Collects, Uses, or Discloses Children's Personal Information Within**  
16                   **Subway Surfers without Verifiable Parental Consent.**

17           57. The Developer Defendants' Subway Surfers app contains each of the SDK  
18 Defendants' behavioral advertising SDKs.

19           58. Each SDK Defendant knows or should know that it operates within Subway  
20 Surfers.

21           59. Each SDK Defendant knows or should know the age rating or suggested guidance  
22 for Subway Surfers listed in the Google Play Store, the Apple App Store, or Amazon, within  
23 which the SDK Defendant operates.

24           60. Accordingly, each SDK Defendant knows or should know that its behavioral  
25 advertising SDK is contained within Subway Surfers, among other child-directed apps.

26           61. The Developer Defendants did not inform the Plaintiffs, their children, or class  
27 members that the SDK Defendants' behavioral advertising SDKs are incorporated into and  
28 operate within the Game Tracking Apps, including Subway Surfers, to collect Plaintiffs'  
children's and class members' personal information in the form of persistent identifiers.

1           62. Each SDK Defendant failed to inform the Plaintiffs, their children, or class  
2 members that its behavioral advertising SDK is incorporated into and operates within Subway  
3 Surfers to collect the Plaintiffs' children's and class members' personal information in the form  
4 of persistent identifiers.

5           63. The Developer Defendants did not obtain verifiable parental consent to track  
6 children playing the Game Tracking Apps, including Subway Surfers, via persistent identifiers,  
7 over time and across different websites and online services.

8           64. Each SDK Defendant failed to obtain verifiable parental consent to track children  
9 playing Subway Surfers, via persistent identifiers, over time and across different websites and  
10 online services.

11           65. Each SDK Defendant systemically tracks each user of Subway Surfers, including  
12 users under the age of 13, over time and across different websites and online services, through its  
13 behavioral advertising SDK.

14           66. Each SDK Defendant does this by operating within Subway Surfers to collect, use,  
15 and share persistent identifiers from children who play Subway Surfers.

16           67. Accordingly, each SDK Defendant, in coordination with the Developer  
17 Defendants, collects, uses, and/or discloses the personal information of the Plaintiffs' children's  
18 and class members under the age of 13, in the form of persistent identifiers, to track children's  
19 activity over time and across different websites and online services.

20           68. By affirmatively incorporating the SDK Defendants' behavioral advertising SDKs  
21 into their child-directed apps and permitting them to track children by collecting, using, or  
22 disclosing their persistent identifiers without verifiable parental consent, the Developer  
23 Defendants violated COPPA.

24           69. Further, each SDK Defendant knew or should have known that its SDK had been  
25 incorporated into Subway Surfers and that engaging in the above-described tracking and  
26 collection of children's personal information violated COPPA.

27  
28



1                   **6. The Developer Defendants Engage in Substantially Similar Conduct in**  
2                   **Their Other Game Tracking Apps by Incorporating the SDK**  
3                   **Defendants' Behavioral Advertising SDKs into Those Game Tracking**  
4                   **Apps.**

5                   70. The Developer Defendants' other Game Tracking Apps also contain the behavioral  
6                   advertising SDKs, which operate in a substantially similar manner as in Subway Surfers.

7                   71. Defendant AdColony's AdColony SDK is incorporated into the following  
8                   additional Game Tracking Apps developed by Kiloo: Smash Champs, Frisbee Forever 2,  
9                   Spellbinders, and Tesla Tubes. The AdColony SDK is also incorporated into Sybo's Blades of  
10                  Brim.

11                 72. Defendant Chartboost's Chartboost SDK is incorporated into the following  
12                 additional Game Tracking Apps developed by Kiloo: Smash Champs, Frisbee Forever, Frisbee  
13                 Forever 2, Stormblades, Spellbinders, and Tesla Tubes.

14                 73. Defendant Flurry's Flurry SDK is incorporated into the following additional Game  
15                 Tracking App developed by Kiloo: Spellbinders.

16                 74. Defendant InMobi's InMobi SDK is incorporated into the following additional  
17                 Game Tracking Apps developed by Kiloo: Smash Champs, Stormblades, Spellbinders, and Tesla  
18                 Tubes.

19                 75. Defendant ironSource's Supersonic SDK is incorporated into the following  
20                 additional Game Tracking App developed by Kiloo: Spellbinders.

21                 76. Defendant Tapjoy's Tapjoy SDK is incorporated into the following additional  
22                 Game Tracking Apps developed by Kiloo: Smash Champs and Spellbinders.

23                 77. Defendant Vungle's Vungle SDK is incorporated into the following additional  
24                 Game Tracking Apps developed by Kiloo: Spellbinders and Tesla Tubes.

25                   **D. Fraudulent Concealment and Tolling.**

26                   78. The applicable statutes of limitations are tolled by virtue of Defendants' knowing  
27                   and active concealment of the facts alleged above. Plaintiffs and class members were ignorant of  
28                   the information essential to the pursuit of these claims, without any fault or lack of diligence on  
                    their own part.

1           79.     At the time the action was filed, Defendants were under a duty to disclose the true  
2 character, quality, and nature of its activities to Plaintiffs and the classes. Defendants are  
3 therefore estopped from relying on any statute of limitations.

4           80.     Defendants' fraudulent concealment is common to the classes.

5           **E.     Named Plaintiff Allegations**

6           **Plaintiff Michael McDonald and His Children, P.G.M., P.S.M., and P.R.M.**

7           81.     In or around 2014 or 2015, Mr. McDonald downloaded the Developer Defendants'  
8 App "Subway Surfers" onto his mobile devices in order for his children, P.G.M., P.S.M., and  
9 P.R.M., to play the game. P.G.M., P.S.M., and P.R.M. thereafter frequently played Subway  
10 Surfers on these devices an ongoing and continuous basis.

11          82.     On information and belief, during the time P.G.M., P.S.M., and P.R.M. played  
12 Subway Surfers, one or more of the SDK Defendants had, with the permission of the Developer  
13 Defendants, embedded one or more advertising SDKs which collected, disclosed, or used  
14 personal information and persistent identifiers of P.G.M., P.S.M., and P.R.M.. Defendants did not  
15 collect P.G.M.'s, P.S.M.'s, or P.R.M.'s personal information to provide support for the internal  
16 operations of Subway Surfers, but instead to profile P.G.M., P.S.M., and P.R.M. for commercial  
17 gain.

18          83.     The Defendants never asked Mr. McDonald for his verifiable parental consent – in  
19 any form or at any time – to collect, disclose, or use his children's personal information, including  
20 persistent identifiers, as required by COPPA.

21          84.     The Defendants never provided direct notice – as required by COPPA – to Mr.  
22 McDonald regarding Defendants' practices with regard to collecting, using, and disclosing his  
23 children's personal information, or regarding the rights of Mr. McDonald or his children under  
24 COPPA, either when Mr. McDonald initially downloaded the app, or afterwards, on the app's  
25 home or landing screen.

26          85.     Defendants' tracking and collection of P.G.M.'s, P.S.M.'s, and P.R.M.'s personal  
27 information without his verifiable parental consent is highly offensive to Mr. McDonald and  
28

1 constitutes an invasion of his children’s privacy and of Mr. McDonald’s right to protect his  
2 children from this invasion.

3 **Plaintiff Tamara Draut and Her Child, H.D.-F.**

4 86. In 2015 or 2016, Ms. Draut downloaded the Developer Defendants’ App “Subway  
5 Surfers” onto her mobile device in order for her daughter to play the game. H.D.-F. thereafter  
6 frequently played Subway Surfers on this device on an ongoing and continuous basis.

7 87. On information and belief, during the time H.D.-F. played Subway Surfers on the  
8 device, one or more of the SDK Defendants had, with the permission of the Developer  
9 Defendants, embedded one or more advertising SDKs which collected, disclosed or used  
10 persistent identifiers of H.D.-F. Defendants did not collect H.D.-F.’s personal information to  
11 provide support for the internal operations of Subway Surfers, but to profile H.D.-F. for  
12 commercial gain.

13 88. The Developer Defendants never asked Ms. Draut for her verifiable parental  
14 consent – in any form or at any time – to collect, disclose, or use her child’s personal information,  
15 including persistent identifiers, as required by COPPA.

16 89. The Developer Defendants never provided direct notice to Ms. Draut – as required  
17 by COPPA – regarding Defendants’ practices with regard to collecting, using, and disclosing her  
18 child’s personal information, or regarding the rights of Ms. Draut or her child under COPPA,  
19 either when Ms. Draut initially downloaded the app, or afterwards, on the app’s home or landing  
20 screen.

21 90. Defendants’ tracking and collection of H.D.-F.’s personal information without Ms.  
22 Draut’s verifiable parental consent is highly offensive to Ms. Draut and constitutes an invasion of  
23 her child’s privacy and of Ms. Draut’s right to protect her child from this invasion.

24 **VI. CLASS ALLEGATIONS**

25 91. Plaintiffs seek class certification of the classes and subclass set forth herein  
26 pursuant to Federal Rule of Civil Procedure 23.

27  
28

1           92.     Plaintiffs seek class certification of claims for the common law privacy cause of  
2 action “Intrusion Upon Seclusion,” on behalf of a multi-state class, with a class defined as  
3 follows:

4                   **The Multi-state Class:** all persons residing in the States of  
5 Alabama, Alaska, Arizona, Arkansas, California, Colorado,  
6 Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa,  
7 Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota,  
8 Missouri, Nevada, New Hampshire, New Jersey, New Mexico,  
9 North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South  
10 Dakota, Texas, Utah, Vermont, Washington, and West Virginia  
11 who are younger than the age of 13, or were younger than the age  
12 of 13 when they played the Game Tracking Apps, and their parents  
13 and/or legal guardians, from whom Defendants collected, used, or  
14 disclosed personal information without verifiable parental consent.

15           93.     Plaintiffs seek class certification of a claim for violation of the State of California  
16 Constitution Right to Privacy on behalf of a subclass of the Multi-state Class, with a subclass  
17 defined as follows:

18                   **The California Subclass of the Multi-state Class:** all persons  
19 residing in the State of California who are younger than the age of  
20 13, or were younger than the age of 13 when they played the Game  
21 Tracking Apps, and their parents and/or legal guardians, from  
22 whom Defendants collected, used, or disclosed personal  
23 information without verifiable parental consent.

24           94.     Plaintiffs seek class certification of a claim for violation of the State of New York  
25 General Business Law § 349 on behalf of a class defined as follows:

26                   **The New York Class:** all persons residing in the State of New  
27 York who are younger than the age of 13, or were younger than the  
28 age of 13 when they played the Game Tracking Apps, and their  
parents and/or legal guardians ,from whom Defendants collected,  
used, or disclosed personal information without verifiable parental  
consent.

          95.     Plaintiffs reserve the right to modify or refine the Class or Subclass definitions  
based upon discovery of new information and in order to accommodate any of the Court’s  
manageability concerns.

          96.     Excluded from the Classes and Subclass are: (a) any Judge or Magistrate Judge  
presiding over this action and members of their staff, as well as members of their families; (b)  
Defendants, Defendants’ predecessors, parents, successors, heirs, assigns, subsidiaries, and any  
entity in which any Defendant or its parents have a controlling interest, as well as Defendants’

1 current or former employees, agents, officers, and directors; (c) persons who properly execute and  
2 file a timely request for exclusion from the Classes or Subclass; (d) persons whose claims in this  
3 matter have been finally adjudicated on the merits or otherwise released; (e) counsel for Plaintiffs  
4 and Defendants; and (f) the legal representatives, successors, and assigns of any such excluded  
5 persons.

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

10       98.     **Numerosity (Rule 23(a)(1)).** The Classes and Subclass are so numerous that  
11 joinder of individual members herein is impracticable. The exact number of Class or Subclass  
12 members, as herein identified and described, is not known, but download figures indicate that the  
13 Game Tracking Apps have been downloaded more than a billion times.<sup>8</sup>

14       99.     **Commonality (Rule 23(a)(2)).** Common questions of fact and law exist for each  
15 cause of action and predominate over questions affecting only individual Class and Subclass  
16 members, including the following:

17               i.     Whether Developer Defendants engaged in the activities referenced  
18 in paragraphs 39 to 90 via the Game Tracking Apps;

19               ii.    Whether the SDK Defendants engaged in the activities referenced  
20 in paragraphs 39 to 90 via the Game Tracking Apps;

21               iii.   Whether Defendants provided disclosure of all the activities  
22 referenced in paragraphs 39 to 90 on a website as required by COPPA;

23               iv.    Whether Defendants directly notified parents of any of the activities  
24 referenced in paragraphs 39 to 46, 52, 55-77, 80-90;

25               v.     Whether Defendants sought verifiable parental consent prior to  
26 engaging in any of the activities referenced in paragraphs 39 to 46, 52, 55-77, 80-90;

27 \_\_\_\_\_  
28 <sup>8</sup> See n 2, *infra*.

1 vi. Whether Defendants provided a process or mechanism for parents  
2 to provide verifiable parental consent prior to engaging in any of the activities referenced in  
3 paragraphs 39 to 46, 52, 55-77, 80-90;

4 vii. Whether Defendants received verifiable parental consent prior to  
5 engaging in any of the activities referenced in paragraphs 39 to 46, 52, 55-77, 80-90;

6 viii. Whether Defendants' acts and practices complained of herein  
7 violate COPPA;

8 ix. Whether Defendants' acts and practices complained of herein  
9 amount to acts of intrusion upon seclusion under the law of Alabama, Alaska, Arizona, Arkansas,  
10 California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas,  
11 Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New  
12 Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota,  
13 Texas, Utah, Vermont, Washington, and West Virginia;

14 x. Whether Defendants' conduct violated Subclass members'  
15 California constitutional Right to Privacy;

16 xi. Whether Defendants' acts and practices complained of herein  
17 violate New York General Business Law § 349;

18 xii. Whether members of the Classes and Subclass have sustained  
19 damages, and, if so, in what amount; and

20 xiii. What is the appropriate injunctive relief to ensure Defendants no  
21 longer illegally collect children's personal information to track them over time and across  
22 different websites or online services.

23 100. **Typicality (Rule 23(a)(3)).** Plaintiffs' claims are typical of the claims of members  
24 of the proposed Classes and Subclass because, among other things, Plaintiffs and members of the  
25 Classes and Subclass sustained similar injuries as a result of Defendants' uniform wrongful  
26 conduct and their legal claims all arise from the same events and wrongful conduct by  
27 Defendants.  
28

1           101.   **Adequacy (Rule 23(a)(4)).** Plaintiffs will fairly and adequately protect the  
2 interests of the proposed Classes and Subclass. Plaintiffs' interests do not conflict with the  
3 interests of the Classes and Subclass members and Plaintiffs have retained counsel experienced in  
4 complex class action and data privacy litigation to prosecute this case on behalf of the Classes  
5 and Subclass.

6           102.   **Predominance & Superiority (Rule 23(b)(3)).** In addition to satisfying the  
7 prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under  
8 Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only  
9 individual Class and Subclass members, and a class action is superior to individual litigation and  
10 all other available methods for the fair and efficient adjudication of this controversy. The amount  
11 of damages available to individual Plaintiffs is insufficient to make litigation addressing  
12 Defendants' conduct economically feasible in the absence of the class action procedure.  
13 Individualized litigation also presents a potential for inconsistent or contradictory judgments, and  
14 increases the delay and expense presented by the complex legal and factual issues of the case to  
15 all parties and the court system. By contrast, the class action device presents far fewer  
16 management difficulties and provides the benefits of a single adjudication, economy of scale, and  
17 comprehensive supervision by a single court.

18           103.   **Final Declaratory or Injunctive Relief (Rule 23(b)(2)).** Plaintiffs also satisfy  
19 the requirements for maintaining a class action under Rule 23(b)(2). Defendants have acted or  
20 refused to act on grounds that apply generally to the proposed Classes and Subclass, making final  
21 declaratory or injunctive relief appropriate with respect to the proposed Classes and Subclass as a  
22 whole.

23           104.   **Particular Issues (Rule 23(c)(4)).** Plaintiffs also satisfy the requirements for  
24 maintaining a class action under Rule 23(c)(4). Their claims consist of particular issues that are  
25 common to all Class and Subclass members and are capable of class-wide resolution that will  
26 significantly advance the litigation.

27  
28

1 **VII. CLAIMS FOR RELIEF**

2 **COUNT I**  
3 **Intrusion Upon Seclusion**  
4 **(Brought on Behalf of the Multi-state Class)**

5 105. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

6 106. Plaintiffs and Class members have reasonable expectations of privacy in their  
7 mobile devices and their online behavior, generally. Plaintiffs' and Class members' private  
8 affairs include their behavior on their mobile devices as well as any other behavior that may be  
9 monitored by the surreptitious tracking employed or otherwise enabled by the Game Tracking  
10 Apps.

11 107. The reasonableness of such expectations of privacy is supported by Developer  
12 Defendants' unique position to monitor Plaintiffs' and Class members' behavior through their  
13 access to Plaintiffs' and Class members' private mobile devices. It is further supported by the  
14 surreptitious, highly-technical, and non-intuitive nature of Defendants' tracking.

15 108. Defendants intentionally intruded on and into Plaintiffs' and Class members'  
16 solitude, seclusion, or private affairs by intentionally designing the Game Tracking Apps (as well  
17 as all SDKs identified in this Complaint) to surreptitiously obtain, improperly gain knowledge of,  
18 review, and/or retain Plaintiffs' and Class members' activities through the monitoring  
19 technologies and activities described herein.

20 109. These intrusions are highly offensive to a reasonable person. This is evidenced by,  
21 *inter alia*, the legislation enacted by Congress, rules promulgated and enforcement actions  
22 undertaken by the FTC, and countless studies, op-eds, and articles decrying the online tracking of  
23 children. Further, the extent of the intrusion cannot be fully known, as the nature of privacy  
24 invasion involves sharing Plaintiffs' and Class members' personal information with potentially  
25 countless third-parties, known and unknown, for undisclosed and potentially unknowable  
26 purposes, in perpetuity. Also supporting the highly offensive nature of Defendants' conduct is  
27 the fact that Defendants' principal goal was to surreptitiously monitor Plaintiffs and Class  
28 members—in one of the most private spaces available to an individual in modern life—and to  
allow third-parties to do the same.



1 110. Plaintiffs and Class members were harmed by the intrusion into their private  
2 affairs as detailed throughout this Complaint.

3 111. Defendants' actions and conduct complained of herein were a substantial factor in  
4 causing the harm suffered by Plaintiffs and Class members.

5 112. As a result of Defendants' actions, Plaintiffs and Class members seek injunctive  
6 relief, in the form of Defendants' cessation of tracking practices in violation of COPPA, and  
7 destruction of all personal data obtained in violation of COPPA.

8 113. As a result of Defendants' actions, Plaintiffs and Class members seek nominal and  
9 punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek  
10 punitive damages because Defendants' actions – which were malicious, oppressive, willful –  
11 were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive  
12 damages are warranted to deter Defendants from engaging in future misconduct.

13 **COUNT II**

14 **California Constitutional Right to Privacy**  
15 **(Brought on Behalf of the California Subclass of the Multi-state Class)**

16 114. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

17 115. Plaintiffs and Subclass members have reasonable expectations of privacy in their  
18 mobile devices and their online behavior, generally. Plaintiffs' and Subclass members' private  
19 affairs include their behavior on their mobile devices as well as any other behavior that may be  
20 monitored by the surreptitious tracking employed or otherwise enabled by the Game Tracking  
21 Apps.

22 116. The reasonableness of such expectations of privacy is supported by Developer  
23 Defendants' unique position to monitor Plaintiffs' and Subclass members' behavior through their  
24 access to Plaintiffs' and Subclass members' private mobile devices. It is further supported by the  
25 surreptitious, highly-technical, and non-intuitive nature of Defendants' tracking.

26 117. Defendants intentionally intruded on and into Plaintiffs' and Subclass members'  
27 solitude, seclusion, right of privacy, or private affairs by intentionally designing the Game  
28 Tracking Apps (as well as all SDKs identified in this Complaint) to surreptitiously obtain,

1 improperly gain knowledge of, review, and/or retain Plaintiffs' and Subclass members' activities  
2 through the monitoring technologies and activities described herein.

3 118. These intrusions are highly offensive to a reasonable person, because they  
4 disclosed sensitive and confidential information about children, constituting an egregious breach  
5 of social norms. This is evidenced by, *inter alia*, the legislation enacted by Congress, rules  
6 promulgated and enforcement actions undertaken by the FTC, and countless studies, op-eds, and  
7 articles decrying the online tracking of children. Further, the extent of the intrusion cannot be  
8 fully known, as the nature of privacy invasion involves sharing Plaintiffs' and Subclass members'  
9 personal information with potentially countless third-parties, known and unknown, for  
10 undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly  
11 offensive nature of Defendants' conduct is the fact that Defendants' principal goal was to  
12 surreptitiously monitor Plaintiffs and Subclass members—in one of the most private spaces  
13 available to an individual in modern life—and to allow third-parties to do the same.

14 119. Plaintiffs and Subclass members were harmed by the intrusion into their private  
15 affairs as detailed throughout this Complaint.

16 120. Defendants' actions and conduct complained of herein were a substantial factor in  
17 causing the harm suffered by Plaintiffs and Subclass members.

18 121. As a result of Defendants' actions, Plaintiffs and Subclass members seek  
19 injunctive relief, in the form of Defendants' cessation of tracking practices in violation of  
20 COPPA, and destruction of all personal data obtained in violation of COPPA.

21 122. As a result of Defendants' actions, Plaintiffs and Subclass members seek nominal  
22 and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek  
23 punitive damages because Defendants' actions – which were malicious, oppressive, willful –  
24 were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive  
25 damages are warranted to deter Defendants from engaging in future misconduct.

26 **COUNT III**  
27 **Violation of N.Y. Gen. Bus. Law § 349**  
28 **(Brought on Behalf of the New York Class)**

123. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

1 124. Plaintiffs and Class members are “persons” within the meaning of New York  
2 General Business Law § 349(h).

3 125. Each Defendant is a “person,” “firm,” “corporation,” or “association” within the  
4 meaning of N.Y. Gen. Bus. Law § 349.

5 126. Section 349 makes unlawful “[d]eceptive acts or practices in the conduct of any  
6 business, trade or commerce.”

7 127. Defendants conduct constitutes “deceptive acts or practices” within the meaning of  
8 N.Y. Gen. Bus. Law § 349. Defendants surreptitiously tracked children without disclosing their  
9 activities to their parents, in violation of applicable laws.

10 128. Defendants conduct occurred in the conduct of trade or commerce, and was  
11 directed at consumers.

12 129. Defendants conduct was misleading in a material way, because, *inter alia*,  
13 Defendants utilized technology—in the form of the SDKs described in this Complaint—into the  
14 Game Tracking Apps, yet failed to provide the required disclosures or obtain verifiable parental  
15 consent prior to tracking children over time and across websites and other online portals, as well  
16 as prior to sharing any of the data so obtained with third-parties or using said data for commercial  
17 purposes or any other undisclosed purposes. Given (1) the entirely passive and secretive nature  
18 of the tracking technology at play, and (2) the obligations *not to track children* under federal law  
19 absent *both* transparent disclosures *and* verified parental consent, it is clear that Defendants  
20 purposely misled Class members, in the course of surreptitiously tracking children playing the  
21 Game Tracking Apps.

22 130. As a result of Defendants’ deceptive acts and practices, Plaintiffs and Class  
23 members were injured and damaged in that they suffered a loss of privacy and autonomy through  
24 Defendants’ acquisition and use of children’s personal information, for Defendants’ own benefit,  
25 without the Class members’ knowledge or verifiable parental consent.

26 131. Because Defendants’ willful and knowing conduct caused injury to Plaintiffs and  
27 Class members, the Class seeks recovery of actual damages or \$50, whichever is greater,  
28 discretionary treble damages up to \$1,000, punitive damages, reasonable attorneys’ fees and

1 costs, an order enjoining Defendants’ deceptive conduct, and any other just and proper relief  
2 available under N.Y. Gen. Bus. Law § 349. Plaintiffs and Class members seek punitive damages  
3 because Defendants’ actions – which were malicious, oppressive, willful – were calculated to  
4 injure Plaintiffs and made in conscious disregard of Plaintiffs’ rights. Punitive damages are  
5 warranted to deter Defendants from engaging in future misconduct.

6 **VIII. PRAYER FOR RELIEF**

7 WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated,  
8 respectfully requests that this Court:

- 9 a) Certify this case as a class action, appoint Plaintiffs as Class and Subclass  
10 representatives, and appoint Plaintiffs’ counsel to represent the Classes and  
11 Subclass;
- 12 b) Find that Defendants’ actions, as described herein, constitute: (i) violations of  
13 New York General Business Law § 349, (ii) breaches of the common law claim of  
14 intrusion upon seclusion in the states of Alabama, Alaska, Arizona, Arkansas,  
15 California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois,  
16 Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri,  
17 Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio,  
18 Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont,  
19 Washington, and West Virginia; and (3) a violation of the right to privacy under  
20 California Constitution, Article I, Section 1;
- 21 c) Enter a declaratory judgment that Defendants’ actions of collecting, using, or  
22 disclosing personal information of child users without first obtaining verifiable  
23 parental consent violates COPPA;
- 24 d) Enter an order permanently enjoining Defendants from collecting, using, or  
25 disclosing personal information of child users without first obtaining verifiable  
26 parental consent;
- 27 e) Award Plaintiffs and Class and Subclass members appropriate relief, including  
28 actual and statutory damages and punitive damages, in an amount to be determined

- 1 at trial;
- 2 f) Award equitable, injunctive, and declaratory relief as may be appropriate;
- 3 g) Award all costs, including experts' fees, attorneys' fees, and the costs of
- 4 prosecuting this action; and
- 5 h) Grant such other legal and equitable relief as the Court may deem appropriate.

6 Dated: July 31, 2017

Respectfully Submitted,

7 /s/ Michael W. Sobol

8 Michael W. Sobol (State Bar No. 194857)  
msobol@lchb.com  
9 LIEFF CABRASER HEIMANN & BERNSTEIN, LLP  
275 Battery Street, 29th Floor  
10 San Francisco, CA 94111-3339  
Telephone: 415.956.1000  
11 Facsimile: 415.956.1008

12 Nicholas Diamand  
ndiamand@lchb.com  
13 Douglas I. Cuthbertson  
dcuthbertson@lchb.com  
14 Abbye R. Klamann (State Bar No. 311112)  
aklamann@lchb.com  
15 LIEFF CABRASER HEIMANN & BERNSTEIN, LLP  
250 Hudson Street, 8th Floor  
16 New York, NY 10013-1413  
Telephone: 212.355.9500  
17 Facsimile: 212.355.9592

18 Hank Bates (State Bar No. 167688)  
hbates@cbplaw.com  
19 Allen Carney  
acarney@cbplaw.com  
20 David Slade  
dslade@cbplaw.com  
21 CARNEY BATES & PULLIAM, PLLC  
519 W. 7<sup>th</sup> St.  
22 Little Rock, AR 72201  
Telephone: 501.312.8500  
23 Facsimile: 501.312.8505

24 *Attorneys for Plaintiffs and the proposed Classes*

25

26

27

28

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

**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: July 31, 2017

Respectfully Submitted,

/s/ Michael W. Sobol

---

Michael W. Sobol (State Bar No. 194857)  
msobol@lchb.com  
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP  
275 Battery Street, 29th Floor  
San Francisco, CA 94111-3339  
Telephone: 415.956.1000  
Facsimile: 415.956.1008

Nicholas Diamand  
ndiamand@lchb.com  
Douglas I. Cuthbertson  
dcuthbertson@lchb.com  
Abbye R. Klamann (State Bar No. 31112)  
aklamann@lchb.com  
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP  
250 Hudson Street, 8th Floor  
New York, NY 10013-1413  
Telephone: 212.355.9500  
Facsimile: 212.355.9592

Hank Bates (State Bar No. 167688)  
hbates@cbplaw.com  
Allen Carney  
acarney@cbplaw.com  
David Slade  
dslade@cbplaw.com  
CARNEY BATES & PULLIAM, PLLC  
519 W. 7<sup>th</sup> St.  
Little Rock, AR 72201  
Telephone: 501.312.8500  
Facsimile: 501.312.8505

*Attorneys for Plaintiffs and the Proposed Classes*